

Application Guide for the Inter-American Model Law on Document Management



Funded by
European Union



OAS

More rights for more people.

Inter-American Juridical Committee

Authorities as of August 7th, 2020

Ruth Stella Correa Palacio (Chair)
Luis García-Corrochano Moyano (Vice Chair)
George Rodrigo Bandeira Galindo
Milenko Bertrand Galindo Arriagada
Miguel Ángel Espeche Gil
Duncan B. Hollis
José Antonio Moreno Rodríguez
Alix Richard
Eric P. Rudge
Mariana Salazar Albornoz
Íñigo Salvador Crespo

Technical Secretariat of the Inter-American Juridical Committee

Department of International Law of the Secretariat for Legal Affairs.

This publication was prepared by the Department of International Law of the Secretariat for Legal Affairs of the Organization of American States, under the supervision of Jaime Moreno-Valle, Senior Legal Officer. Copyright © 2021. First edition, February 16, Washington DC.

OAS Cataloging-in-Publication Data

Organization of American States. Secretariat for Legal Affairs. Department of International Law.

Application guide for the Inter-American Model Law on Document Management / [Prepared by the Department of International Law of the Secretariat for Legal Affairs of the Organization of American States].

v. ; cm. (OAS. Official records ; OEA/Ser.D/XIX.12 2020 Add.2) ; (OEA/Ser.P AG/RES.2958 (L-O/20) ISBN 978-0-8270-7195-7

1. Freedom of information--America. 2. Freedom of expression--America.
3. Government information--America. I. Title. II. Series. III. Series: OEA/Ser.P AG/RES.2958 (L-O/20)

OEA/Ser.D/XIX.12 2020 Add.2

Graphic Design: Claudia Saidon - Graphic Ideas Inc.

Table of Contents

Explanatory Note	7
Chapter 1 Document Management Policy	9
1.1. Documents and files	10
1.2. Implementing a document management policy	12
1.3. Appointment of an authority to lead the management policy	15
1.4. Document management processes	16
Chapter 2 Document Analysis, Classification, and Description	21
2.1. Archive identification	22
2.2. Document classification	25
2.3. Document description	28
Chapter 3 Document Appraisal, Transfer, and Elimination	31
3.1. Document appraisal	32
3.2. Document transfer	35
3.3. Document elimination	38
Chapter 4 Information Access and Security	43
4.1. Access to public documents	43
4.2. Analysis of legal access to documents	46
4.3. Management of document access requests	48

4.4. Access restrictions and control	51
4.5. Minimum security measures for documents containing personal data	54
4.6. Exercise of the rights of access, rectification, cancellation, and objection of personal data	59
4.7. Information security	62
4.8. Reuse of public information	64

Chapter 5 Conservation and Contingency Management **69**

5.1. Preparation of an integrated document conservation plan	69
5.2. Custody and control of facilities	71
5.3. Environmental control	74
5.4. Preparation of a contingency management plan	76
5.5. Risk assessment	78

Chapter 6 Awareness Raising and User Assistance Services **81**

6.1. Awareness-raising	81
6.2. Assistance to the administration by archive services	83
6.3. Public assistance	85

Chapter 7 Electronic Administration **91**

7.1. Interoperability	91
7.2. Metadata	93
7.3. Document digitization	95

Chapter 8 Staff Profiles and Document Management Training **99**

8.1. Staff Responsibilities and Qualifications	99
8.2. Communication plan	101
8.3. Continuing education plan	103

Bibliography and Resources **107**

Addenda **133**

Explanatory Note

In October 2020, the General Assembly of the Organization of American States (OAS) approved the Inter-American Model Law 2.0 on Access to Public Information, as a renewed effort of the Organization to strengthen transparency and accountability, public trust in democratic institutions, and citizen empowerment –all of them key elements for the development of a democratic society.

As an additional resource for Member States, the Model Law 2.0 has been enhanced with an Inter-American Model Law on Document Management and its corresponding Application Guide, prepared not in the context of the consultation process, but in tandem by expert consultants. While these two instruments are not a part of the provisions of the Model Law 2.0 itself, they were nonetheless approved as *addenda* thereto, in order to provide a tool that responds to the needs of the Member States in a comprehensive manner, strengthening their efforts in the adoption or reform of legislation that guarantees access to public information, using these new standards as a reference.

Therefore, this Application Guide must be studied together with the Inter-American Model Law on Document Management, both of which were prepared with invaluable support and technical advice from the Red de Transparencia y Acceso a la Información (*Transparency and Access to Information Network - RTA*) and the Government of Spain's Subdirección General de los Archivos Estatales del Ministerio de Cultura y Deporte (Sub-Directorate General of the State Archives of the Ministry of Culture and Sports), within the framework of the European Union Cooperation Program with Latin America EUROsociAL +.

Document Management Policy

1.1	Documents and files	10
1.2	Implementing a document management policy	12
1.3	Appointment of an authority to lead the management policy	15
1.4	Document management processes	16

Definition of a document management policy

A document management policy is a declaration of intent adopted by the whole institution as a strategic pillar that sets out the main areas of activity, processes, responsibilities, and objectives in the area of document and archive management.

According to the main technical and regulatory references in archival matters, it is considered good practice for institutions to establish, maintain, document, and promulgate their own document management policy that defines documentary procedures and practices to ensure that the institution's information needs are covered and has the added benefit of facilitating accountability to stakeholders.

1.1 Documents and files

Definition of document

A document is defined as any information created, received, and kept as evidence, testimony, and an asset by an institution in the course of its activities or by virtue of its legal obligations, regardless of medium or technology platform.

The term “document” is always understood to be synonymous with “archive document”; that is, the material evidence of a deed or act carried out by physical or legal persons, whether public or private, in the exercise of their functions, with certain material and formal characteristics.

Definition of archive service

The archive service is the area responsible for document management, retention, and administration functions.

Description of the good practice

Initiatives in relation to transparency and access to public information depend to a large extent on the quality, reliability, and accessibility of the public archives with custody of that information. If the archives are not properly organized and well managed, it will be very complicated to confirm the authenticity and integrity of public information or meet the established deadlines for responding to the public and management. However, when there are adequate archive management controls in place, with effective standards and procedures, both members of the public and public officials can trust not only in the reliability of the data extracted from the archives, but also in the existence of a complete documentary record of the activities of public administrations.

The public administration generates and receives a considerable amount of documentation as a result of the necessary activities to fulfill its purposes and as a record of those activities. Such documents are not only important for the institution internally, but also have an external dimension in that they guarantee rights and duties for the administration as well as private citizens, and may be subject to control and verification, as well as be used to audit the administration's activities.

Public administrations generate a documentary heritage that is an essential part of the collective historical memory. At the same time, it is also constantly providing information on the powers of the public administration, which means that special attention should be given to processing, custody, and distribution of public documents, particularly in a context of transparency and access to information.

Documents contain information that constitutes a valuable resource and important asset for the institution.

Most of activities of public administrations that were once based on paper documents and files have been either partially or completely automated. As administrations migrate to an on-line environment, electronic documents, files, and archives will become the basis for:

- Managing resources
- Serving the public
- Measuring progress and results
- Protecting the rights and duties of all persons and of the administration itself.

Recommendations

1. Adopting standardized document management criteria is essential for the administration and society in general, as it allows documents to be protected and preserved as proof and evidence of their functions and activities.

2. Standardizing document management policy and procedures ensures:

- a.** Proper attention to and protection of documents;
- b.** That their probative value and information they contain can be efficiently and more-effectively preserved and recovered through the use of standardized practices and processes based on good practice.

3. Streamlining documentation through its various phases ensures effective and adequate management by integrating processing strategies for documents—whether in conventional or electronic media—in an institution’s overall management.

1.2 Implementing a document management policy

Definition of a document management policy

A document management policy is a declaration of intent adopted by the whole institution as a strategic pillar that sets out the main areas of activity, processes, responsibilities, and objectives in the area of document and archive management.

Description of the good practice

The scope of a document management policy, insofar as the institution’s creation and control of documents are concerned, should include high-level strategies capable of supporting all the functions and activities that the institution performs, as well as protecting the integrity of documents for as long as necessary.

The successful implementation of a document management policy in any institution yields a series of benefits:

- It helps the institution to fulfill its objectives more effectively and with a high degree of efficiency thanks to the definition of a set of documents, applications, and management processes adequate to the institution’s needs and objectives.
- It ensures transparency and traceability in decision-making within the institution and recognizes the responsibility of management and other members of the institution, as well as their capacity for good governance.
- It enables the institution as a whole to operate effectively by optimizing its activities and protecting its interests and the rights of current and future stakeholders.
- Activities are carried out in accordance with the legal, regulatory, technical, and accountability requirements that apply to the institution.

Recommendations

- 1.** The institution’s senior management should visibly and proactively support the implementation and maintenance of a document management policy and include it as an indispensable resource for achieving the institution’s strategic objectives.
- 2.** The document management policy should be designed taking account of the following elements:
 - a.** It should be aligned with the institution’s basic purpose and facilitate the achievement of its objectives.
 - b.** It should include commitments to satisfy requirements and continuous improvement.

c. It should be disseminated throughout the institution and be available to all personnel involved in the creation, maintenance, and use of documents.

3. The document management policy should be supported by a package of documents that includes the procedures, guidelines, models, and other documents that make up the institution's document and archive management system.

4. The institution should facilitate and encourage training and instruction for its personnel responsible for the creation and maintenance of documents, in keeping with the guidelines and procedures contained in the document management policy.

5. It is suggested that the document management policy include the following:

a. It should be founded on a preliminary analysis of how the institution actually functions, with document management procedures designed accordingly.

b. It should be as consistent as possible with the applicable standards on document and archive management at both national and international levels.

c. It should be presented using systems that facilitate its comprehension (relying on plain language, as opposed to technical jargon, and simple explanatory graphics, instead of complex diagrams).

d. Concrete objectives should be specified to gauge progress in implementation of the document management policy.

1.3 Appointment of an authority to lead the management policy

Definition of leadership

Leadership is the set of management or executive skills by which an individual can influence a particular group of persons and make them work enthusiastically as a team to meet goals and objectives. It is also understood as the capacity to take the initiative, manage, rally, promote, incentivize, motivate, and evaluate a group or team.

Description of the good practice

Establish a unit or agency in the administration, institution or organization to develop and lead the document management policy. This will make it possible to ensure that document management decisions, measures, and activities are established in accordance to law and properly documented. The authority designated to lead the document management policy, depending on the context where it is implemented, may be an archive management unit, a national records office, regional or local agencies, etc.

The International Council on Archives encourages national or regional archives to play a key role in supporting document management in public administrations.

Recommendations

1. An executive will first be assigned chief responsibility in the area of document management with a view to the allocation of the necessary resources, supervision of the various stages of implementation, and relevant activities planning.

2. The senior management of the institution should appoint a specific management representative who, aside from their other responsibilities, should:

- a.** Ensure that the document management policy and system are established, implemented, and maintained in accordance with the necessary requirements;
- b.** Be committed to communicating and raising awareness about the document management policy and archival processing throughout the institution;
- c.** Be committed to ensuring the sufficiency of technical, material, and human resources;
- d.** Be responsible for ensuring that the roles and responsibilities set out in the document management policy and system are correctly assigned and documented and that the staff who perform those duties have the appropriate competencies and receive the necessary training.

3. As an option, senior management may appoint a representative for document management and archives at the operational level, should the size and complexity of the institution and its document management processes make that appropriate.

1.4 Document management processes

Definition of process

A process is a linked sequence of activities that produce an added value to meet the needs of another person or unit, whether inside or outside the institution.

Description of the good practice

According to the leading technical and regulatory models for managing organizations and archives, it is regarded as a good practice for institutions to standardize and document their working processes in order to facilitate completion of tasks, objectives, and activities, thereby homogenizing all actions, facilitating continuous improvement of processes, and supporting continuing education for the institution's personnel.

By analyzing processes, institutions can identify the creation, incorporation, and control of those documents that they handle in the course of their various procedures. It also provides the necessary basis for determining the following:

- Identification of all the documents needed to document a particular function or activity performed in the institution.
- Development of functional classification charts to identify, organize, and locate documents.
- The continuity of links between documents and their context within the institution.
- Establishing guidelines or rules for identifying and managing the institution's documents over time.
- Identifying the owners of and responsibilities for documents over time.
- Setting appropriate time frames for the retention or elimination of documents by the institution, in accordance with its functions and activities.
- Analyzing risk management and defining an information security and control policy in the context of the institution's document management system.

That analysis of processes should crystallize into the standardization of its procedures, which will help boost effectiveness and efficiency in the institution's day-to-day running by allowing the corporate strategy to be deployed based on a clear and precise identification of all its activities and responsibilities.

Standardizing procedures also depends on all the institution's personnel working together as a team, which makes it possible to incorporate the key element of participatory management and training as one of the main continuous improvement objectives.

The systematic operation that comes from standardizing procedures in an institution offers a number of advantages:

- It allows expected outcomes in an institution to be predicted.
- It ensures that operations are conducted homogeneously throughout the institution, following the same guidelines, and that they are uniformly documented.
- It facilitates assignment and identification of responsibilities.
- It facilitates communication and relations among the institution's members.

Recommendations

1. Documenting procedures continues to be the tool most used for meeting the requirements set down in international quality standards, and the same thing is true for the institutions' management standards based on their documents. Hence, documenting procedures and standardizing them are pivotal in quality assurance and document management.

2. Before documenting anything, in order to ensure that procedures are standardized in the most suitable way possible, the following elements must first be identified:

- a.** What procedures does the institution carry out? What are the objectives of each procedure? Who benefits from those procedures (otherwise known as users)? What added value does the institution offer with that procedure?

- b.** Who is responsible for each procedure and who participates in it?

- c.** How specifically does the institution perform the various activities that go into the procedure?

3. Once those elements have been identified it is advisable to consider creating a package of documents that reflects everything that has been identified. To adequately document standardized procedures within an institution, a management tool known as a process map can be developed. A process map is not the hierarchical organizational chart of an institution, but functional flowchart of the business activities that the institution carries out in order to deliver added value to its users.

4. If the standardization of procedures in any institution is to achieve the desired result, it must be accompanied by a firm and resolute strategy to encourage education of the institution's staff in the areas of quality assurance and continuous improvement, stimulating buy-in, continuing education, and teamwork by everyone in the institution.

Document Analysis, Classification, and Description

2.1	Archive identification	22
2.2	Document classification	25
2.3	Document description	28

Definition of intellectual control

Intellectual control is the set of operational processes for document management that serve to address the intellectual needs of an institution's users in the area of document management, the added value of which becomes a fundamental resource for managing all the other institution's documentary or management processes.

This section examines good practices related to archive management processes whose purpose is to maintain effective intellectual control of documents kept in the archives and to have appropriate representations of those documents, so that the information contained in the fonds can be effectively managed.

2.1 Archive analysis

Definition of analysis

Analysis is the set of preliminary management activities that are used to analyze the actions performed in an institution and to map the full extent of the types of documents being handled. Analyzing any organization's organizational and functional structure reveals the way in which the documents handled by that organization are managed.

Description of the good practice

According to the main technical and regulatory references in archival matters, it is considered good practice for institutions to analyze their objectives and strategies, legal framework, structure, risk factors, and all the activities they carry out, together with the documentation that they have produced and continue to produce in connection with those activities, so as to garner as much knowledge as possible about the institution, its competencies, and all the changes that it has undergone over time, in order to establish on that basis a document management system that addresses all its expectations and realities.

An analysis is an intellectual activity that consists of conducting a thorough investigation of the document producer— i.e., the institution—and the different types of documents that it handles. Therefore, it is considered that the analysis must be done before the document and archive management system is implemented and be based on the following information that must be gathered:

- The institution's past and current objectives and strategies.
- The institution's past and present hierarchical structure.
- The legal, economic, or political framework that affects or has affected how the institution functions.

- The institution's past and present critical factors or weaknesses.
- The institution's past and present functions, activities, and operations.
- The institution's past and present business flows and processes.
- Types of documents previously and currently handled by the institution in connection with its process flows
- The document management system or systems previously and currently used by the institution.

A thorough analysis of this nature will yield a comprehensive knowledge of the institution's requirements and needs. That knowledge is known as the organization of the fonds and offers a comprehensive overview of the institution's fonds. That system of organization can be used to design basic tools in the various document management processes (classification charts, document appraisal or retention tables, document disposition, series organization, etc.).

Recommendations

1. The first step before any other in effectively implementing a document management policy is analysis, since that will make it possible to ensure that the management system ultimately designed and implemented is tailored to the structure and needs identified.
2. Information gathering should be systematic and encompass different sources, including analysis of regulatory documentation, analysis of documentation produced by the institution itself, interviews with the institution's staff, etc. The greater the number of information sources, the greater the knowledge of the institution.
3. It is advisable to systematize all the administrative categories that support the institution's structure, as well as functional categories, as that will reflect the entire institution from a document

perspective. This systematization is known as the principle of origin and allows all the documentation of an institution to be organized in the most effective way possible, thus avoiding mixing documents from different categories as well as their decontextualization.

4. It is recommended that the analysis be done starting with various fundamental—not necessary consecutive—elements:

a. Analysis of the organization. This consists of examining the institution that handles the documents. To carry it out, the most advisable thing is to gather all the legislation in force and extract it according to a uniform approach. The legislation will provide information about the organizational structure and basic functions, as well as their evolution over time. This organic analysis can also be completed with an examination of documents and staff interviews; however, it is better to use such sources for analyzing other elements.

b. Analysis of functions. This consists of examining an institution's functions, activities, and processes. The compilation of the legal framework yields information about the institution's basic functions, which will need to be supplemented with information on each function's lower tiers (activities, processes, actions). Those procedures will not appear in the legal framework but they can be examined through document analysis and staff interviews.

c. Document analysis. This consists of examining an institution's different document types and series. Once the information has been extracted from the organizational and functional analysis, it will be necessary to verify how it is reflected in the institution's documents. Therefore, the main source of information for this area of analysis is the actual documents handled by the institution (types or collections of documents produced in the course of a particular activity).

2.2 Document classification

Definition of document classification

Document classification is the basic operational process for designing the set of document management procedures or strategies in an institution, the result of which offers essential added value for planning and determining numerous subsequent procedures, such as establishing document retention periods, information access methodology, or the possibilities of information and document retrieval from the document repository.

Description of the good practice

According to the main technical and regulatory references on document management, it is considered good practice for institutions to develop a document classification chart that reflects all the institution's activities and supports all document management processes.

The classification chart is the fundamental tool for the regular functioning of any institution as well as for developing any document management process.

In concrete terms, a classification chart offers an institution the following advantages:

- It establishes linkages between different documents managed in the institution.
- It ensures that documents are denominated in a consistent manner over time.
- It assists with information retrieval and the documents containing that information.
- It allows security and access levels to be defined for collections of documents classified by documentary series.
- It enables levels of clearance to be granted to individuals.

- It distributes responsibility for management of document groupings.
- It distributes documents for the effective performance of the institution's work.
- It facilitates establishing appropriate time frames and measures for the appraisal (retention or elimination) of each document.

The classification chart should be based on the functions or activities that are carried out in the institution. A functions-based classification system can provide a systematic and effective framework for document management. A functions examination performed during the preliminary analysis of the institution will yield knowledge about all the institution's activities and situate them in the context of the objectives and strategies set by management.

The classification chart is a tool that reflects the functions, activities, and operations of an institution. It can be used to develop other tools of critical importance for other document and archive management processes in an institution (thesauri, indexing rules, series catalogues, access and appraisal tables, document elimination and retention, etc.)

Recommendations

1. A classification chart can reflect the simplicity or complexity of any institution. Therefore, the preliminary analysis first done of the institution must be as thorough as possible in order to gain as much knowledge as possible about the activities and documents being handled.
2. The classification chart should be designed in partnership with those who create and manage the documents, since it is they who are most familiar with the day-to-day workings of their respective procedures.
3. The classification chart should be reviewed regularly to take account of the institution's changing needs, thus ensuring that its

structure is kept up to date and reflects any alterations that may occur in its functions or activities.

4. The classification chart should be structured hierarchically as follows:

- a. The first level reflects the function.
- b. The second level reflects the activities that make up the function.
- c. The third level reflects the groups of operations or procedures that go into each activity.

More levels may be included depending on the complexity of the institution's functions. The degree of precision of the classification chart must be determined by the institution that it represents and reflect the complexity of each of the functions carried out in it.

5. Those responsible for developing the classification chart can confirm if their tool is functioning properly by checking that it meets the following parameters:

- a. The chart uses the denominations that appear in its functions and activities structure, not those of the units that make up the institution.
- b. The chart is pertinent to the institution and seeks coherent linkage between the various units that share information and document groupings based on the way in which its functions interrelate.
- c. The hierarchical structure of the classification chart goes from the broadest to the narrowest concept; in other words, from the high-level functions of the institution to the most specific operations or actions.
- d. The terms used in the chart are unambiguous and reflect the daily practice of the institution.

- e. The chart is composed of a sufficient number of groupings that contemplate all the functions that generate or manage documents.

2.3 Document description

Definition of document description

Document description is an essential function not only in the processing of archival information that facilitates access to archives and information about documents by means of descriptive instruments, but also for understanding the context and content of documents, their provenance, the functions that they reflect, the matters that they concern, their characteristics, and volume.

Description of the good practice

Archival description is directly linked to the prior processes of analysis and classification, since information can only be described if it is properly organized. Moreover, the mere fact that an archive is well organized does not, in itself, guarantee that the information it contains can be accessed and consulted. For that, its contents need to be described.

Therefore, description is an essential requirement for other processes, such as those associated with document appraisal, archive dissemination, and archive reference and consultation services. A fonds cannot be properly appraised, conserved, and disseminated if its contents, institutional provenance, and the functions that prompted its creation and use are not known.

Recommendations

1. Archive documents must be represented in a comprehensible way that provides information about the context of their creation, institution, and contents.
2. One of the primary aims of implementing the technical function of description is to facilitate access to documents.
3. Correct description of the information contained in documents will make it possible to verify the authenticity of the provenance of those same archive documents.
4. Before taking any steps with regard to archival description, a diagnostic study of the situation must be carried out.
5. The government will propose steps for the design of a description policy for its institutions or system of archives.
6. An archival description plan or institutional archive systems should be established in institutions.
7. Archival policies that apply to the whole institution or system of archives will be adopted in accordance with the guidelines set by the respective governing entities for archival matters.

Document Appraisal, Transfer, and Elimination

3.1	Document appraisal	32
3.2	Document transfer	35
3.3	Document elimination	38

Definition of document appraisal

Document appraisal is an archival processing phase that consists of analyzing and determining the primary and secondary values of document series and establishing time frames for transfer, access, and retention or elimination, whether total or partial.

Definition of retention calendar

The retention calendar is the instrument resulting from the appraisal of document series produced by an institution. The calendar identifies series and types of documents, as well as documents classed as essential; it also assigns retention time frames and standardizes retention formats.

3.1 Document appraisal

Description of the good practice

It is considered good practice for the institution to design and implement an appraisal system, including several processes that go into series identification and, therefore, the activities they record and analysis of the value of documents in order to propose their selection for permanent retention or elimination and the relevant time frames.

Appraisal is an integral part of information and document management policies and systems.

All appraisal systems should rest on three pillars: first, it must be governed by a regulatory law; second, it must be under the direction of an authority with vested powers and responsibilities; third, it must produce and apply decisions, which are normally reflected in what are generally known as appraisal calendars.

This section groups together the good practices that will enable this procedure to be optimized.

Recommendations

1. The organization's management must approve the appraisal standards. Irregular destruction of documents can give rise to severe financial penalties in some cases and in some countries liability to criminal prosecution. It is essential for the institution to have rules on the approval of retention time frames for its documents and regularized destruction systems.

2. The subject of appraisal per se are document series, understood as the collection of individual or compound documents produced by an institution that reflects one or more activities or processes carried out in exercise of its competencies. Single document units or general archives or fonds are not appraised.

3. Administrative documents and their production contexts are subject to appraisal because the aim is to discern not only administrative uselessness, but their permanence as a record and memory.

4. Physical and electronic documents are equally subject to appraisal.

5. Appraisal identifies the series that contain essential information for the institution, thus ensuring that it is properly protected, retained, and preserved; it also identifies documents that underpin rights and duties, not only of the institution, but also of third parties.

6. Destruction is not an end but a means in the appraisal process; the aim is not to eliminate simply to reduce the volume of documents, but to get rid of what is pointless to preserve for posterity.

7. It is necessary to ensure the long-term retention of documents that will help in the future to explain how a society or an entity involved from various standpoints (social, political, economic, technological, etc.).

8. An appraisal procedure must be established that determines the point in a document's lifespan at which it may be consulted by persons, and in what circumstances and conditions, always in accordance with the law, particularly the provisions that deal specifically with access to public information.

9. All appraisal systems should rest on three pillars: first, it must be governed by regulatory standards; second, it must be under the direction of an authority with vested powers and responsibilities; third, it must produce and apply decisions, which are normally reflected in what are generally known as retention calendars or document retention tables.

10. Once responsibility for elimination has been created, specific bodies or entities—e.g., an institutional appraisal committee—should be established in the institution to sanction, control, and quantify appraisal. To that end, criteria and procedures must be established for exercising that responsibility in the institution.

11. Responsibility for the document appraisal process should be shared by administrative managers, document managers, archivists, lawyers, and users.

12. It is essential to document all operations deriving from appraisal. Thus, the appraisal and elimination process will be situated within a transparent and reliable framework, be aligned with the quality assurance systems, and integrate the archive in the institution's management systems.

13. The document series appraisal form is intended to provide the body or committee that sanctions and controls appraisal with as much information as possible, so that they can weigh the value of the documents in the document series under appraisal.

14. At a minimum, the retention calendar should include the following elements:

a. The document series data. They are filled out by the Archive and include the following information:

- Series denomination, producing unit, purpose of administrative management
- series length in years
- type of medium
- series volume
- documents in the series
- organization
- legislation and regulation
- administrative procedure
- series location
- antecedent or related series
- Summary documents and duplicates
- Proposed appraisal
- Proposed user access
- Proposed decision and comments

b. Information to be filled out by the appraisal committee after its meeting to adopt the appraisal decision. It includes the following:

- Appraisal decision
- Decision on access
- Decision on standardization of administrative procedure, as appropriate
- Comments

c. Data for the document series appraisal file or certificate. It includes:

- Decision number
- Approval meeting
- Date of decision
- Signatures of those responsible

15. The appraisal should not wait for the documents to enter the archive but should be done in advance, even before the documents are produced. By streamlining their production and use, procedures can be standardized and the production of useless documents avoided, while decisions can also be taken on control and regulation of access.

16. Incorporating the appraisal criteria in the electronic document design, redesign, or production phase is essential. Therefore, it is vital to involve the information providers or document producers.

3.2 Document transfer

Definition of document transfer

Document transfer is the usual procedure for entering material in an archive by transferring fractions of documents series once they have reached the time limit set by the rules established in the appraisal for each stage of the lifespan of documents.

Description of the good practice

It is considered good practice for institutions to design and implement a transfer procedure for archive documents based on the results of the appraisal phase, taking into account the main activities of the process, regardless of the document format.

Recommendations

1. Once the time limit set for retention in document-producing units has been reached, documents must be transferred to the archive in order to reduce the space that offices use for document retention and to improve effectiveness in the management of infrequently used documents, even if they still retain their administrative value.
2. The transfer calendar is the management instrument that governs the physical transfer of documents to the storage areas managed by the archive. Under that calendar, each unit is assigned a deadline for transferring documents.
3. The document retention period in producing units is set by the appraisal committee or another competent body, based on an analysis of each document series and the relevant standards.
4. Usually, the annual transfer date is established by mutual agreement between the person with that responsibility in each unit and the person in charge of the archive, so that the transfer operation interferes as little as possible with the normal activities of the office producing the documents.
5. All document transfers are to be accompanied by a delivery list or form which should provide the necessary information about the documents being transferred.
6. The delivery list should describe the contents of the documents in an identifiable, thorough, and relevant way, otherwise it will not be possible to monitor whether or not a specific file has been transferred or allow efficient retrieval of documents.
7. The receiving archive will compare or check the data contained in the delivery list in order to verify that the information shown matches the documents being received, since from that point forward the archive becomes responsible for them. Once verified, the data to be filled out by the archive is included and the list is signed, which is understood as approval by the person in charge of the archive.
8. The delivery list or transfer form is drawn up in triplicate, with one of the copies returned to the unit or sending archive and the receiving archive keeping the other two: one in the general admissions register and the other in the sending units register.
9. Transfers are also made in electronic management systems (though no physical document transfers occur) and involve a series of fundamental changes:
 - a. The entry of documents in the archive entails a change of responsibility, which transfers from the manager to the archivist.
 - b. Following the moment of transfer, the policies on access, migration, and retention and destruction will apply in accordance with the instructions of the competent appraisal committee.
10. When electronic documents are transferred from one document management system to another, provision must be made for the following:
 - a. Format compatibility
 - b. Medium compatibility
11. Electronic document metadata must be transferred along with the document in order to enable its identification, authenticity, and any retention procedures that may be necessary in the future.
12. Electronic documents are entered in the archive together with their metadata and the appropriate signatures. The archive

may add a stamp or signature as a guarantee of the integrity and authenticity of the document throughout its lifetime, which could do away with the task of maintaining the signature verification system.

13. Aside from metadata and the appropriate signatures, the documents should be accompanied by other supplementary documents, such as:

- a.** Indications as to procedures for use and access privileges
- b.** Indications as to procedures for prevention, correction, and discovery of information losses or changes thereto
- c.** Indications as to retention procedures in relation to media deterioration and technological obsolescence.

3.3 Document elimination

Definition of document elimination

Document elimination is the process by which documents are destroyed or computer systems are decommissioned or wiped, once their value (administrative, legal, informational, historic, testimonial) has been analyzed and found to be worthless for all intents and purposes.

Description of the good practice

It is considered good practice for institutions to design and implement a process for elimination of document series and units as part of the archival procedure that identifies documents that are to be destroyed in accordance with the time frames established in the appraisal phase. Document series or units are always physically destroyed when they cease to have value in an administrative or

probative sense or in terms of establishing or extinguishing rights, and have neither developed significant historical or testimonial value nor are expected to do so.

Recommendations

- 1.** Document series or units should only be physically destroyed once they have completely lost their value and administrative utility and have no historical worth that might warrant their permanent conservation; it should only be done on the basis of a regulated and authorized elimination process.
- 2.** Physical destruction should be done by the body responsible at the archive or public office where they are located, using any method that ensures the impossibility of their reconstruction and subsequent use, or recovery of any of the information they contain.
- 3.** Documents that contain private or secret information must be eliminated according to a procedure that guarantees the preservation of their information and the impossibility of recomposition.
- 4.** Strip-cut or cross-cut shredding is the most appropriate method for eliminating paper documents. The paper is turned into strips or particles, whose size is chosen according to the level of protection required for the information contained in the documents to be destroyed.
- 5.** Electronic documents have specific characteristics that must be taken into account when eliminating them:
 - a.** They are stored in storage media with a specific format
 - b.** The information contents are independent of the medium and format
 - c.** The media can usually be reused
 - d.** Their lifespan is short compared with a paper medium

- e.** The destruction procedures should take account of the characteristics of the media best suited for the conservation of electronic documents
 - f.** There may be multiple copies of documents that are not always tracked
- 6.** Bearing in mind the characteristics of electronic documents, it is recommendable to use wiping (understood as the procedure for eliminating data or files from a medium or set of media, allowing its reuse) and destruction (understood as the physical destruction of a storage medium containing electronic documents).
- 7.** Suitable wiping techniques must be identified for each medium (optical, magnetic, external memories, etc.) and type of information, and a record kept of the wiping procedures carried out.
- 8.** Documents marked for destruction should be protected against any possible external intrusion until they are destroyed.
- 9.** All document handling and transportation operations during the transfer and up to the moment of destruction must be done by authorized and identifiable personnel. The transportation should be used exclusively for documents to be eliminated and travel directly to the place where they will be destroyed.
- 10.** Hiring a company specializing in document destruction services may be an advisable option, depending on the volume of documents and the technical means required. In such cases, particular care should be taken with the destruction process:
- a.** A representative of the person responsible for the documents should be required to witness their destruction and verify the conditions in which it is done as well as the results.
 - b.** It must be guaranteed that the documents are destroyed at their facilities using their own means, without any subcontracting that would entail the documents being handled by other companies without the knowledge of the person responsible for the documents.
- c.** A certificate of destruction of the documents should be required that formally states that the information no longer exists, as well as where, when, and how it was destroyed.
- 11.** The place or containers used to store documents to be eliminated require effective security measures against possible external intrusion. They should not be left exposed outside buildings. They should also not be piled up in places where people walk by or on open premises.
- 12.** The elimination process should always be documented in a record of elimination.
- 13.** Once the authorization obtained becomes enforceable, the body responsible for the custody of documents will open an elimination file for the documents or document series concerned.

Information Access and Security

4.1	Access to public documents	43
4.2	Analysis of legal access to documents	46
4.3	Management of document access requests	48
4.4	Access restrictions and control	51
4.5	Minimum security measures for documents containing personal data	54
4.6	Exercise of the rights of access, rectification, cancellation, and objection of personal data	59
4.7	Information security	62
4.8	Reuse of public information	64

4.1 Access to public documents

Definition of access to public information

Access to public information is the fundamental right of persons to consult information in the possession, custody, or control of any obligated entity, having been produced or received by public authorities in the exercise of their functions and that is not subject to the exceptions regime. Where that information is recorded in document form, the right of access to public documents is also recognized and applies to all archived information in any format or medium.

This section looks at good practices in relation to access, one of the most important archival functions. The subject is examined from three perspectives: policy on access to public documents, reuse of information in the public sphere, and active citizen participation. Implementing these good practices will ensure transparency and access to public information.

Description of the good practice

Access to public documents is one of the main challenges facing public institutions in general, and archival institutions in particular. That is because it involves the realization of a human right that is recognized in international treaties as well as in many of our countries' constitutions and laws. Consequently, guaranteeing that right is an obligation for public administrations, as one of the main instruments for ensuring transparency, accountability and, therefore, open government. Accordingly, it is generally considered that document and archive management policies should, in turn, include a policy on access to public documents.

Recommendations

1. International best practice recommends the adoption at the highest decision-making level of a policy on access to public documents and an implementation guide to that end that is consistent with the legal framework in force.
2. At a minimum, the document setting out that policy should contain:
 - a. A declaration of principles by the institution on access to public documents and a list of commitments to that end. The declaration of principles and commitments should clearly recognize people's right of access to public documents in the broadest possible terms, on an equal and impartial footing, including the possibility of challenging denials of access.

- b. Clear information about existing restrictions, their reasons, and their basis (legal and regulatory standards, judicial decisions, internal policies and rules of procedure, agreements with document donors or depositors)

- c. Clear information on the necessary administrative procedure, as applicable, for requesting access: competent authority, time limits on decisions, established challenges regime, application form.

- d. Definition of a series of indicators on exercise of the right of access for periodic evaluation of compliance with the policy.

3. It is recommended that compliance with the policy be periodically evaluated (at least annually), that mechanisms be introduced for correcting shortcomings or making improvements to the policy, and that a series of indicators be used for that evaluation.

4. The document containing the access policy should be disseminated as broadly as possible, periodically updated, and available on the institution's website.

5. The access policy implementation guide should set out the necessary technical and administrative processes for performance of the legal obligations and commitments specified in the policy and describe how responsibilities and duties with regard to access are distributed.

6. It is recommended that the institution's declaration of principles on access to public documents endorse or be based on the Principles of Access to Archives adopted by the International Council on Archives at its General Assembly on August 24, 2012; on international standards and good practice; and on the ethical principles relating to access contained in the professional code of ethics.

7. As one of those principles, victims of serious crimes under international law should be guaranteed access to archives and documents containing the evidence they need to uphold their

rights and document violations of those rights, including when the documents or archives concerned are not accessible for the general public.

8. The ICA Technical Guidance on Managing Archives with Restrictions (2014) contains a number of recommendations based on internationally recognized practices for implementing the necessary restrictions on access in order to safeguard other rights and legal interests that warrant protection under legal and regulatory standards.

4.2 Analysis of legal access to documents

Definition of legal access

Legally accessible documents are archive documents that may be consulted under laws in force.

Description of the good practice

The analysis of legal and regulatory access is the technical process concerned with identifying categories of content in each documentary series that may be subject to restriction on the basis of a provision of law, as well as with determining statutory time limits on access that might be applicable, as appropriate, under those provisions; appropriate security measures for guaranteeing secrecy where the law so requires; and possible means for facilitating full or partial access to documents when necessary to comply with a legal provision. The findings of the analysis, contained in various system instruments (in particular, the access and security table) inform, together with the appropriate user permissions, the relevant access controls and decision-making processes in relation to access.

Recommendations

- 1.** It is considered good practice for this process to be based on a prior analysis of the institution's legal framework (centering on general principles with regard to rights, conditions and restrictions on access under the legal framework in which the institution operates, as well as provisions contained in specific laws on privacy, information security, the right of access, and archives); an analysis of the institution's activities; and an assessment of the risks arising from access and use of documents and systems.
- 2.** The process may be carried out as a standalone review or as part of the analysis and appraisal processes, whether in advance, during the creation phase, or on accumulated funds.
- 3.** It is recommended that structured forms be used, so that the data to be analyzed are gathered in a standardized way.
- 4.** If possible, the contents of the analysis on legal and regulatory access to document series should be disseminated for the information of the professional community and potential users.
- 5.** It is also considered good practice for those communities to establish communication and participation mechanisms, either during the execution or validation of this process, or after the fact, for review. Such mechanisms can be either formal (e.g., through appraisal committees) or informal (web-based public forums).
- 6.** It is considered good practice to develop access and security charts or tables. An access and security table is a formal instrument for identifying rights of access and the restrictions regime that applies to documents. The table amounts to a classification of document categories according to their access restrictions and security conditions.
- 7.** The results of the analysis may also be included in other system instruments, such as series analysis and appraisal studies (especially when the accessibility analysis is done in tandem with that process), retention calendars (which would, thus, be understood as

retention and access calendars), and archival description systems. In that connection, international archival description standards contemplate elements designed for reporting on the accessibility of archived documents and their groupings.

8. Both the list of different protection categories and the measures associated with them are dynamic elements that vary as factors of how they are regarded socially, legal and regulatory changes, advances in their definition by legal doctrine, administrative precedents, and case law. Through continuous monitoring of those aspects, the various instruments containing the results of the analysis of legal access and the attendant controls can be updated, thereby ensuring the archive's optimal compliance with statutory obligations and ethical commitments.

9. In certain legal contexts, the analysis will facilitate decisions in administrative proceedings on access to public information by providing the competent authority with necessary decision-making criteria to that end.

10. It is considered good practice to use this analysis to identify and propose improvements in the design of documents, so that they do not incorporate more protection-prone data than is necessary to adequately document the activity or process that they record.

4.3 Management of document access requests

Description of the good practice

The rules governing access to public information and archives will be implemented through regulated procedures. The good practices that we gathered refer to the technical process of managing requests, rather than to the administrative procedure.

Recommendations

1. The institution should provide reference information on its documents—including those subject to any type of restriction—and the procedure for requesting access to them. The document access policy should be publicly disseminated, available to users at all times, and compatible with the laws in force.

2. Direct access, without the need for any kind of procedural formalities, should be provided to documents in series classified as unrestricted on the basis of the accessibility analysis process; it should also be provided to internal users or those legally authorized to access restricted documents. The foregoing is without prejudice to appropriate access and security controls.

3. It is good practice to make standard access request forms available to the public.

4. Users should also be afforded the necessary assistance for filling out requests, in accordance with the contents and formalities required by the applicable rules.

5. When the request concerns documents that are not in the possession of the institution, it should be forwarded to the relevant institution. The obligated entity that received the request should notify the applicant that their request has been forwarded to another obligated entity to handle [Model Law, Art. 25 (2)]. When that is not possible, the user will be offered the necessary guidance to enable them to satisfy their need for information.

6. All requests shall be answered in writing at the earliest opportunity and within legally established time limits, even those that are refused under the laws in force. Responses granting access shall describe the manner and conditions in which said access will be provided. Responses denying access must be supported by the exceptions regime, clearly inform the applicant of the reasons why the volume of material is considered reserved, provide a specific description of the provisions of the Law establishing that reservation, advise them of their right to appeal, and provide them with such other information as that Law may require.

7. It is recommended that a requests log or system, preferably automated, be used to control the necessary workflow for access to public documents, document the processes conducted in handling requests, including the decisions adopted, and offer quantitative data on request management. Such an obligation is consistent with the provisions contained in the Model Law.

8. It is considered good practice to involve document and archive management professionals in decision-making on access. Particularly, in order to advise the authority in charge of making decisions on access about the contents of requested documents and possible grounds for restriction.

9. Where possible, technical reports issued on the accessibility of requested documents should be based on the accessibility analyses of the document series concerned. At a minimum, the report should contain the following:

a. A mention of the data contained in the document or documents that may be subject to protection under current law.

b. Specific conditions for access to those data when they are covered by a statute and objective criteria that might qualify the decision of the competent authority. In particular, attention should be drawn to those cases in which the information subject to protection is manifestly public (because it is legally subject to active disclosure or has become general knowledge by other means) or no longer requires such protection (because the statutory time limits have run or the protected interest has ceased to exist).

c. The possibility of, and proposals for, dissociating information, depersonalizing it, or providing partial access to it without distorting it or rendering it meaningless.

10. Following the dissociation of private data or of data that are otherwise subject to protection, responses to access requests should be published, in particular those that offer criteria for interpreting future requests concerning documents with similar or equivalent contents.

11. Statistics on access to public documents should be published periodically (at least annually). In particular, the following should be disseminated for each specific period:

a. Number of access requests received.

b. Number of access requests answered in a timely/tardy manner.

c. Number of requests with a response pending.

d. Number of requests denied; principal reasons for denial; specific sections of the law invoked for denying information (in whole or in part), frequency of invocation.

e. Appeals lodged against refusals to release information.

f. Application fees charged.

g. Any other information required by law.

4.4 Access restrictions and control

Definition of access restriction

Access restriction is the exclusion of certain information from the general regime on unrestricted access, based on a clear and precise regime of legally established exceptions to protect public and private interests (national security, privacy, etc.) Under such laws, access to documents containing information subject to restriction is limited—usually for a specific period of time—to certain authorized persons, except where partial access may be offered.

Description of the good practice

It is considered good practice, in relation to document and archive management systems, for public institutions to implement the necessary security measures and access controls to prevent, in accordance with the rights and legal restrictions in force, unauthorized access to confidential information. That includes the necessary measures to provide, where possible, partial access to documents or to conceal certain data, and to inform users of that circumstance when the law so requires.

Recommendations

1. The security measures and controls on document access should be established in accordance with the law, applicable technology, and, in particular, the institution's information security policy.
2. One of the main access control instruments recommended is a user permissions register: The register categorizes users according to their access rights: Its development consists of:
 - a. Identifying the access needs of the institution's various operational areas.
 - b. Identifying different user profiles.
 - c. Identifying users with access to specific document groups.
 - d. Assigning user profiles to both internal and external users
3. Controlling access to documents consists of applying to each document the access conditions appropriate to their class, as defined in the access and security table. It also consists of allowing each user to access and use documents according to those conditions and the permissions assigned to them in the user permissions register.

4. All document and archive management system users must show some kind of identification and provide certain minimum personal and contact data in order to access documents. Where access relates to restricted documents, other types of credential sufficient to demonstrate access clearance may be required.

5. The necessary measures should be established to control physical access to premises where documents—particularly restricted ones—or the equipment and systems used to store them are located, in order to prevent unauthorized entry.

a. In the case of documents on traditional media, the above may entail placing restricted documents in locations separate from the rest of the storage area or even in special security furniture.

b. Electronic documents may require the installation of security firewalls and separate physical storage devices or spaces.

6. The implementation of document tracing mechanisms is recommended; i.e., a system to monitor their access, use, or handling through the creation, incorporation, and conservation of information on such processes.

a. The institution should keep a document access log, especially for restricted documents.

b. In electronic information systems, that entails introducing audit trails to record users' activities in connection with documents and/or the management system itself.

7. The necessary mechanisms should be set up to allow partial access to documents or conceal certain data, with users advised in advance of that fact. The following procedures may be used:

a. Data masking: This consists of generating a copy of a document on which confidential or restricted data have been concealed.

b. Depersonalization or anonymization: This consists of producing of a new version of a document in which data that would allow certain persons to be identified have been concealed.

c. Partial access to files: The withdrawal or temporary concealment of certain restricted documents in order to permit access to the rest, with the user informed of the documents that have been excluded; the specific reasons for their exclusion; a reasonable estimate of the volume of material that is confidential; the specific legal provisions supporting that confidentiality, and any other information required by law.

4.5 Minimum security measures for documents containing personal data

Definition of personal data

Personal data means any numeric, alphabetic, graphic, photographic, acoustic or any kind of data or information relating to an identified or identifiable natural person, whose identity can be determined by an identification number or one or more factors specific to the physical, physiological, mental, economic, cultural, or social identity of that natural person.

Description of the good practice

It is considered good practice for public institutions to implement measures to prevent disclosure of sensitive personal data, as well as to take steps to avert security risks. In that connection, public authorities should adopt measures to protect the security of personal data and prevent their unauthorized alteration, loss, transmission, or access.

Recommendations

- 1.** The archiving of media or documents should be done in such a way as to ensure the correct conservation of documents, the location and consultation of information, and the exercise of the right of access.
- 2.** Obligated entities should assign one or more security officers responsibility for coordinating and controlling the application of security measures.
- 3.** Concerning personnel duties and obligations:
 - a.** The duties and obligations of each user or user profile with access to such files is clearly defined and documented by the institution, with reasoned cause provided for their need to access those documents.
 - b.** The security officer should adopt the necessary measures so that staff can easily familiarize themselves with the security rules that apply to the performance of their duties, as well as the consequences to which they could be liable in the event of a breach.
- 4.** Concerning the copying or reproduction of documents containing personal data:
 - a.** The copying or reproduction of documents containing personal data should only be done under the supervision of personnel authorized by the security officer.
 - b.** All discarded copies or reproductions should be securely destroyed to prevent access to the information they contain or its subsequent recovery.
 - c.** In the case of documents containing personal data on electronic media, a backup copy of the data and the procedures for their recovery should be kept at a different location

to that of the computers used to process them, and in all cases the security measures guaranteeing the integrity and recovery of the information should be complied with.

5. Concerning access to documentation:

a. Access to documentation should be limited to exclusively to authorized personnel.

b. Each authorized person who requests access to documentation containing personal data should be correctly identified.

c. A user register should be established that logs their access and identifies which authorized person has accessed documentation containing personal data, and on what date.

d. If the loan of documentation is requested, the date set for the documentation's return should be logged. Once the return date is reached, the officer designated for that purpose should require the user to return it and make a record of any incident in the access log.

e. Only duly authorized personnel should be able to grant, alter, or void authorized access to resources, and should do so in accordance with the criteria established by the institution.

f. Personnel from outside the institution who access resources should be subject to the same security conditions and obligations as the institution's personnel.

6. Procedures should be implemented to ensure the integrity of documentation by means of a document index or sequential numbering of its pages.

7. A security document should be drawn up that sets out measures, standards, and procedures of conduct

8. Concerning management of the security document:

a. The security officer should draw up a security document that sets out mandatory technical and organizational measures for all personnel with access to information containing personal data.

b. At a minimum, the document should contain the following:

- Scope of application, specifying in detail the protected resources
- Measures, standards, and procedures of conduct, as well as rules for ensuring security
- Staff duties and obligations in relation to document access
- Description of the information access procedure
- Description of information systems, as appropriate
- Incident notification, management, and response procedure
- Identification of the security officer
- Periodic controls to verify compliance with the document's provisions

c. When data are processed on behalf of third parties, the security document should identify the processing carried out and include an express reference to the contract or document governing the conditions of the commission, the identity of the person responsible, and the duration of the commission.

d. The security document should be kept current at all times and be revised whenever there are significant changes in the processing system used. In all cases, a change should be considered significant when it could potentially impact compliance with the security measures in place.

e. The contents of the security document should be kept consistent at all times with the provisions in force on security of personal data security.

f. The various user profiles authorized to access documents containing personal data should be informed, at a minimum, with the security measures that they should apply and with the duties and obligations to which they are subject.

9. In managing **electronic documents containing personal data** and matters relating to computer security, plans should be adopted for dealing with threats and technology changes.

10. Concerning user identification and authentication in relation to electronic documents:

a. The institution, person in charge of information systems containing personal data should adopt appropriate measures to ensure correct user identification and authentication.

b. The institution should establish a mechanism that unequivocally and individually identifies all users who attempt to access the information system and verifies their clearance.

c. For password-based authentication mechanisms, there should be an assignment, distribution, and storage procedure that ensures password confidentiality and integrity.

Passwords should be changed at regular, set intervals and, while valid, should be stored in an unintelligible form.

d. The institution should establish a mechanism that limits the number of repeated unsuccessful attempts to access the information system.

11. Data transmission involving documentation containing personal data over public or wireless electronic communication networks should be done using encryption or another mechanism that ensures that the information is not intelligible and cannot be manipulated by third parties.

4.6 Exercise of the rights of access, rectification, cancellation, and objection of personal data

Definition of ARCO rights

The so-called ARCO rights (access, rectification, cancellation, objection) are the measures that physical persons can take to exercise control over their personal data.

Description of the good practice

Given the existence of documents containing people's sensitive personal data and the right to have one's confidentiality respected, institutions are responsible for adopting suitable procedures for receiving and responding to requests for access, rectification, and cancellation of personal data, as well as for seeking to ensure that such data are accurate and up-to-date.

In such situations, the owners of personal data or their accredited representatives are entitled to request institutions for the information contained in documents about them, be informed about the purpose for which that information has been gathered, directly consult the documents containing their data, and demand the rectification, update, nondisclosure, or cancellation of the information that concerns them.

Recommendations

1. Concerning management of the right to information:

a. Users from whom personal data are requested for inclusion in their files should be expressly advised in advance of the following in a precise and unambiguous way:

- The existence of processing of personal data, the purpose for gathering those data, and the recipients of the information.
- If their responses to the questions they are asked are compulsory or optional.
- The consequences of obtaining the data or of the refusal to supply them.
- The possibility of exercising the rights of access, rectification, and cancellation.¹
- The identity and address of the person responsible for processing the data, or of their representative, as applicable.

b. The information referred to in the section above should be included in a clearly legible way in questionnaires and other forms used to gather personal data.

2. Concerning management of the right of access to one's own files:

a. In this context, the right of access means the right of users to obtain information about whether their personal data are being processed, which entitles the applicant to directly consult the documents contained in their files or to be given a copy of the totality of such files or part thereof.

b. The cost of reproduction and copying the requested documents shall be borne by the applicant, in accordance with the law.

c. If magnetic or electronic copies can be made available and the interested party provides a storage medium for the information, reproduction should be free of charge.

¹ It was considered appropriate in the context of this draft model law not to mention the right of objection, as it does not arise in the context of public administrations.

d. Under the right of access, the user is entitled to obtain from the person responsible for processing information about specific data or about the entirety of their data submitted for processing.

3. Concerning the right to rectification of personal data:

a. The right to rectification entitles the user to have any inaccurate or incomplete data in their files changed.

b. The rectification request should state which data is to be rectified and how it is to be corrected, and should be accompanied by documentation justifying the request.

4. Concerning the right to cancellation of personal data:

a. The right to cancellation is the right to erasure of any inappropriate or excessive data.

b. The cancellation request should state which data is to be canceled and be accompanied by documentation justifying the request, as appropriate.

c. Decisions on data cancellation requests are taken by the staff who enter the data in the files.

5. The rights of access, rectification, and cancellation are personal and exercised by the bearers of those rights or their representatives; in the case of the latter, their status as such must be accredited.

6. If, when invoking the right with the institution, the user receives no reply, they may resort to the internal and external appeal procedures provided by law.

4.7 Information security

Definition of information security

Information security is the preservation of the confidentiality, integrity, and availability of information, which may also involve other properties, such as authenticity, traceability, non-repudiation, and reliability.

Description of the good practice

It is considered good practice in the context of electronic administration to create the necessary conditions for confidence in the use of electronic media by means of measures to ensure the security of systems, data, communications, and electronic services, so that persons and public administrations can exercise rights and fulfill duties through those media.

In this context, network and information security means the capacity of networks or information systems to withstand, with a degree of confidence, any accidents or illicit or ill-intentioned acts that might compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted data and of the services that those networks and systems offer or provide access to.

Security measures should be proportional to the importance and category of the information system to be protected.

Security measures can be divided into three groups:

- **Organizational framework:** The array of measures relating to the security structure overall.
- **Operational framework:** The measures that protect the operation of the system as an integral group of components with a specific purpose.

- **Protection measures:** The protections for specific assets, consistent with their nature and the quality required of the level of security of the aspects concerned.

Recommendations

- 1.** Legal and technical standards should be adopted so that people and public administrations can feel security and confidence in their electronic interactions.
- 2.** Confidence should be based on the fact that information systems will provide services and protect information in accordance with their functional specifications, without uncontrolled modifications or interruptions, or information falling into the hands of unauthorized persons.
- 3.** Information security should be managed within the administration, and the security of externally accessible resources and information assets should be maintained.
- 4.** All staff accessing assets should:
 - a.** Know and accept their responsibility with respect to security.
 - b.** Have the proper training in relation to matters of security and responsibility.
 - c.** Maintain professional secrecy, not divulge restricted information, and respect confidentiality.
 - d.** Promptly report any weakness in the system through formal channels.
- 5.** Assets must be protected, as must infrastructure, by means of access control mechanisms and protection against external contingencies.

6. Information should be protected against unwanted modifications by means of mechanisms to ensure its integrity.
7. A plan of action should be developed to minimize the effects of a catastrophe, in order to protect the integrity, availability, and preservation of information.
8. The risks and impacts associated with the absence of continuity of information systems should be evaluated, regulations on security standards adhered to, and audits performed.
9. Infrastructure should be used in a secure manner, with its status monitored and any incidents reported; routines should be established for monitoring registration of incidents and failures.
10. Any system should consider the security requirements of documents for their entire lifespan.
11. A continuous improvement process should be established for incident management.

4.8 Reuse of information

Definition of reuse of public information

Reuse of public information means the use by third parties (natural or legal persons) of public information for commercial ends or otherwise, where such use is not an administrative activity.

Description of the good practice

The reuse of public information is the use by natural or legal persons of information generated by public-sector agencies or in their custody for purposes other than those originally intended, whether for profit or not.

The reuse of such information offers significant economic potential and added value, as it facilitates the development and creation of new products, services, and markets. The reuse of public information can be done by administrations other than the ones that generated the information or by individuals and enterprises. Furthermore, by making public information available, public administrations increase administrative transparency, strengthen democratic values and the right to information, and enable citizen participation in public policies.

Recommendations

1. Create a consistent legal framework with an objective and subjective sphere of application, as well as all the rules of development that may be necessary to enable public information to be reused and made available to any natural or legal person, whether private or public.
2. Harmonize the provisions of public administrations on the reuse of information with the general regulatory framework on access to information.
3. Limit the sphere of application by listing those public documents or categories of documents that are not subject to reuse (e.g., documents and information that affect the security of the State, documents protected by copyright or industrial property rights, etc.) in accordance with the exceptions regime in force.
4. Where documents subject to intellectual property rights are authorized for reuse, verify that the necessary license has been granted and that sufficient exploitation rights are assigned by the rights holders.
5. Design a reuse regime that guarantees full observance of the principles that enshrine protection of personal data as a fundamental human right. Where possible, consider the dissociation or removal of personal data that could affect the rights of third parties, provided that that is technically and economically feasible.

6. The conditions for reuse must be clear, just, transparent, and nondiscriminatory, as well as consistent with the principles of free competition and public service.

7. It would be advisable to include in the conditions for reuse such aspects as the guarantee that documents will not be altered or their information falsified or distorted, that the source be stated, etc.

8. Conform to standards and good practice on competition by limiting exclusive agreements as much as possible, reserving them for very specific cases and exceptions.

9. Consider and design specific reuse strategies for documents and information kept in archives, libraries, museums, and other cultural centers.

10. Encourage documents to be made available electronically, such as on websites, thereby stimulating the growth of the information and knowledge society.

11. Promote the use of data, open formats and pertinent metadata associated with documents, and harmonize the provisions on reuse of public information with electronic administration processes.

Conservation and Contingency Management

5.1	Preparation of an integrated document conservation plan	69
5.2	Custody and control of facilities	71
5.3	Environmental control	74
5.4	Preparation of a contingency management plan	76
5.5	Risk assessment	78

This section examines good practice relating to the processes included in an institutional conservation and contingency management plan.

5.1 Preparation of an integrated document conservation plan

Definition of plan

A plan is a systematic model of action prepared in advance for directing or steering an institution's policy.

Definition of conservation

Conservation is the array of processes and measures designed, on one hand, to preserve documents or prevent their possible physical alteration, and on the other, to restore those that have been altered.

Description of the good practice

The integrated conservation plan covers three closely related aspects: document safekeeping and control programming, authorization and inspection of storage areas, and their location and construction.

Document preservation should be a part of every integral objective of any institution and, therefore, of its overall strategy.

Recommendations

1. The institution should have in place a conservation plan that offers continuity and coherence over time.
2. All preventive conservation decisions adopted by the organization as part of its document management should be documented, duly reasoned, and subsequently disseminated.
3. The institution should evaluate its needs by conducting studies on the state of conservation of its fonds and on the environmental situation of the facilities that will underpin the conservation plan.
4. In general, the institution should give priority to implementing preventive measures as a safeguard against the need for repairs.
5. Studies on the state of conservation of the institution conducted by expert staff should cover the environment, storage, security, access, maintenance, conservation treatments, and conservation practices and policies.

6. The institution should establish priorities with regard to preventive actions to be implemented based on criteria as to impact, feasibility, and urgency. To that end, it will be necessary to have an officer in charge of implementing the conservation plan, who should appear in the organization chart and be known throughout the institution.

7. Implementing preventive conservation is something that concerns everyone and every activity in the institution. The active engagement of all the institution's staff through their awareness of the duties that they are required to perform in line with their training and functions is vital.

8. With respect to management and safekeeping of electronic documents, the institution's conservation plan should include the necessary measures to ensure the integrity, accessibility, confidentiality, authenticity, reliability, and identity of documents. Those measures should be designed in partnership with an interdisciplinary team composed of information technology specialists, document managers, and archivists.

5.2 Custody and control of facilities

Definition of custody

Custody is the legal responsibility that requires the archival institution to control and adequately conserve fonds, regardless of their ownership.

Description of the good practice

It is considered good practice in the area of document management for the institution to take responsibility for seeing to the conservation of its document fonds, as an indispensable requirement both for preserving the institutional memory and

for the availability of useful instruments for decision-making on its business.

Recommendations

1. The institution should give close attention to the necessary technical and environmental conditions for housing its document fonds as a prerequisite for the choice or construction of the building where it will reside. Accordingly, it should be aware about aspects such as pollution, particularly in urban environments, given the high concentration of combustion particulates and pollutant gases. Other factors to consider when evaluating the risks to which the material might be exposed will be the proximity of water or gas conduits, as well as fuel storage facilities.

2. The institution should ensure that the architects or engineers involved in the construction of the building that will be used as an archive for its fonds have precise technical knowledge of the needs involved.

3. The section on the center's services and installations should examine the characteristics and state of water, gas, and electricity conduits, artificial lighting, ventilation system, heating, alarms, and fire detection and extinguishing systems. Identification, age, and compliance with technical norms are essential. Particular attention should be given to the following:

- a.** Water and electricity conduits that pass through archive storage areas.
- b.** The existence of filters in ventilation systems.
- c.** Regulation of the relative humidity and temperature system.
- d.** Renewal or recycling of contaminated air.
- e.** Detection of possible points of entry of contaminated air.
- f.** The state and functioning of burglar alarms.

4. The archive document storage areas should:

- a.** Be equipped with security systems.
- b.** Be at a safe distance from the building's mechanical rooms and from any electrical installations or water pipes that pass through them.
- c.** Have protected windows to protect against the harmful effects of sunlight on documents.
- d.** Be fitted with a fire detection and alarm system and other protective equipment.
- e.** Be permanently ventilated to reduce relative humidity and temperature fluctuations.

5. The institution should contribute to the better preservation of the fonds in its keeping by ensuring that it selects adequate archive furnishings. To that end:

- a.** Wooden bookcases and shelves that can support less weight, are more combustible, and are more vulnerable to biological hazards. Noncombustible aluminum or steel fittings without backs and with smooth, non-abrasive surfaces and rounded edges to avoid damage to documents are preferable.
- b.** Shelves should be installed away from walls, short of the ceiling, and have the bottom shelf away from the floor. This will allow air to circulate, limit the effects of humidity, and facilitate cleaning.
- c.** Passageways between shelves should have sufficient separation between units to permit easy access and work.

6. Poor quality storage boxes and folders can adversely impact the security of the objects that they are supposed to protect. Therefore, the institution should ensure that the chemical composition of those elements is appropriate, thereby contributing to the longevity of the fonds in its keeping.

7. The institution should have an adequate solution for the problem of preserving photographic, audiovisual, and large-format documents by using appropriate furniture (horizontal or special) and containers (special boxes, cases, or encapsulation).

8. Institutions that have electronic documents in that keeping should design an electronic document management policy that is applied from the moment the document enters the system and extends throughout its life span by:

- a.** Creating electronic repositories.
- b.** Analyzing the risks that affect the correct conservation of electronic documents: obsolescence, system failures, lack of backup copies, data corruption, or unauthorized access.
- c.** Drawing up contingency plans to ensure the integrity, accessibility, confidentiality, authenticity, reliability, and identity of documents. Where appropriate, corrective measures should also be planned, such as making authentic electronic copies with a change of format.
- d.** Implementing conservation mechanisms with applications that contemplate issues relating to backup copies, replication systems, and information protection systems.

5.3 Environmental control

Definition of environmental control

In the area of document management, environmental control means inspection, monitoring, and implementation of the necessary measures to reduce or prevent the deterioration of document fonds.

Description of the good practice

Evaluating environmental parameters by means of measurement and analysis tools followed by their comparison with the recommended appropriate values will determine whether or not measures are needed.

Recommendations

- 1.** Regularly recording temperature and relative humidity should ensure the absence of fluctuations in readings. Accordingly, installing adequate climate control systems capable of maintaining standard conservation norms will considerably retard the deterioration of fonds.
- 2.** The institution must protect its fonds against possible damage resulting from improper exposure to light intensity, in accordance with standard conservation norms.
- 3.** The institution must protect its fonds against possible adverse effects by contaminants in the form of gases or particles; therefore, it should ensure air quality control in its archive storage areas.
- 4.** The institution should consider comprehensive pest control, which consists of using non-chemical means (climate control, food sources, and building entry points) as an overall strategy against infestation.
- 5.** Chemical treatments should only be used in crisis situations that threaten rapid damage or when insects cannot be eradicated by more conservative methods.
- 6.** The institution should consider that a proper archive and appropriate handling is a practical and economic way of extending the life of the fonds in its keeping.
- 7.** Cleaning procedures should be consistent with conservation standards and appropriate handling techniques, which the institution should disseminate among its cleaning staff.

8. Cleaning should be done regularly and at a frequency determined by how quickly dust and grime build up in storage areas.

5.4 Preparation of a contingency management plan

Definition of a contingency plan

A contingency plan is an instrument whose purpose is to correct deficiencies, take effective action in preventing disasters, and define goals, risks, and those with responsibilities.

Description of the good practice

Designing a plan for managing contingencies at archives is a priority recommendation for the adequate preservation and protection of repositories. Although losses are often unavoidable, their consequences can be reduced by having in place a plan that attenuates risks and the damage caused to documents.

Recommendations

1. A contingency management plan can be divided into three parts:

- a.** Planning: Defining objectives, needs, and resources in order to establish protocols that are set down in a document.
- b.** Protection: Using all available resources to prevent or minimize the impact.
- c.** Response and recovery: Protocols designed to save the fonds from the disaster.

2. Setting responsibilities and their adoption by the organization are essential for establishing a contingency management plan. The distribution of responsibilities establishes who is responsible for planning and who is supposed to do the work of salvage and evacuation.

3. Appointing a contingency committee serves to bring together specialists from different disciplines (building maintenance, safety experts, insurance adjusters, etc.). It performs an advisory role and is responsible for implementing the plan, corrective and priority measures, and action protocols.

4. The contingency team is the one that acts, reports, and evaluates situations in the event of risks.

5. The salvage brigade intervenes to evacuate document fonds affected by a loss, but always after the safety experts have ensured the environmental stability of the building affected.

6. Everyone involved in the plan should attend training courses on document handling and rescue.

7. The contingency management plan should contain the following information:

- a.** The building plans, with information about essential documents, extinguishers, and evacuation routes.
- b.** Chains of communication to be activated in emergencies, which should be kept current (companies, experts, etc.).
- c.** Staff instructions, with basic actions to carry out specific protocols for the coordinator and teams, and fonds evacuation and relocation procedures.
- d.** Damage assessment and response review forms.
- e.** Insurance policy and information about institutional networks (experts, transportation companies, and suppliers).

5.5 Risk assessment

Definition of risk assessment

A risk assessment is the process of comparing the estimated risk with a preset criterion for determining its magnitude. The risk is expressed in terms that combine the probability with the consequences of an unwanted event.

Description of the good practice

A risk assessment should be done before action protocols are developed, since it provides information about the institution's real needs. Studying those needs will yield knowledge about protection strengths and weaknesses, thus enabling actual risks to be evaluated.

Recommendations

1. Compare the different risk values obtained in order to have an instrument that enables the institution to determine which risks are a priority and, therefore, warrant most attention.
2. Evaluate the institution's risks by studying the following variables:
 - a. Analysis of the region's climate and geological factors.
 - b. The building's location.
 - c. Update the building plans, showing evacuation routes, the electrical system, and water conduits.
 - d. Location of toxic products.

- e. A review of the state of the building, installations, and funds.

3. That information should be materialized in a risk map that shows the probability and seriousness of threats, thereby serving as a guide for establishing and monitoring inspection routines. The risk map must be kept current and enable action priorities to be established.

4. For the purposes of emergency recovery, the institution should be equipped with a prompt initial response, a detailed disaster plan, trained personnel, a committed administration, effective communication, and swift and informed decisions.

Awareness Raising and User Assistance Services

6.1	Awareness-raising	81
6.2	Assistance to the administration by archive services	83
6.3	Public assistance	85

This section deals with good practices relating to the services that the Archive provides, which should be aligned with the institution's established information policy.

6.1 Awareness-raising

Definition of awareness-raising

Awareness-raising is the process that seeks to promote the use of documents produced or received by institutions, enabling closer relations with users and enhancing their recognition, presence, and credibility as administrative and cultural management units.

Description of the good practice

It is considered good practice for an archive service to raise awareness about its contents: its document funds, document-produc-

ing institutions and, in general, the information contained in the documents.

The purpose of awareness-raising is to inform people and society at large about the transcendental importance of archives, their usefulness, and the services that they provide for the benefit of the community.

Recommendations

1. Involve other professionals, such as educators, graphic designers, teachers, communicators, artists, and IT experts, among others.
2. The educational potential of archives should be leveraged, given the social and cultural benefits.
3. It is essential to have an area and personnel that specialize in awareness-raising.
4. Develop an awareness campaign, the goals and mission of which are defined in line with the institution's established information policy.
5. Identify the types of users that the campaign will mainly target. An awareness campaign can target any kind of user; however, awareness-raising can be directed at specific spheres, such as schools or universities.
6. Select and prepare the collections, exhibits, or documents, as appropriate, that will be used in the awareness campaign.
7. Awareness-raising can take various forms, from broad-spectrum activities that require significant spending and resources, to low-cost, simple actions. Some of those activities are:
 - a. Exhibits—either virtual or physical
 - Virtual exhibits are designed to be accessed over the Internet (on the archive's website) or via digital media (CD or DVD).

- Physical exhibits can be permanent, temporary, or touring.
 - b. Guided tours, both on-site and virtual (on the archive's website).
 - c. Publications: Archive guide, inventories, catalogs, classification charts, studies, campaigns, thematic guides, etc.
 - d. Creation of a profile or page on a social media platform.
 - e. Creation of a graphic documentation account: graphic content on Flickr, Photobucket, and the like.
 - f. Creation of a video channel: uploads of self-produced videos or selections of third-party videos to sites like YouTube or Vimeo.
 - g. Other awareness measures include educational services, videos, open-days, pamphlets, newsletters, competitions, and historic tourism, among others.
8. Gather statistics on numbers of visits and user satisfaction, as well as other data that could provide important information for the campaign's validation and adaptation (number of followers on social media, media impact, number of posts, etc.).

6.2 Assistance to the administration by archive services

Definition of assistance to the administration

Assistance to the administration means the service that an institution provides to internal users in order to meet their needs through the activities that it performs.

Description of the good practice

It is considered good practice for an archive to provide comprehensive assistance to the line offices of its institution as a basic part of its regular functions.

The assistance provided to a line organization may be regarded as one of the basic processes connected with the services that an archive offers its internal users, in which internal users are defined as the various units that make up the institution to which the archive belongs, as the area in charge of the safekeeping of its documents.

Recommendations

1. The archive should keep permanently available for the administration the documents that the latter has generated and transferred to it; it should also answer any queries on background that the administration may pose.

2. If possible, the archive should provide various types of services to the document-producing institution:

- a.** Design and follow-up of document management plans.
- b.** Document management training for the institution's staff.
- c.** Assistance to the institution in daily document management.
- d.** Document transfers to the archive from various administrative units.
- e.** Management of administrative loans of documents in the archive's keeping.

3. Consultation and loan processes by the document producing administration should be regulated procedures.

4. To avoid any serious incidents or problems with administrative loans and the attendant responsibility changes, it is advisable that the following recommendations be implemented:

a. Every administrative loan should be accompanied by a specific delivery list indicating the documents that are on temporary loan and who the person responsible for their safekeeping will be outside of the archive.

b. Administrative loans should be the direct responsibility of a person in the administrative unit that requests the loan. The name of that person should be recorded on the delivery list for the loan and they will be the point of contact in the event of any incident.

c. To avoid the bad practice of incorporating loaned documents in new administrative processes, consideration should be given to the volume of administrative loans at the time of appraisal and planning of the calendars for transfers from administrative units to the archive. The fewer the administrative loans, the more effective transfers can be.

d. Mechanisms for effective control of access and security levels should be applied to administrative units in order to distinguish which administrative units may access the various documents in safekeeping, in accordance with their level of access.

6.3 Public assistance

Definition of public assistance

Public assistance means the service that an institution provides to external users in order to meet their needs through the activities that it performs.

Description

It is considered good practice for the archives of public institutions to have in place an assistance area to act as intermediary between, on one hand, users and, on the other, documents and archival information, whether on-site or, in particular, virtual.

Among the main functions of archives are to inform society about the documentary heritage held on their premises and facilitate access to them by persons outside the institution, in line with the criteria in place for access to such documents.

Hence the need for any archive, whatever type it may be, to have a public assistance area that can coordinate the activities that the archive needs to carry out for:

- Addressing requests for archival information
- Providing access to documents
- Document reproduction

Recommendations

1. The range of public assistance services offered by the archive, as well as the rules and conditions for their access and use should be available in writing and disseminated as widely as possible, in particular via the institution's website.

2. The array of services should be presented in menu form and include a series of commitments to quality of service provision, indicators for evaluating their fulfillment, and a mechanism for users to register complaints and suggestions. The services menu should also be available in writing and disseminated as widely as possible, in particular via the institution's website and at the archive consulting room.

3. It is appropriate to establish a multichannel service for attending to archival information requests: in person, by telephone, by mail (postal or electronic), or via web-based services (instant messaging, CRM system forms, etc.).

a. Deferred assistance to requests (by mail or online forms) will be subject to appropriate lead times clearly indicated on the services menu.

b. Queries submitted in person, by telephone, or via instant messaging services should be answered immediately, where feasible, with as long a schedule as possible for that purpose, the times for which should be publicly advertised.

c. If possible, archival information requests should be centrally managed and the following types of data recorded: requester's personal and contact details; query data (date and manner, archivist responsible, response date); data about the subject (topic or matter, document groupings referenced); and the content of the response to the request.

4. Other forms of interaction with users should be established, particularly through institutional profiles on social media platforms.

5. As much access as possible should be provided, both via computer and directly, to copies or electronically distributed versions of documents not subject to any legal or regulatory restrictions, in the form of digital objects available on the institution's website, where possible, through archival description systems or any other systems that allow information to be retrieved via search functions; in addition, the information should be provided in context.

6. On-site access to documents should occur on suitable premises, by the appropriate means, and with sufficient technical and administrative staff, following registration of the user and notification to them of the rules in force.

7. The archive should have a reading room with enough places for potential on-site users. It is recommended that the reading room be equipped with the following elements, in particular:

a. Tables and adequate lighting for reading.

b. Devices for consulting original documents or copies (book rests, microfilm readers, computers, etc.).

c. Points of access to archival description systems (inventories and traditional description instruments in hard copy, computers with access to electronic information systems).

d. A reference library: encyclopedias and reference works, legislation catalogues.

e. Sufficient electrical outlets at reading places to power electronic devices (laptop computers, tablets, smart phones, etc.).

f. Shelves to store archival units, with separate spaces for those that have not yet been consulted or that have been reserved for an agreed space of time, and for those that have already been consulted and can be returned to the storage area by archive staff.

8. Access to the reading room and the documents themselves should be in accordance with a set of written rules disseminated as widely as possible and notified to users. Printed copies of the rules should be visibly available at strategic places in the room.

9. Users should have access at all times to assistance from technical staff, who, in particular, will:

a. Provide information about the services offered by the archive, the rules and conditions governing correct access and use of documents, the use of description instruments and systems, copy requests, and other services provided by the archive.

b. Conduct reference interviews so that the technician can interpret the user's information needs and offer them the necessary resources to satisfy them.

c. Manage document access requests.

d. Participate in instruction activities for users.

e. Receive and process complaints and suggestions in relation to the service.

10. The archive should have the necessary staff and means to provide a document reproduction service in accordance with a set of written rules disseminated as widely as possible.

Electronic Administration

7.1 Interoperability	91
7.2 Metadata	93
7.3 Document digitization	95

This section examines good practice relating to the processes required to ensure adequate management in the context of electronic administration.

7.1 Interoperability

Definition of interoperability

The capacity of ITC systems and of the business processes they support to exchange data and enable the exchange of information and knowledge.

Description of the good practice

It is considered good practice in the context of electronic administration to incorporate the concept of interoperability as

a requirement to enable information systems and supported processes to share data and allow exchange of information and knowledge among them. This encompasses:

- **Technical interoperability**, which has to do with the interconnection of computers through the agreement on standards in order to present, gather, exchange, process, and transport data;
- **Semantic interoperability**, which seeks to ensure that the data being transported mean the same to connected systems;
- **Organizational interoperability**, which seeks to organize the business processes and the institution's internal structure for better data exchange.

Recommendations

1. The institution should have an interoperability policy that registers the following basic principles: overall quality, multidimensional nature, and a multilateral solutions approach.

2. Interoperability is defined as multilateral because of the need to share, reuse, and collaborate. The degree of cooperation will determine the success of initiatives.

3. Interoperability should have a threefold dimension: organizational, semantic, and technical. There is also a fourth dimension, the temporal, which requires the institution to guarantee access to information throughout the lifespan of electronic documents.

4. Organizational interoperability encourages institutions to:

- a.** Establish and publicize the conditions of access and use for the services provided in their electronic administration.
- b.** Simplify their organizational complexity.
- c.** Publicly update their administrative processes and services.

d. Publicize and update their organizational structure, in particular indicating their registry and points of public assistance.

5. Semantic interoperability requires the development and implementation of a data exchange model to be used for exchanging information.

6. Technical interoperability requires institutions to:

a. Use open standards and make complementary use of standards that are in general public use.

b. Be technologically neutral, ensuring a free choice of alternatives for people and avoiding any kind of technological discrimination.

c. Publish a list of the open and complementary standards accepted to facilitate interoperability.

d. Seek to link their infrastructure with that of other institutions, in order to facilitate service and information interoperability.

7.2 Metadata

Definition of metadata

In the area of document management, metadata means the data that describe the context, content, and structure of documents and their management over time.

Description of the good practice

It is considered good practice in the context of electronic administration to have adequate metadata implementation as necessary contextual information of electronic documents and files.

Recommendations

1. Institutions should ensure the availability and integrity of the metadata of their electronic documents.
2. Metadata implementation in electrical documents and files should:
 - a. Ensure the registration of documents' correct contextual information.
 - b. Help with the location and retrieval of documents through the use of controlled vocabularies, value systems, and other standardized descriptive systems.
 - c. Improve dissemination of information.
 - d. Control access to documents.
 - e. Enable document access or transfer between institutions.
 - f. Enable execution of instructed actions on documents.
 - g. Ensure conservation of key documents.
 - h. Ensure preservation of information over time.
 - i. Standardize descriptions.
 - j. Help with data migration planning and other conservation needs.
 - k. Provide a benchmark for assessing document management quality.
 - l. Effectively integrate information about electronic documents in intellectual control systems.
 - m. Ultimately, ensure interoperability.

3. Electronic document management metadata should be articulated in metadata schemes that match the particular characteristics and management needs of each institution. It is advisable to adapt an existing metadata schema so that each institution creates its application profile.
4. The metadata schema and profile should include three categories: mandatory, complementary, and optional metadata.
5. The metadata schema should include precise descriptions of all its elements and sub-elements.
6. The complementary metadata that the institution identifies as necessary for its document management processes should be incorporated in document management software.

7.3 Document digitization

Definition of digitization

Digitization is the technical process that involves the generation and subsequent processing of a digital image from an original document in a non-digital format. The concept of digitization excludes documents originally generated in a digital format.

Description of the good practice

It is considered good practice in the framework of document management to establish minimum requirements for electronic images resulting from digitization by standardizing basic parameters for those processes, ensuring the necessary flexibility for their application by different public administrations, while adhering to the premise of obtaining complete and true electronic images of the original document.

Recommendations

- 1.** The digitization process should be set down in a formal procedure and imparted to the institution staff involved in document production.
- 2.** The digitization process should cover format standardization, quality levels, technical conditions, and the associated metadata.
- 3.** It should be understood that the digital components of an electronic document resulting from a digitization process are the electronic image, the metadata, and the electronic signature, as appropriate.
- 4.** The electronic image obtained through digitization should be true to the original content, ensure its integrity, guarantee the legibility of the electronic image obtained, adhere to the proportions of the source document, and not add any characters that do not appear in the original.
- 5.** Outsourcing the digitization service does not exempt the institution from the responsibility to guarantee the integrity of the result of that process.
- 6.** Metadata registration in a digitization process should include not only the mandatory minimums, but also the necessary complementary metadata that reflect aspects of the digitization process itself.
- 7.** If possible, the effort should be made to automate metadata capture, assuming that the digitization mechanisms allow that to be configured.
- 8.** A necessary part of the digitization process is preventive maintenance and routine checks to ensure the quality of the image and its metadata by developing a continuous quality control program to verify output consistency.

Staff Profiles and Document Management Training

8.1	Staff Responsibilities and Qualifications	99
8.2	Communication plan	101
8.3	Continuing education plan	103

8.1 Staff Responsibilities and Qualifications

Definition of job profile

A job profile is a means of compiling the necessary personnel requirements and qualifications that an employee must have to enable them to perform their duties satisfactorily in an institution: level of education, experience, job functions, instruction and knowledge requirements, as well as the necessary aptitudes and personality characteristics.

Description of the good practice

Institutions should define the responsibilities and competencies of all staff involved in the document management policy. The purpose of defining responsibilities, competencies, and their interactions is to establish and maintain an adequate document management regime that meets the needs of all interested parties, both internal and external. Responsibilities and competencies should be defined based on the institution's standardized practices or rules.

The institution should introduce a continuing education and awareness program in relation to document management. Training in the requirements of document management and its practical application should include all personnel, whether internal or external, who are in charge of all or part of an activity, or involved in the creation, maintenance, and control of documents incorporated in document management systems.

Recommendations

1. Different categories should be established for defining the competencies, responsibilities, duties of all staff involved in document management.
2. The institution's executive management should assume the highest level of responsibility in order to ensure the success of the document management action plan by resourcing the low levels, promoting compliance with document management procedures at all levels of the institution, and consolidating an adequate regulatory framework.
3. It is advisable for the heads of management units or intermediate organizational groupings to be responsible for ensuring that the personnel under their supervision generate and maintain the documents for which they are responsible as an integral part of their work and in accordance with established policies, procedures, and norms.

4. Highly qualified managers, IT technicians, and archive professionals should assume responsibility for planning and implementing at the practical and technical level the necessary procedures and processes for correct document management and for establishing the necessary technical norms for correct administration of the document management policy.

5. Set up multidisciplinary work teams of qualified technicians to plan the document management policy, which will require involving different institution personnel:

- a. With specific obligations in the areas of security, design, and systems relating to information and communication technologies.
- b. With obligations to verify and sanction fulfillment of norms.
- c. To create, receive, and maintain documents as part of their daily work, so that it is done in accordance with established policies, procedures, and norms.

6. If the institution's document management plan is implemented by external contractors, it is important to ensure that they comply with the standards set down in the institution's policies and the law.

8.2 Communication plan

Definition of a communication plan

A communication plan is an instrument that sets out the communication policies, strategies, resources, objectives, and actions, whether internal or external, proposed by an institution.

Description of the good practice

A communication plan should ensure that the procedures and benefits of document and archive management are understood throughout the institution. It should clearly explain the document management guidelines and situate the procedures and processes in a context that enables all the personnel to understand the reasons why document management is necessary.

The communication plan should articulate procedures to ensure that the basic documents associated with the institution's document and archive management policy are accessible to and reach all its members and that they are aware of their importance and significance.

Recommendations

1. The communication plan should be proactive and develop the necessary instruments to make all the personnel aware and engaged in fulfilling document and archive management rules; guidelines, recommendations, good practice guides, etc. are useful to that end.
2. The communication plan may be articulated in synergy with certain aspects of the continuing training plan and use surveys in areas of the institution where fulfillment of established procedures is identified as weak.
3. Specific codes of ethics or of conduct may be developed or adopted for archive and document management technicians, given the importance of their competencies with regard to management and archival processing of documents in the institution.
4. The communication plan could include mechanisms for all members of the work team to provide feedback on the management policy and its implementation, which is especially useful for planning a review and assessment of that policy.

5. Stimulate mindfulness in the institution's employees at all times and encourage them to support and achieve the objectives of the document management policy.

8.3 Continuing education plan

Description of the good practice

It is considered good practice for public institutions to provide training to all staff that take on any kind of responsibility in the area of document management, and to educate both internal and external users about archive services.

Recommendations

1. The institution should determine the level of training needed for its staff to perform the document and archive management processes, and should introduce the necessary education activities to provide that training.
2. It is recommended that a staff education plan be implemented to provide training and refresher courses in knowledge and skills relating to document and archive management.
 - a. The education plan should be approved and managed at the institution's senior management levels and suitably resourced.
 - b. It should clearly explain the document management policies and situate the procedures and processes in a context that enables staff personnel to understand why document management is necessary.
3. Application of the staff education plan should encompass all personnel that take on any kind of responsibility in the area

of document management. Having said that, the activities it envisages should be differentiated in order to be appropriate to specific groups or, in certain cases, individual members of staff. In particular, the activities should target:

- a.** Managers.
- b.** Archive and document management specialists.
- c.** General staff responsible for creating or using documents.
- d.** External services companies, fellowship recipients, and volunteers.

4. It is also recommended to have an education plan for archive users, both internal and external.

- a.** It will be up to the archive's assistance service to provide users with a basic initial education about the correct access and use of documents, the use of description instruments and systems, copy requests, and other services provided by the archive.
- b.** The archive's dissemination activities should include awareness and education about archives.

5. Staff and user education activities should cover awareness of the importance and significance of public archives and document management processes, the responsibilities of the actors involved, and the rights of the public in that regard.

6. Public institutions should promote information literacy campaigns to enhance the abilities of the public with respect to access to archives and public documents. Particularly, in relation to:

- a.** Discovery and use of archival information systems.
- b.** Document access application procedure.

c. Information use.

7. If possible, appropriate educational materials for each type of user should be made publicly available on the institution's website.

8. Give consideration to an internal and/or external education methodology and the instruments that it should include.

9. Provide education programs on document management rules and practices to the institution's staff at all levels and, where appropriate, to contractors and/or staff of other institutions involved in such processes.

10. Use assessment procedures to contrast staff competency levels with the objectives of the education program.

11. Periodically review the efficiency and effectiveness of training programs through outcome reporting to encourage the necessary changes and achieve continuous improvement.

12. Through surveys or interviews, evaluate the level of satisfaction of persons who have participated in education activities.

13. Design mechanisms for staff that have already received training to benefit from the enhancements made to educational activities.

Bibliography and Resources

Chapter 1 Document Management Policy

Bibliography

- CRUZ MUNDET, J. R. 2006. *La gestión de documentos en las organizaciones*. Madrid: Ediciones Pirámide.
- INTERNATIONAL STANDARD ORGANIZATION. 2011a. *ISO 30300:2011. Information and documentation. Management system for records. Fundamentals and vocabulary*.
- INTERNATIONAL STANDARD ORGANIZATION. 2011b. *ISO 30301:2011. Information and documentation. Management system for records. Requirements*.
- INTERNATIONAL STANDARD ORGANIZATION. 2016. *ISO 15489-1:2016. Information and documentation. Records management. Part I: Concepts and principles*.
- INTERNATIONAL STANDARD ORGANIZATION. 2008. *ISO/TR. 2008 26122:2008. Information and documentation. Work process analysis for records*.
- INTERNATIONAL STANDARD ORGANIZATION. 2009. *ISO 23081-2:2009. Information and documentation. Managing metadata for records: Part II: Conceptual and implementation issues*.
- INTERNATIONAL STANDARD ORGANIZATION. 2011a. *ISO 30300:2011. Information and documentation. Management system for records. Fundamentals and vocabulary*.
- INTERNATIONAL STANDARD ORGANIZATION. 2011b. *ISO 30301:2011. Information and documentation. Management system for records. Requirements*.
- INTERNATIONAL STANDARD ORGANIZATION. 2011c. *ISO/TR 23081-3:2011. Information and documentation. Managing metadata for records: Part III: Self-assessment method*.

- INTERNATIONAL STANDARD ORGANIZATION. 2017. *ISO 23081-1:2017. Information and documentation. Records Management processes. Metadata for records: Part I: Principles.*

Resources

- COLOMBIA. ARCHIVO GENERAL DE LA NACIÓN. Programa de Gestión Documental. Disponible en: <http://www.archivo-general.gov.co/transparencia/gestion-informacion-publica/Programa-de-Gestion-Documental-PGD>.
- COLOMBIA. CONTADURÍA GENERAL DE LA NACIÓN. 2013. *Programa de gestión documental de la UAE Contaduría General de la Nación.* Disponible en: <http://www.contaduria.gov.co/wps/wcm/connect/65155c34-4a85-4096-a06a-47b53b6b42e0/GESTION+DOCUMENTAL+VERSI%C3%93N+2.pdf?MOD=AJPERES>
- ECUADOR. PERERO GONZÁLEZ, Ginna Isabel. 2012. *Modelo de un sistema de gestión documental para el manejo de archivos administrativos, dirigido al Gobierno Autónomo Descentralizado Parroquial de José Luis Tamayo, provincia de Santa Elena, año 2013.* La Libertad.

Chapter 2 Document Analysis, Classification, and Description

Bibliography

- BARBADILLO ALONSO, J. Clasificaciones y relaciones funcionales en los documentos de archivos. *Tábula: revista de archivos de Castilla y León*, 13, pp. 95-104.
- BARBADILLO ALONSO, J. 2011. *Las normas de descripción archivística. Qué son y cómo se aplican.* Gijón: Trea.
- BONAL ZAZO, J. L. 2001. *La descripción archivística normalizada. Origen, fundamentos, principios y técnicas.* Gijón: Trea.

- BONAL ZAZO, J. L.; GENERELO LANASPA, J. J.; TRAVESÍ DE DIEGO, C. 2006. *Manual de Descripción Multinivel. Propuesta de adaptación de las normas internacionales de descripción archivística* [en línea]. 2ª ed. Valladolid: Junta de Castilla y León. Disponible en: http://www.aefp.org.es/NS/Documentos/NormasDescriptivas/MDM2_2006.pdf
- COMISIÓN DE NORMAS ESPAÑOLAS DE DESCRIPCIÓN ARCHIVÍSTICA, NEDA-MC. *Modelo conceptual de descripción archivística: entidades, relaciones y atributos*, Madrid, 2017. Disponible en: <https://sede.educacion.gob.es/publiven-ta/d/20886C/19/0>
- COMISIÓN SUPERIOR CALIFICADORA DE DOCUMENTOS ADMINISTRATIVOS, *Cuadro de Clasificación de Funciones Comunes de la Administración General del Estado*, Madrid, 2018. Disponible en: <https://www.mecd.gob.es/dam/jcr:4889f307-13b0-460a-88c4-5f930c4ac204/ultima-version-ccf-20180110.pdf>
- CRUZ MUNDET, J. R. 2005. *Manual de Archivística.* Edición corregida y actualizada. Madrid: Fundación Germán Sánchez Ruipérez.
- CRUZ MUNDET, J. R. 2006. *La Gestión de documentos en las organizaciones.* Madrid: Ediciones Pirámide.
- DELGADO GÓMEZ, Alejandro, "Sistemas de clasificación en múltiples dimensiones: la experiencia del Archivo Municipal de Cartagena", *Innovar o morir. En torno a la clasificación*, Revista Tábula: Revista de Archivos de Castilla y León, 13, 2010, pp. 125-136.
- DELGADO GÓMEZ, A. 2004. *Normalización de la descripción archivística: Introducción a Encoded Archival Description (EAD)* [en línea]. Cartagena: Archivo Municipal; Archivo 3000. Disponible en: http://iibi.unam.mx/archivistica/alejandro_delgado-ead_espanol.pdf
- DÍAZ RODRÍGUEZ, A. La clasificación como proceso de gestión de documentos. En *Tábula: revista de archivos de Castilla y León*, 13, pp. 79-94.
- FOSCARINI, F. 2010. La clasificación de documentos basada en funciones. *Revista Tábula: revista de archivos de Castilla y León*, 13, pp. 41-58.

- FRANCO ESPIÑO, Beatriz; PÉREZ ALCÁZAR, Ricard (coords.). *Modelo de Gestión de Documentos y Administración de Archivos para la Red de Transparencia y Acceso a la Información* [en línea]. RTA, 2014. Disponible en: <http://mgd.redrta.org/>. Con especial atención a G04/O. *Guía de Implementación Operacional: Control intelectual y representación. G04/D01/O. Directrices: Identificación y Clasificación. G04/D02/O. Directrices: Descripción archivística.*
- GÓMEZ, R.; BRIGAS, R. 2005. Normalización y requisitos funcionales de la descripción archivística: una propuesta metodológica. *Scire*, 11, (1), pp. 103-112.
- HEREDIA HERRERA, A. 1991. *Archivística General: Teoría y práctica*. Sevilla: Diputación Provincial de Sevilla.
- HEREDIA HERRERA, A. 2010. Clasificación, Cuadros de Clasificación y e-gestión documental. *Tábula: revista de archivos de Castilla y León*, 13, pp. 139-152.
- HEREDIA HERRERA, A. 2011. *Lenguaje y vocabulario archivísticos. Algo más que un diccionario*. Sevilla: Junta de Andalucía.
- HERNÁNDEZ OLIVERA, L. (ed.). 2008. Ahogados en un mar de siglas. Estándares para la gestión, descripción y acceso a los recursos archivísticos. *Tábula*, 11. [Actas del V Congreso de Archivos de Castilla y León, León, 1-3 de octubre de 2008].
- INTERNATIONAL STANDARD ORGANIZATION. 2016. *ISO 15489-1:2016. Information and documentation. Records management. Part 1: Concepts and principles.*
- LA TORRE, J. L.; MARTÍN-PALOMINO, M. 2000. *Metodología para la identificación y valoración de fondos documentales (Escuela Iberoamericana de Archivos: Experiencias y materiales)*. Madrid: Ministerio de Educación, Cultura y Deporte de España.
- LERESCHE, F. 2008. *Las bibliotecas y los archivos: compartir normas para facilitar el acceso al patrimonio* [en línea]. Traducción de Elena Escolano. En: *Conferencia 74 Congreso General de IFLA: Quebec, 10-14 agosto 2008*. Disponible en: <http://archive.ifla.org/IV/ifla74/papers/156-Leresche-trans-es.pdf>
- PITTI, D. V. 2004. Creator Description. Encoded Archival Context [en línea]. En: TAYLOR, A. G.; TILLET, B. B. (eds.). *Authority Control in Organizing and Accessing Information: Definition and International Experience*. Nueva York: The Haworth Information Press, pp. 201-226. Disponible en: http://eprints.rclis.org/4181/1/pitti_eng.pdf
- RAMÍREZ DELEÓN, J. A. 2011. *Descripción archivística: diseño de instrumentos de descripción*. [en línea]. México: Instituto Federal de Acceso a la Información y Protección de Datos; Archivo General de la Nación. Gestión de Documentos y Administración de Archivos: Colección Cuadernos Metodológicos. Cuaderno 4. Disponible en: <http://inicio.ifai.org.mx/Publicaciones/cuaderno4.pdf>
- VILLASECA REYES, O. 2012a. *Directrices para la organización documental*. Santiago de Chile: Archivo Nacional de Chile. Serie Directrices y Normas Técnicas para la gestión de archivos.
- VILLASECA REYES, O. 2012b. *Directrices para la identificación de fondo documental*. Santiago de Chile: Archivo Nacional de Chile. Serie Directrices y Normas Técnicas para la gestión de archivos.
- VV.AA. 1992. *Actas de las Primeras Jornadas sobre metodología para la identificación y valoración de fondos documentales de las Administraciones Públicas (20-22 de marzo de 1991)*. Madrid: Ministerio de Cultura.

Chapter 3 Document Appraisal, Transfer, and Elimination

Bibliography

- AENOR. UNE-EN 15713: 2010. *Destrucción segura del material confidencial. Código de buenas prácticas*.
- AUSTRALIA. NORTHERN TERRITORY GOVERNMENT. 2010. *Guidelines for the destruction of a public sector organisation's temporary value records (Issued November 2010)*. Disponible en: http://www.nt.gov.au/dcis/info_tech/records_policy_standards/tempo_value_records_disposal.shtml
- AUSTRALIA. STATE RECORDS AUTHORITY OF NEW SOUTH WALES. 2010a. *Guideline 3: Destruction*. Disponible en: <https://www.prov.vic.gov.au/sites/default/files/2016-05/1013g3%20v1.1%20ST%2020130717.pdf>

- AUSTRALIA. STATE RECORDS AUTHORITY OF NEW SOUTH WALES. 2010b. Destruction of Records. Sydney. Disponible en: <https://www.records.nsw.gov.au/recordkeeping/advice/retention-and-disposal/destruction-of-records>
- CANADÁ. UNIVERSITY OF BRITISH COLUMBIA. InterPARES 2 Project. 2010. *Creator Guidelines - Making and Maintaining Digital Materials: Guidelines for Individuals - Guía del Preservador - Preservación de Documentos de Archivos Digitales: Lineamientos Para los Organizaciones*. Traducción al español: Juan Voutssás. Disponible en: [http://www.interpares.org/ip2/display_file.cfm?doc=ip2\(-pub\)guia_del_preservador.pdf](http://www.interpares.org/ip2/display_file.cfm?doc=ip2(-pub)guia_del_preservador.pdf)
- CASELLAS I SERRA. L. E. 2010. *La valoración de documentos electrónicos*. Disponible en: http://iibi.unam.mx/archivistica/valoracion_casellas-barnard.pdf Con resultados del Subgrupo de documentos electrónicos que forma parte del Foro Iberoamericano de Evaluación Documental (FIED).
- CERMENO, L.; RIVAS, E. 2011. Valoración, selección y eliminación. En CRUZ MUNDET, J.R. (Dir.) *Administración de documentos y archivos. Textos documentales*. Madrid: Coordinadora de Asociaciones de Archivos. Disponible en: <http://www.archiveros.net/LIBRO.ARCHIVOS.IBEROAMERICANOS.pdf>
- CHILE. ARCHIVO NACIONAL DE CHILE. 2012. *Instructivo para transferencias de documentos tradicionales al Archivo Nacional de Chile*. Santiago de Chile. Serie Protocolos de Trabajo y Mejores Prácticas para la gestión de archivos
- DORANTES CACIQUE, M.T. 2011. *La valoración documental en el siglo XXI. El principio pro homine en la archivística: valoración documental, valoración de la información y derechos*. México. Disponible en: <http://www.te.gob.mx/documentacion/3seminario/files/t9/dorantes.pdf>
- ESPAÑA. COMISIÓN SUPERIOR CALIFICADORA DE DOCUMENTOS ADMINISTRATIVOS, Recomendaciones para el borrado lógico de documentación electrónica y destrucción física de soportes informáticos de la Administración General del Estado, Madrid, 2017. Disponible en: <http://www.mecd.gob.es/dam/jcr:8a4186d5-73cc-4eb8-b5de-c1272ab8da7c/recomendaciones-destruccion.pdf>
- ESPAÑA. GENERALITAT DE CATALUNYA. 2012. *Metodologia per a l'elaboració de propostes d'avaluació i accés documental*. Aprobado en la reunión de 18 de diciembre de 2012. Disponible en: http://cultura.gencat.cat/web/.content/dgpc/arxius_i_gestio_documental/03_cnaatd/03_Avaluacio_disposicio/avaluacio_i_acces/metodol_dipleg_04.pdf
- ESPAÑA. MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE. 2003. *Criterios generales para la valoración de los documentos de la Administración General del Estado*. (Documento aprobado por la Comisión Superior Calificadora de Documentos Administrativos, en sesión de 27 de noviembre de 2003.) Disponible en: <http://www.mcu.es/archivos/docs/MetodologiaComSup.pdf>
- ESPAÑA. MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO. INTECO. 2011. *Guía sobre almacenamiento y borrado seguro de información*. Disponible en: http://www.inteco.es/guias_estudios/guias/guia_borrado_seguro
- FENOGLIO, N. C. 2010. *Proyecto: Evaluación de documentos en Iberoamérica. Antecedentes y perspectiva*. Disponible en: <http://blogs.ffyh.unc.edu.ar/evaluaciondedocumentos/files/2012/06/Norma-C.-Fenoglio1.pdf>
- FRANCO ESPÍÑO, Beatriz; PÉREZ ALCÁZAR, Ricard (coords.), *Modelo de Gestión de Documentos y Administración de Archivos para la Red de Transparencia y Acceso a la Información* [en línea]. RTA, 2014. Disponible en: <http://mgd.redrta.org/>. Con especial atención a G05/O. *Guía de Implementación Operacional: Valoración; G05/D01/O. Directrices: Instrumentos para la valoración; G05/D02/O. Directrices: Transferencia de documentos; G05/D03/O. Directrices: Eliminación de documentos*.
- INTERNATIONAL COUNCIL ON ARCHIVES. *Parliamentary institutions: the criteria for appraising and selecting documents. Las instituciones parlamentarias: criterios para la evaluación y selección de documentos*. Trabajos de la Sección de archivos y archivistas de parlamentos y partidos políticos.
- INTERNATIONAL COUNCIL ON ARCHIVES. 2005. *Manual on appraisal (Draft)*. Committee on Appraisal. Disponible en: <https://www.ica.org/en/draft-manual-appraisal>

- INTERNATIONAL COUNCIL ON ARCHIVES. 2013. *Guidelines on Appraisal and Disposition of Student Records*. Section on University and Research Institutions Archives. Disponible en: https://www.ica.org/sites/default/files/SUV_Appraisal_disposition_student_records_EN.pdf
- INTERNATIONAL COUNCIL ON ARCHIVES / INTERNATIONAL RECORDS MANAGEMENT TRUST. *Managing public sector records: a study programme. Building Records Appraisal Systems*. Disponible en: http://www.irmt.org/documents/educ_training/public_sector_rec/IRMT_build_rec_appraisal.pdf
- INTERNATIONAL STANDARD ORGANIZATION. 2016. *ISO 15489-1:2016. Information and documentation. Records management. Part 1: Concepts and principles*.
- LA TORRE, J. L.; MARTÍN-PALOMINO, M. 2003. *Metodología para la identificación y valoración de fondos documentales*. Madrid: State Archives Office
- MILLARUELO, A.; PÉREZ DE LEMA, A. 2014. *Destrucción o eliminación segura de documentación electrónica y soportes informáticos*. En MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS, 2016. *Política de gestión de documentos electrónicos*. 2ª edición. Madrid: 2016. Disponible en: <http://www.minhafp.gob.es/Documentacion/Publico/SGT/PO-LITICA%20DE%20GESTION%20DE%20DOCUMENTOS%20MINHAP/politica%20de%20gestion%20de%20documentos%20electronicos%20MINHAP-ponencias%20complementarias%20al%20documento.pdf>
- PARADIGM PROJECT: Appraisal and disposal *Workbook on Digital Private Papers*. Disponible en: http://www.paradigm.ac.uk/workbook/pdfs/04_appraisal_disposal.pdf
- TÁBULA: REVISTA DE ARCHIVOS DE CASTILLA Y LEÓN. 2003. 6. *El Refinado arte de la destrucción: la selección de documentos*.
- TORREBLANCA, A.; CONDE, M. L. 2003. *Sistemas de eliminación de documentos administrativos*. Murcia: Dirección General de Cultura.

Resources

- COLOMBIA. ARCHIVO GENERAL DE LA NACIÓN. Tablas de retención documental. Disponible en: <http://www.archivo-general.gov.co/transparencia/gestion-informacion-publica/Tablas-de-Retencion-Documental-TRD>
- ESPAÑA. MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE. Comisión Superior Calificadora de Documentos Administrativos. Grupo de Trabajo de Series y Funciones Comunes. Estudios de identificación y valoración. Disponible en: <http://www.mcu.es/archivos/MC/CSCDA/EstudiosIdentificacion.html>
- ESPAÑA. MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE. Comisión Superior Calificadora de Documentos Administrativos. Formularios. Disponible en: <http://www.mcu.es/archivos/MC/CSCDA/Formularios.html>

Chapter 4 Information Access and Security

Bibliography

- ALBERCHI FUGUERAS, R. 2008. *Archivos y derechos humanos*. Gijón: Trea.
- BETHAULT, D. 2012. El modelo francés de reutilización de la información del sector público. En: *II Jornada sobre la reutilización de la información del sector público: acceso y uso de la información: Madrid, 15 y 16 de febrero de 2012*. Madrid: Universidad Complutense de Madrid.
- CANCIO, J. 2012. Marco legal en España: Real decreto 1495/2011. En: *II Jornada sobre la reutilización de la información del sector público: acceso y uso de la información: Madrid, 15 y 16 de febrero de 2012*. Madrid: Universidad Complutense de Madrid.
- CENTRO DE ARCHIVOS Y ACCESO A LA INFORMACIÓN PÚBLICA (CAinfo). 2012. *Seguridad nacional y acceso a la información en América Latina: estado de situación y desafíos* [en línea]. Documento preparado por Centro de Archivos y

- Acceso a la Información Pública (CAinfo) con la asistencia técnica del Centro de Estudios para la Libertad de Expresión y Acceso a la información (CELE) de la Facultad de Derecho de la Universidad de Palermo, Argentina. Montevideo: CAinfo. Disponible en: <http://www.palermo.edu/cele/pdf/NS-AI.pdf>
- CLAPTON, G.; HAMMOND, M.; POOLE, N. 2011. *PSI re-use in the cultural sector. Final report*. Londres: Curtis+Cartwright Consulting. Disponible en: http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=9020
 - COLLADO, L. 2012. "Usos potenciales de los mapas, directorios y otros productos informativos de la información pública". En: *Il Jornada sobre la reutilización de la información del sector público: acceso y uso de la información: Madrid, 15 y 16 de febrero de 2012*. Madrid: Universidad Complutense de Madrid.
 - COMISIÓN EUROPEA. 2001. Decisión 2001/264/CE del Consejo, de 19 de marzo de 2001, por la que se adoptan las normas de seguridad del Consejo. Disponible en: <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32001D0264&qid=1401793082125&from=EN>
 - COMISIÓN EUROPEA. 2003. Directiva Europea 2003/98/CE, de 17 de noviembre de 2003, del Parlamento Europeo y del Consejo, relativa a la reutilización de la información del sector público. Disponible en: <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:02003L0098-20130717&qid=1401779418320&from=EN>
 - COMISIÓN EUROPEA. 2013. *Opinion 06/2013 on open data and public sector information ('PSI') reuse*. Disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf
 - CHILE. CONTRALORÍA GENERAL DE LA REPÚBLICA. 2012. *Manual de Buenas Prácticas para la Tramitación de Solicitudes de Acceso a la Información. Ley 20.285 sobre Acceso a la Información Pública* [en línea]. Santiago de Chile: Contraloría General de la República. Disponible en: http://www.oas.org/juridico/PDFs/mesicic4_chl_bue_acc.pdf
 - DAVARA FERNÁNDEZ DE MARCOS, I. 2011. *Hacia la estandarización de la protección de datos personales. Propuesta sobre una «tercera vía o tertium genus» internacional*. Madrid: La Ley.
 - DUCHEIN, M. 1983. *Los obstáculos que se oponen al acceso, a la utilización y a la transferencia de la información conservada en los archivos: Un estudio del RAMP* [en línea]. Programa General de Información y Unisist. París: UNESCO. Disponible en: <http://unesdoc.unesco.org/images/0005/000576/057672so.pdf>
 - ESPAÑA. GOBIERNO VASCO. 2010. Manual de seguridad. Disponible en: https://euskadi.net/contenidos/informacion/bp_segurtasuna/es_dit/adjuntos/MSPLATEA_c.pdf
 - ESPAÑA. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. 2013. *Guía de aplicación de la Norma Técnica de Interoperabilidad de Reutilización de Recursos de Información*. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio/pae_Normas_tecnicas_de_interoperabilidad.html#REUTILIZACIONRECURSOS
 - FERNÁNDEZ CUESTA, F. 2012. Al servicio de la transparencia. El papel de los archiveros y la gestión documental en el acceso a la información pública. *Métodos de información* [en línea], 3 (5), pp. 153-166. Disponible en: <http://www.metodosdeinformacion.es/mei/index.php/mei/article/view/IIMEI3-N5-153166/768>
 - FERNÁNDEZ CUESTA, F. 2011. *Protección de datos en archivos públicos: introducción a su estudio* [en línea]. HERNÁNDEZ OLIVERA, L. (dir.). Trabajo Grado de Salamanca, Universidad de Salamanca. Disponible en: <http://hdl.handle.net/10366/111529>
 - FRANCO ESPÍÑO, Beatriz; PÉREZ ALCÁZAR, Ricard (coords.), *Modelo de Gestión de Documentos y Administración de Archivos para la Red de Transparencia y Acceso a la Información* [en línea]. RTA, 2014. Disponible en: <http://mgd.redrta.org/>. Con especial atención a G02/G. *Guía de Implementación Gerencial: Gobierno Abierto y Transparencia. G02/D01/G. Directrices: Acceso a los documentos públicos. G02/D03/G. Directrices: Re-*

utilización de la información. G06/O. *Guía de Implementación Operacional: Control de acceso y G06/D01/O. Directrices: Requisitos de seguridad y acceso. G06/D02/O. Directrices: Gestión de solicitudes de acceso. G06/D03/O. Directrices: Restricciones y control de acceso.*

- FUMEGA, S. 2014. *El uso de las tecnologías de información y comunicación para la implementación de leyes de acceso a la información pública* [en línea]. Santiago de Chile: Consejo para la Transparencia. Disponible en: http://redrta.cplt.cl/_public/public/folder_attachment/55/1a/1a3b_6f48.pdf
- GLOVER, M. et al. 2006. *Freedom of information: history, experience and records and information management implications in the USA, Canada and the United Kingdom*. Pittsburgh: ARMA International Educational Foundation. Disponible en: http://armaedfoundation.org/wp-content/uploads/2016/12/Freedom_of_Information_in_US_UK_and_Canada.pdf
- GÓMEZ, R. [et. al.]. 2010. Metodología y gobierno de la gestión de riesgos de tecnologías de la información. *Revista de Ingeniería* [en línea], 31, pp. 109-118. Disponible en: <http://www.redalyc.org/articulo.oa?id=121015012006>
- GÓMEZ FERNÁNDEZ, L.; ANDRÉS ÁLVAREZ, A. 2012. *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad de sistemas de información para PYMES*. 2ª ed. Madrid: AENOR.
- GONZÁLEZ QUINTANA, A. 2010. Archivos y derechos humanos. Recomendaciones desde el Consejo Internacional de Archivos. En: BABIANO MORA, J. (coord.). *Represión, derechos humanos, memoria y archivos. Una perspectiva latinoamericana*. Madrid: Fundación 1º de mayo, pp. 189-199.
- INTERNATIONAL COUNCIL ON ARCHIVES. 2012. *Principios de acceso a los archivos*. Trad. de Esther Cruces Blanco. París: ICA. Disponible en: https://www.ica.org/sites/default/files/ICA_Access-principles_SP.pdf
- INTERNATIONAL COUNCIL ON ARCHIVES. 2014. *Principios de acceso a los archivos. Guía técnica para la gestión de archivos de uso restringido*. París: ICA. Disponible en: https://www.ica.org/sites/default/files/Technical%20Guidance%20on%20Managing%20Archives%20with%20restrictions_SP.pdf
- INTERNATIONAL COUNCIL ON ARCHIVES (ICA). 2014. *Guía técnica para la gestión de archivos de uso restringido* [en línea]. París: ICA. Disponible en: https://www.ica.org/sites/default/files/Technical%20Guidance%20on%20Managing%20Archives%20with%20restrictions_SP.pdf
- NOTA: La traducción al español de este documento cuenta con algunos errores, por lo que recomendamos, en la medida de lo posible, acudir a la versión original en inglés: INTERNATIONAL COUNCIL ON ARCHIVES (ICA). 2014. *Technical Guidance on Managing Archives with Restrictions* [en línea]. París: ICA. Disponible en: <https://www.ica.org/en/technical-guidance-managing-archives-restrictions-0>
- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). 2010. *ISO 16175-3:2010: Information and documentation - Principles and functional requirements for records in electronic office environments - Part 3: Guidelines and functional requirements for records in business systems*. Ginebra: ISO.
- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). 2011. *ISO 16175-2:2011: Information and documentation - Principles and functional requirements for records in electronic office environments - Part 2: Guidelines and functional requirements for digital records management systems*. Ginebra: ISO.
- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). 2016. *ISO 15489-1:2016: Information and documentation - Records management - Part 1: Concepts and principles*. Ginebra: ISO.
- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). 2013. *ISO/IEC 27001:2013. Information technology -- Security techniques -- Information security management systems*. Ginebra: ISO.
- JOYANES AGUILAR, L. 2012. Ciberespacio y libre acceso a la información. En: *Il Jornada sobre la reutilización de la información del sector público: acceso y uso de la información: Madrid, 15 y 16 de febrero de 2012*. Madrid: Universidad Complutense de Madrid.
- ORENGA, L.; SOLER, J. 2010. *Com es fa un Quadre de Seguretat i Accés?* [presentación en línea]. Material docente del curso homónimo celebrado los días 10 y 17 de noviembre de 2010

en Tarragona y Barcelona, para la Associació d'Arxivers de Catalunya. Disponible en:

<http://www.slideshare.net/JoanSolerJimnez/com-es-fa-un-quadre-de-seguretat-i-accs>

- ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA). 2010a. *Ley Modelo Interamericana sobre Acceso a la Información Pública* [en línea]. AG/RES. 2607 (XL-O/10). Disponible en: http://www.oas.org/dil/esp/AG-RES_2607-2010.pdf
- ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA). 2010b. *Comentarios y guía de implementación para la Ley modelo interamericana sobre acceso a la información* [en línea]. CP/CAJP-2841/10. Disponible en: http://www.oas.org/es/sla/ddi/docs/AG-RES_2841_XL-O-10_esp.pdf
- PARLAMENTO EUROPEO. 2013. Directiva 2013/37/UE del Parlamento Europeo y del Consejo de 26 de junio de 2013, por la que se modifica la Directiva 2003/98/CE relativa a la reutilización de la información del sector público. Disponible en: <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32013L0037&qid=1401780323623&from=EN>
- PELEGRÍN, J. 2012. La revisión de la Directiva europea 2003/98 sobre reutilización de la Información del Sector Público. En: *II Jornada sobre la reutilización de la información del sector público: acceso y uso de la información: Madrid, 15 y 16 de febrero de 2012*. Madrid: Universidad Complutense de Madrid.
- RAMÍREZ DELEÓN, J. A. 2007. *Archivos gubernamentales: Un dilema de la transparencia*. México: INFODF. Disponible en: http://www.cevat.org.mx/retaip/documentos/material_apoyo/ensayo/Ensayo2.pdf
- RAMOS SIMÓN, L. F.; MENDO CARMONA, C.; ARQUERO AVILÉS, R. 2009. La producción informativa y documental del Estado: hacia un inventario de los recursos públicos. En: *Revista española de documentación científica*, (32), 1, pp. 40–59.
- SCARENSI, M. J. 2014. La legislación archivística y el acceso a la información en América Latina. En: TORRES, N. (comp.). *Hacia una política integral de gestión de la información pública. Todo lo que siempre quisimos saber sobre archivos (y nunca nos animamos a preguntarle al acceso a la información)* [en línea]. Buenos Aires: Centro de Estudios en Libertad de Expresión

y Acceso a la Información (CELE); Universidad de Palermo, pp. 109-154. Disponible en: http://www.palermo.edu/cele/pdf/Hacia_una_politica_integral-kk.pdf

- SERRA SERRA, J. 2013. Una interpretación metodológica de la norma ISO 15489 para la implantación de un sistema de gestión de documentos. En: *Jornadas Ibéricas de Archivos Municipais: Políticas, Sistemas e Instrumentos nos Archivos Municipais, 04 e 05 de Junho 2013* [en línea]. Lisboa: Arquivo Municipal. Disponible en: http://arquivomunicipal.cm-lisboa.pt/fotos/editor2/j_serra.pdf
- TORRES, N. (comp.). [2013]. *Acceso a la información y datos personales: una vieja tensión, nuevos desafíos* [en línea]. Buenos Aires: Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE). Disponible en: http://www.palermo.edu/cele/pdf/DatosPersonales_Final.pdf
- TRONCOSO RAIGADA, A. 2009. Reutilización de información pública y protección de datos personales. En: *Revista general de información y documentación*, 19, pp. 243–264.
- VALENTÍN RUIZ, F. J.; BUENESTADO DEL PESO, R. 2012. Aproximación al panorama actual de la reutilización de la información del sector público. En *Textos universitarios de Biblioteconomía i Documentació*, 29.
- VRIES, M. 2012. El proyecto ePSIplatform en sus últimos desarrollos. En: *II Jornada sobre la reutilización de la información del sector público: acceso y uso de la información: Madrid, 15 y 16 de febrero de 2012*. Madrid: Universidad Complutense de Madrid.

Resources

- COMISIÓN EUROPEA. Digital Agenda for Europe. A Europe 2020 Initiative. Revision of the PSI Directive. Disponible en: <http://ec.europa.eu/digital-agenda/news/revision-psi-directive>
- COMISIÓN EUROPEA. Digital Agenda for Europe: key initiatives. Disponible en: http://europa.eu/rapid/press-release_MEMO-10-200_en.htm

- COMISIÓN EUROPEA. Legal Aspects of Public Sector Information (LAPSI) thematic network outputs. Disponible en: <https://ec.europa.eu/digital-single-market/en/news/legal-aspects-public-sector-information-lapsi-thematic-network-outputs>
- ESPAÑA. GOBIERNO DE ESPAÑA. datos.gob.es. Disponible en: <http://datos.gob.es/es>
- ESPAÑA. GOBIERNO VASCO. Open Data Euskadi. Disponible en: <http://opendata.euskadi.eus/inicio/>
- ESPAÑA. MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL. Plan Avanza. Disponible en: <http://www.agenda-digital.gob.es/agenda-digital/planes-anteriores/Paginas/plan-avanza.aspx>
- ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Acceso a la información. Disponible en: http://www.oas.org/es/sla/ddi/acceso_informacion_ley_modelo.asp

Chapter 5 Conservation and Contingency Management

Bibliography

- BELLO, C.; BORRELL, À. 2008. *Los documentos de archivo: cómo se conservan*. Gijón: Trea.
- CALDERÓN DELGADO, Marco. *Conservación Preventiva de documentos*. Archivo Nacional. Costa Rica. Disponible en: http://www.archivonacional.go.cr/pdf/conservacion_preventiva_documentos.pdf
- COLOMBIA. PRESIDENCIA DE LA REPÚBLICA. 2016. *Guía para la conservación de documentos*. Bogotá. Disponible en: <http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/G-GD-01-conservacion-documentos.pdf>
- FRANCO ESPIÑO, Beatriz; PÉREZ ALCÁZAR, Ricard (coords.), *Modelo de Gestión de Documentos y Administración de Archivos para la Red de Transparencia y Acceso a la Información* [en línea]. RTA, 2014. Disponible en: <http://mgd.redrta.org/>. Con especial atención a G07/O. *Guía de Implementación Operacio-*

nal: Control físico y conservación y G07/D01/O. Directrices: Plan integrado de conservación. G07/D02/O. Directrices: Custodia y control de las instalaciones.

- HAEBERLEN, T.; LIVERI, D.; LAKKA, M. 2013. *Good Practice Guide for securely deploying Governmental Clouds*. European Union Agency for Network and Information Security. Disponible en: <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/good-practice-guide-for-securely-deploying-governmental-clouds>
- MARTÍNEZ REDONDO, Piedad, *Plan de conservación documental. Estrategias y procesos de conservación para asegurar el adecuado mantenimiento de los documentos en soporte papel*. UPRA. Colombia. Disponible en: <http://www.upra.gov.co/documents/10184/18526/Plan+de+Conservaci%C3%B3n+Documental+-+UPRA+-+version+1.0+Final.pdf/c1821ed8-5c0e-400f-b4c1-31b79d31c471>
- MILLARUELO, A. 2014. Estrategia de conservación de documentos en repositorio, conforme al calendario de conservación. Ponencia nº 5. En MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS, 2016. *Política de gestión de documentos electrónicos*. 2ª edición. Madrid: 2016. Disponible en: <http://www.minhfp.gob.es/Documentacion/Publico/SGT/POLITICA%20DE%20GESTION%20DE%20DOCUMENTOS%20MINHAP/politica%20de%20gestion%20de%20documentos%20electronicos%20MINHAP-ponencias%20complementarias%20al%20documento.pdf>
- OGDEN, S. 1998. *El manual de preservación de bibliotecas y archivos del Northeast Document Conservation Center*. Santiago de Chile: DIBAM. Disponible en: <http://www.dibam.cl/Recursos/Publicaciones/Centro%20de%20Conservaci%C3%B3n/archivos/OGDEN.PDF>
- ROTAECHE GONZÁLEZ DE UBIETA, M. 2007. *Transporte, depósito y manipulación de obras de arte*. Madrid: Editorial Síntesis.
- SÁNCHEZ HERNANPÉREZ, A. 1999. *Políticas de Conservación en Bibliotecas. Instrumenta Bibliológica*. Madrid: Arco Libros.
- TACÓN CLAVAIN, J. 2008. *La conservación en archivos y bibliotecas: prevención y protección*. Madrid: Ollero y Ramos.
- TACÓN CLAVAIN, J. 2011. *Soportes y técnicas documentales: causas de su deterioro*. Madrid: Ollero y Ramos.

- SASTRE NATIVIDAD, Garazi. *Preservación y conservación de documentos digitales* [en línea]. En: ArchivPost. Salamanca: Asociación de Archiveros de Castilla y León, 2015. Disponible en: <http://www.acal.es/index.php/archivpost-a-fondo>

Chapter 6 Awareness Raising and User Assistance Services

Bibliography

- ALBERCH I FUGUERAS, R. 2003. La dinamización cultural en el archivo, un reto futuro. En: *VII Jornadas Archivísticas. Aprender y enseñar con el archivo*. Huelva, pp. 127-135.
- ALBERCH, R.; BOIX, L.; NAVARRO, N.; VELA, S. 2001. *Archivos y cultura: manual de dinamización*. Gijón: Trea.
- CAMPOS, J. 2009. *La difusión en los archivos: importante herramienta de proyección ante la sociedad* Disponible en: <http://eprints.rclis.org/20236/1/La%20difusi%C3%B3n%20en%20los%20archivos%20importante%20herramienta%20de%20proyecci%C3%B3n%20ante%20la%20sociedad.pdf>
- CERDÁ DÍAZ, J. 2008. Las exposiciones documentales. Técnicas y tendencias. En: *Tábula: Revista de Archivos de Castilla y León*, 11, pp. 359-384.
- CERDÁ DÍAZ, J. 2010. Los archivos, un lugar para descubrir. Experiencias de dinamización cultural. En: GONZÁLEZ CACHAFEIRO, J. (Coord.). *3ª Jornadas Archivando. La difusión en los archivos. Actas de las Jornadas. León 11 y 12 noviembre de 2010*. Disponible en: http://archivosierrapambley.files.wordpress.com/2011/01/actas_jornadas_2010.pdf
- COX, R.J. Machines in the archives: Technology and the coming transformation of archival reference. *First Monday*.
- CRYMBLE, A. 2010. An Analysis of Twitter and Facebook Use by the Archival Community. En *Archivaria*, 70 Disponible en: <http://journals.sfu.ca/archivar/index.php/archivaria/article/view/13298>
- DUFF, W.; FOX, A. 2006. 'You're a guide rather than an expert': Archival reference from an archivist's point of view. *Journal of the Society of Archivists*.
- ESPAÑA. JUNTA DE CASTILLA Y LEÓN. 2006. *Manual de archivo de oficina*. Valladolid: Junta de Castilla y León.
- ESPAÑA. MINISTERIO DE EDUCACIÓN CULTURA Y DEPORTE. 2003. *Archivo de oficina*. Madrid: Ministerio de Educación, Cultura y Deporte. Disponible en: <https://www.mecd.gob.es/cultura-mecd/dms/mecd/cultura-mecd/areas-cultura/archivos/recursos-profesionales/documentos-tecnicos/archivo-de-oficina.pdf>
- FERNÁNDEZ CUESTA, F. 2008. *Archiblogs: el blog como nueva herramienta de difusión del archivo*. En: *Jornadas Archivando. Un nuevo paradigma en la gestión de archivos*. Disponible en: <http://www.slideshare.net/pacofernandez/jornadas-archivamos-presentation>
- FERNÁNDEZ GIL, Paloma. 1996. Archivos de Oficina: la Teoría Archivística y la Práctica. En: *La organización de documentos en los archivos de oficina: XI Jornadas de Archivos Municipales (Aranjuez, 23-24 Mayo 1996)*. Madrid: Dirección General del Patrimonio Cultural: Ayuntamiento del Real Sitio y Villa de Aranjuez, Archivo Municipal: Grupo de Archiveros Municipales de Madrid, pp. 155-160.
- FRANCO ESPIÑO, Beatriz; PÉREZ ALCÁZAR, Ricard (coords.), *Modelo de Gestión de Documentos y Administración de Archivos para la Red de Transparencia y Acceso a la Información* [en línea]. RTA, 2014. Disponible en: <http://mgd.redrta.org/>. Con especial atención a G08/O. *Guía de Implementación Operacional: Servicios de Archivo y G08/D03/O. Directrices: Difusión. G08/D01/O. Directrices: Atención a la Administración. G08/D02/O. Directrices: Atención al público*.
- JAÉN, L. F. 2006. *La Difusión de Archivos: estrategias para su proyección*. Convención Internacional de Archivistas. Mar del Plata, Argentina.
- NAVARRO BONILLA, D. 2001. El servicio de referencia archivístico: retos y oportunidades. *Revista española de Doc-*

umentación Científica, 24 (2), pp. 178-197. Disponible en: <http://redc.revistas.csic.es/index.php/redc/article/viewFile/49/109>

- SIERRA, L. F. 2011. Difusión en archivos: una visión integradora. En: *Códices* (7), 2. Universidad Lasalle, Colombia. Disponible en: http://eprints.rclis.org/20000/1/Difusi%C3%B3n%20en%20archivos_una%20visi%C3%B3n%20integradora.pdf
- YAKEL, E. 2000. Thinking inside and outside the boxes: archival reference services at the turn of the Century. *Archivaria*, 49, pp. 140-160. Disponible en: <http://journals.sfu.ca/archivar/index.php/archivaria/article/viewFile/12742/13927>

Resources

- CHILE. ARCHIVO NACIONAL DE CHILE. Material educativo. Disponible en: http://www.archivonacional.cl/616/w3-propertyvalue-38641.html?_noredirect=1
- COLOMBIA. ARCHIVO NACIONAL DE LA NACIÓN. AGN para niños, niñas y adolescentes. Disponible en: <http://www.archivogeneral.gov.co/Conozcanos/agn-para-ninos>
- ESPAÑA. MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE. Exposiciones y visitas virtuales de los Archivos. Disponible en: <http://www.mecd.gob.es/cultura-mecd/areas-cultura/archivos/exposiciones-y-visitas-virtuales.html>
- MÉXICO. ARCHIVO GENERAL DE LA NACIÓN. Actividades de difusión. Disponible en: <http://www.agn.gob.mx/menuprincipal/difusion/difusion.html>

Chapter 7 Electronic Administration

Bibliography

- AUSTRALIA. NATIONAL ARCHIVES OF AUSTRALIA. 2010. *Australian Government Recordkeeping Metadata Standard Implementation Guidelines: Exposure Draft*.

- AUSTRALIA. NATIONAL ARCHIVES OF AUSTRALIA. 2011. *Australian Government Recordkeeping Metadata Standard Implementation Guidelines. Version 2.0*.
- AUSTRALIA. DEPARTMENT OF FINANCE AND ADMINISTRATION. 2006. Australian Government Information Interoperability Framework. Disponible en: https://www.finance.gov.au/publications/agimo/docs/Information_Interoperability_Framework.pdf
- BROWN, A. 2008. *Digital Preservation Guidance Note 2: Selecting Storage Media for Long-Term Preservation*. Londres: The National Archives <http://www.nationalarchives.gov.uk/documents/selecting-storage-media.pdf>
- COMISIÓN EUROPEA. 2008. *MoReq2 Specification. Model Requirements for the Management of Electronic Records*.
- COMISIÓN EUROPEA. 2008. *Semantic Interoperability Centre Europe. A Study on Good Practices in Existing Repositories*.
- ESPAÑA. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS, 2016c. *Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0. Documentación complementaria a la Norma Técnica de Política de gestión de documentos electrónicos*. Madrid: 2016. Disponible en: https://www.administracionelectronica.gob.es/pae_Home/pae_Estrategias/Archivo_electronico/pae_Metadatos.html
- FRANCO ESPÍÑO, Beatriz; PÉREZ ALCÁZAR, Ricard (coords.), *Modelo de Gestión de Documentos y Administración de Archivos para la Red de Transparencia y Acceso a la Información* [en línea]. RTA, 2014. Disponible en: <http://mgd.redrta.org/>. Con especial atención a G03/G. *Guía de Implementación Gerencial: Administración electrónica y G03/D01/G. Directrices: Interoperabilidad. G03/D02/G. Directrices: Administración de documentos electrónicos*.
- INTERNATIONAL FEDERATION OF LIBRARY ASSOCIATIONS AND INSTITUTIONS. 2005. Directrices para proyectos de digitalización de colecciones y fondos de dominio público, en particular para aquellos custodiados en bibliotecas y archivos, marzo de 2002. Madrid: Ministerio de Cultura. Disponible en: <https://www.ifla.org/files/assets/preservation-and-conservation/publications/digitization-projects-guidelines-es.pdf>

- INTERNATIONAL STANDARD ORGANIZATION. 2009. *ISO 23081-2:2009. Information and documentation. Records Management process Metadata for records: Part II: Conceptual and implementation issues.*
- INTERNATIONAL STANDARDS ORGANIZATION. *ISO/TR 18492:2005. Long-Term Preservation of Electronic Document-Based Information.*
- INTERNATIONAL STANDARDS ORGANIZATION. 2009. *ISO/TR 15801:2009. Document management -- Information stored electronically -- Recommendations for trustworthiness and reliability.*
- INTERNATIONAL STANDARDS ORGANIZATION. 2010a. *ISO 16175-1:2010. Principles and functional requirements for records in electronic office environments. Part 1: Overview and statement of principles.*
- INTERNATIONAL STANDARDS ORGANIZATION. 2010b. *ISO 16175-2:2010. Principles and functional requirements for records in electronic office environments. Part 2: Guidelines and functional requirements for digital records management systems.*
- INTERNATIONAL STANDARDS ORGANIZATION. 2010c. *ISO 16175-3:2010. Principles and functional requirements for records in electronic office environments. Part 3: Guidelines and functional requirements for records in business systems.*
- INTERNATIONAL STANDARD ORGANIZATION. 2011a. *ISO 30300:2011. Information and Documentation. Management system for records. Fundamentals and vocabulary.*
- INTERNATIONAL STANDARD ORGANIZATION. 2011b. *ISO 30301:2011. Information and Documentation. Management system for records. Requirements.*
- INTERNATIONAL STANDARD ORGANIZATION. 2011c. *ISO 23081-3:2011. Information and documentation. Records Management process Metadata for records: Part III: Self-assessment method.*
- INTERNATIONAL STANDARD ORGANIZATION. 2016. *ISO 15489-1:2016. Information and documentation. Records management. Part I: Concepts and principles.*
- INTERNATIONAL STANDARD ORGANIZATION. 2017. *ISO 23081-1:2017. Information and documentation. Records Management processes. Metadata for records: Part I: Principles.*

- JIMÉNEZ GÓMEZ, C. E. 2012. *Elementos relevantes en la transposición e implantación de los marcos nacionales de interoperabilidad.* XVII Congreso Internacional del CLAD sobre la Reforma del Estado y de la Administración Pública, Cartagena, Colombia, 30 oct. - 2 nov. 2012. Disponible en: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2311879

Resources

- AUSTRALIA. DEPARTMENT OF FINANCE. Australian Government Information Interoperability Framework. Disponible en: <http://www.finance.gov.au/policy-guides-procurement/interoperability-frameworks/information-interoperability-framework/>
- AUSTRALIA. The Australian Government Information Management Office Archive. Digitisation of Records: Better Practice Checklist. Disponible en: <http://www.finance.gov.au/agimo-archive/better-practice-checklists/digitisation.html>
- BRASIL. CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO. 2012. Sustentabilidade. Justicia de trabajo. Disponible en: http://www.tst.jus.br/documents/1692526/0/Cat%C3%A1logo_Ingl%C3%AAs_Espanhol_web.pdf
- CANADÁ. THE UNIVERSITY OF BRITISH COLUMBIA. InterPARES Project. International Research on Permanent Authentic Records in Electronic Systems. Disponible en: <http://www.interpares.org/welcome.cfm>
- COMISIÓN EUROPEA. ISA. Interoperability Solutions for European Administrations. Disponible en: https://ec.europa.eu/isa2/home_en
- COMISIÓN EUROPEA. CEF Building Blocks for a Digital Connected Europe. Disponible en: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/About+CEF+building+blocks>
- COMISIÓN EUROPEA. General Model of Electronic Archiving. Disponible en: <http://kc.dlmforum.eu/gm3>
- NUEVA ZELANDA. ARCHIVES NEW ZEALAND. Digitisation guidance - what's current and what's happening?. Disponible en: <https://records.archives.govt.nz/toolkit-blog/digitisation-guidance-whats-happening/>

- PREMIS. Preservation Metadata Maintenance Activity. Disponible en: <http://www.loc.gov/standards/premis/>
- REINO UNIDO. Digital Preservation Coalition. Disponible en: <https://dpconline.org/>
- UNIÓN EUROPEA. ePractice.eu. Observatorio Europeo de la Administración Electrónica. Disponible en: <http://www.epractice.eu/en/home/>
- UNIÓN EUROPEA. Portal Europeo de Justicia. Disponible en: <https://e-justice.europa.eu/home.do?action=home&plang=es>

Chapter 8 Staff Profiles and Document Management Training

Bibliography

- ALBERCH, R.; COROMINAS, C.; MARTÍNEZ, M. C. 1997. El personal de los Archivos. Función archivística y su plantilla. *Lligall. Revista catalana d'arxivística*, 11, pp. 221-252
- Disponible en: <https://www.um.es/adegap/docsinfo/archivistica.pdf>
- ESPAÑA. MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA, 2016a. *Política de gestión de documentos electrónicos. Guía de aplicación de la Norma Técnica de Interoperabilidad*. 2ª edición. Madrid: 2016. Disponible en: http://www.administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio/pae_Normas_tecnicas_de_interoperabilidad.html#POLITICAGESTION
- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. 2010. ISO/TC46/SC11, *Preservación de documentos digitales. Guía "Cómo empezar"*. Disponible en: <https://committee.iso.org/sites/tc46sc11/home/projects/published/digital-records-processes-and-se.html>
- INTERNATIONAL STANDARD ORGANIZATION. 2011a. *ISO 30300:2011. Information and Documentation. Management system for records. Fundamentals and vocabulary*.

- INTERNATIONAL STANDARD ORGANIZATION. 2011b. *ISO 30301:2011. Information and Documentation. Management system for records. Requirements*.
- INTERNATIONAL STANDARD ORGANIZATION. 2016. *ISO 15489-1:2016. Information and documentation. Records management. Part I: Concepts and principles*.
- LLANSÓ, J.; COSTANILLA, L.; GARCÍA, O.; ZABALZA, I. 2013. *Buenas prácticas en gestión de documentos y archivos. Manual de normas y procedimientos archivísticos de la Universidad Pública de Navarra*. Pamplona: Servicio de Publicaciones.
- MÉXICO. INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES. Lineamientos generales para la organización y conservación de los archivos de la Administración Pública General. <http://cevfaiprivada.ifai.org.mx/swf/cursos/archivos/introduccion.html>

Prepared under the direction of the Department of International Law, Secretariat for Legal Affairs, OAS. Consultants:

Beatriz Franco Espiño, Chief, Document Appraisal and Processing Service State Archives Office Ministry of Education, Culture, and Sport of Spain

Ricard Pérez Alcázar, Department Chief, Archive Programming and Coordination Area State Archives Office Ministry of Education, Culture, and Sport of Spain

Addenda

Inter-American Model Law 2.0 on Access to Public Information



Addendum A Inter-American Model Law on Document Management



ISBN 978-0-8270-7195-7



OAS

More rights for more people