**ORGANIZATION OF AMERICAN STATES**

INTER-AMERICAN JURIDICAL COMMITTEE

CJI


OEA/Sec.General
DDI/doc. 3/20
January 18, 2020
Original: English/Spanish

# MODEL INTER-AMERICAN LAW ON ACCESS TO PUBLIC INFORMATION 2.0

Prepared by the Department of International Law
in compliance with General Assembly Resolution
AG/RES. 2905 (XLVII-O/17) "Strengthening Democracy," paragraph ix)

**Explanatory Note**

This document constitutes the conclusion of the work carried out by the Department of International Law (DIL) of the Secretariat for Legal Affairs in compliance with OAS General Assembly resolution AG/RES. 2905 (XLVII-O/17), *Strengthening Democracy* paragraph (ix). The resolution directs the DIL to "consult with the focal points of the Inter-American Program on Access to Public Information[1] as well as civil society, to identify the thematic areas that require updates or further development in the Model Inter-American Law on Access to Public Information ("the Model Law"), adopted by the General Assembly in 2010,[2] and to convey the results of this process be o Inter-American Juridical Committee for consideration and further development".

In order to best fulfill its mandate, the DIL executed the activities that have been reported[3] to the Inter-American Juridical Committee (CJI) in a timely and detailed manner, including:

- conducting a survey, sent out to more than 4,000 individuals and institutions, including the Inter-American Commission of Women (CIM), the Inter-American Commission on Human Rights (IACHR) aimed at identifying the areas where the Model Law could be further developed;
- organizing four workshops held between April 2018 and May 2019, which were attended by 152 specialists from CSOs as well as authorities from 15 Member States, including many focal points of the Inter-American Program on Access to Public Information, as well as civil society organizations (CSOs); and
- organizing meetings to collect input and specific recommendations from 26 CSOs from 14 Member States: Argentina, Brazil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, Mexico, Paraguay, the United States, Uruguay and Venezuela.

The most commonly identified areas as priorities for revision were: exceptions regime, active transparency, document management, guarantor bodies, political parties and public information within the judiciary branch, all of which became the focus and substance of the workshops held with the guarantor bodies and civil society. In that context, three action items were decided by consensus:

- focus the collective efforts in the development of agreed upon texts on guarantor bodies, exceptions regime, subject entities, active transparency, definition and scope of the right of access to public information;
- to leave the matter of document and management in the hands of expert consultants, as the highly technical content of a model law would require very specialized knowledge; and attach to the revised draft Inter-American Model Law on Access to Public Information ( Model Law 2.0) a proposed Model Law on Document Management and its Application Guide, thought these two latter documents would not technically be a part of the Model Law 2.0; and
- to postpone the discussion of the issue of access to public information in the possession or custody of the judiciary for another time, incorporating the input of information officers from the judicial branches and experts that may contribute a more comprehensive perspective of the particular

[1] AG/RES. 2885 (XLVI-O/16)

[2] AG/RES. 2607 (XL-O/10)

[3] Document DDI/Doc.3/19 Rev.1

intricacies of the judicial processes, among them the need for classifying certain information at specific moments in the process, the implications of disclosure on the protection of victims, witnesses and minors, etc.

It is important to highlight that throughout this undertaking, the DIL has remained mindful of the gender perspective, recognizing the opportunity to propose provisions that make the Model Law 2.0 one of the first legal instruments of the Inter-American System to incorporate a gender perspective by design. To this end, a dedicated workshop was held to exclusively to analyze issues pertaining to gender and access to information, with the participation of specialists whose contributions greatly enriched the agreed upon texts.

In July 2019, the DIL submitted a document[4] for the consideration of the members of the CJI including all the agreed upon provisions and invited them to submit their comments in writing, and eventually proceeded to assemble this document, which consolidates the original text of the Model Law that will remain unchanged with the agreed upon provisions on the areas identified during the consultation process as ripe for updates or enhancements.

By submitting this complete draft Model Law 2.0 to the consideration of the CJI during its 96th regular session, the DIL thereby has fulfilled the mandate conferred by the General Assembly.

****

[4] Document DDI/Doc.3/19 Rev.1

# MODEL INTER-AMERICAN LAW ON ACCESS TO PUBLIC INFORMATION 2.0

## TABLE OF CONTENTS

Regulations

**ADDENDA**

## CHAPTER I. DEFINITIONS, SCOPE, RIGHT OF ACCESS AND INTERPRETATION

### Article 1. Definitions

In this Law, unless the context otherwise requires:

a) "Public Interest Activity" refers to those subjects or areas of management that should be resolved in government political decisions, at any of the levels of administrative, legislative or judicial political organization, and that seek to serve the maximum interest of the community;

b) "Senior Officials" refers to any official within a Public Authority whose total annual salary exceeds [USD$100,000];

c) "Public Authority" refers to any governmental authority and to the private organizations falling under the third paragraph of Article 2 of this Law;

d) "Document" refers to any written Information, regardless of its form, source, date of creation or official status, whether or not it was created by a Public Authority, political parties, unions and non-profit organizations holding the document and whether or not it was classified as confidential;

e) "Public Funds" refers to the financial resources, whether tax-related or not, that are generated, obtained, or originated by the State, regardless of who manages those resources;

f) "Unions" refers to the association of persons and/or companies engaged in the same work and whose main objective is mutual support, wherein they seek the well-being of the group they represent;

g) "Information" refers to any type of datum in the custody or control of a Public Authority, Political Party, Union and Non-Profit Organizations.

h) "Personal Information" refers to information regarding a living person who is or may be identified through such Information;[1]

i) "Information Officer" refers to the individual or individuals appointed by a Public Authority pursuant to Article 18 of this Law;

j) "Non-profit organization" refers to entities recognized by the State that engage in activities designed to serve the public interest, whose purpose is not to make a profit, that have a specific mission and are independent of the State.

k) "Political Party" refers to public interest entities with their own legal status and assets, recognized by national legislation, the purpose of which is to promote the people's participation in democratic life, contribute to the formation of representative political bodies and, as citizen organizations of citizens, to enable citizen access to the exercise of public power;

l) "Publish" refers to the act of making Information accessible to the general public and includes printing, broadcasting and electronic forms of dissemination; and

[1] This definition has been taken from the Principles on Privacy and Personal Data Protection in the Americas, approved during the 84th Regular Session of the Inter-American Juridical Committee (CJI/doc. 450/14).

m) "Interested Third Parties" refers to persons who have a direct interest in preventing the disclosure of Information they provided voluntarily to a Public Authority, because such disclosure either affects their privacy or their commercial interests.

**Article 2. Scope and purpose**

1. This Law establishes the broadest possible application of the right of access to Information that may be in the possession, custody or control of any Public Authority, Political Party, Union and Non-Profit Organization, and that is based on the principles of *pro homine* and *in dubio pro actione* in accordance with which one ought to seek the interpretation most favorable to the exercise of that right.

2. This Law is also based on the principle of maximum disclosure, so that any Information held by subject entities shall be complete, timely and accessible, subject to a clear and narrow exceptions regime to be defined by law as well as legitimate and strictly necessary in a democratic society.

3. This law applies to:

a) any Public Authority belonging to any branch of government (executive, legislative and judicial) and at all levels of the internal governmental structure (central or federal, regional, provincial or municipal);

b) independent or autonomous bodies, organizations or entities owned or controlled by the government, acting by virtue of powers granted by the Constitution or by other laws; and

c) Public Funds, as well as any individual or legal entity that receives or manages public resources or carries out acts of authority at the national or federal level.[2]

3.1 This Law shall likewise apply to private organizations, Political Parties or similar associations, Unions, guilds and Non-Profit Organizations, which must respond to requests for Information but only with respect to the Public Funds or benefits received or the public functions and services performed. In the event that said Public Funds or benefits exceed [XX% of their annual budget / the amount of $XX], the above entities shall also comply with the obligations of active transparency provided in this Law.

4. No public authority shall be exempt from the requirements established in this law, including the legislative and judicial branch, supervisory institutions, intelligence services, armed forces, police, other security bodies, Chiefs of State and government, and the divisions thereof.

Subject entities shall document any action deriving from the exercise of their powers, responsibilities or functions.

5. In the event of any inconsistency, this Law shall prevail over any other law.[3]

**Article 3. Right of access to public information**

1. Any person requesting Information from any Public Authority covered by this Law shall have the following rights, subject only to the provisions of Chapter IV of this Law:

a) to be informed whether or not the Public Authority holds Documents containing the Information requested or from which that Information may be derived;

[2] Comment: the term "public benefits" should not be interpreted broadly, so as to include any financial benefit received from the government.

[3] Comment: While the Model Law does not contain a provision that includes within its scope information in the possession of private companies that is necessary for the exercise or protection of internationally recognized human rights, it is noted that some states, including South Africa, have adopted this approach.

b) if the Public Authority that received the request holds said Documents, to be promptly notified accordingly;

c) if said Documents are not delivered to the requester, to appeal the failure to deliver the Information;

d) to make anonymous requests for Information;

e) to request Information without having to justify the reasons why it is being sought;

f) to be free from any discrimination that may be based on the nature of the request; and

g) to obtain the Information free of charge or at a cost not exceeding the cost to reproduce the Documents.

2. The requester shall not be sanctioned, punished or prosecuted for exercising the right of access to Information.

3. The Information Officer shall make reasonable efforts to assist the requester with regard to the request, to respond to the request accurately and completely and, subject to applicable regulations, to provide timely access to the Documents in the format requested.

4. The Guarantor Body shall make reasonable efforts to assist the requester in connection with an appeal filed in response to a refusal to disclose Information.[4]

### Article 4. Interpretation

1. Anyone tasked with the interpretation of this Law, or any other legislation or regulatory instrument that may affect the right to Information shall adopt the reasonable interpretation that ensures the most effective right to information.

2. When several institutions have jurisdiction over access to public Information and the protection of personal data, close coordination should be sought so that both rights are harmoniously protected.

## CHAPTER II. MEASURES TO PROMOTE OPENNESS

### Article 5. Active transparency

1. All subject entities shall proactively disseminate the key Information established by this Law, without the need for any request for such Information.

2. All subject entities shall allow the broadest access to such Information so as to permit interoperability in an open data format[5] as well as determine strategies for the identification, generation, organization, publication and dissemination of such Information so that it can be easily reused[6] by society.

3. The Guarantor Body is responsible for:

---

[4] Comment: to meet this requirement, it is considered a good practice to make a free legal advisory service available to requesters who need it during the administrative or legal proceeding on access to public Information.

[5] Comment: *Open data* is understood to mean data that can be used, reused and redistributed. They should be in a free and unrestricted format so that derivative services can be created from them.

[6] Comment: The objective of reusing Information is to share it among the largest number of people, using all available media including, *inter alia*, the website, broadcast media, television and the print media.

a) periodically ensuring that subject entities fully implement these obligations;

b) designing policies that facilitate the coordination of efforts and tasks carried out by subject entities in order to comply with their active transparency obligations;[7]

c) issuing the technical guidelines it deems appropriate for establishing information publication formats so as to facilitate the proper standardization thereof and ensuring that such information is accurate, reliable, timely, consistent, comprehensive, updated, accessible, comprehensible, and verifiable and satisfies the principle of non-discrimination.

d) establishing the criteria and protocols for removing key information, ensuring in any case that access to the record of that Information remains available through other mechanisms; and

e) establishing the administrative sanctions corresponding to the head of the administrative unit of the subject entity in the event of a failure to fulfil these obligations.

**Article 6. Classes of key Information subject to proactive disclosure**

1. The following are the key classes of Information subject to proactive disclosure[8] by a subject entity:

A. General Information on the subject entity, including:

a) a detailed description of services provided directly to the public, including Information on their standards and service protocols, as well as procedures to be followed and formats to be used for obtaining said services;

b) a description of their organic structure, the location of their departments and offices, and hours of service to the public;

c) strategic programs and work plans, as applicable, as well as the outcomes, outputs and impacts obtained in the performance of their work;

d) file classification chart and the document arrangement catalogue or similar instruments.

e) simple but complete description of procedures to be followed for making requests for Information and filing appeals as well as complaints regarding actions or omissions of the subject entity;

f) relevant Information on the content of their publication schemes;

g) all laws, regulations, resolutions, policies, guidelines or manuals or other documents containing interpretations, practices or precedents regarding the subject entity's performance of its functions, that affect the general public;

h) reports that pursuant to legal provisions are generated in the performance of their powers, responsibilities or functions, broken down as much as possible;

[7] Comment: The Guarantor Body should verify that declassified Information becomes actively published Information.

[8] Comment: The publication of this Information must be organized by subject, in sequential or chronological order, without grouping, generalizing or modifying concepts, so that people can be informed correctly and without confusion.

i) description of their internal and external oversight, reporting and monitoring mechanisms, as well as their governance codes and the content of audit reports;

j) index of classified Information, as well as Information on the area responsible for that information;

k) index of Information classified as confidential; and

l) index of Information that has been recently declassified.

B. Information on public officials[9]

a) Information on the total number of officials, their names, the positions they hold and their place in the hierarchy, as well as their roles and duties, all broken down by gender and other categories relevant to the role of the subject entity, particularly with reference to higher level positions;

b) a detailed description of the powers and duties of the highest ranking officials, as well as the procedures they follow in adopting decisions;

c) salary scales corresponding to all categories of officials, including all components and sub-components of their salaries. This Information should be updated whenever there are position reclassifications, salary increases or changes in the method of payment;

d) salaries, including bonuses, risk premiums, compensation in cash and in kind, and all other income from any source,[10] including Information on the existing gender-based salary gap;

e) representation expenses and per-diems received;

f) sworn statements of interests and assets, or their equivalent;

g) names of officials who benefit from licenses, permits and concessions in general;

h) mechanisms for evaluation of Senior Officials;

i) calendars[11] of public officials who are in contact with the public;

j) invitations to compete for public positions and consulting assignments, as well as the result of those processes;

k) description of personnel selection and contracting procedures, regardless of the contract form.

[9] Comment: The following section applies to any public official understood as someone who receives Public Funds for his services, regardless of how hired and includes advisors and consultants.

[10] Comment: a record must be kept of donations that public servants may receive.

[11] Comment: Information related to private meetings in which public servants participate must be disclosed, whether their purpose is lobbying, the management of particular interests with respect to the decisions they make or any other purpose.

l) list of individuals or legal entities that for whatever reason are allowed to use public resources or carry out acts of authority, the amounts they utilize, the calls and criteria for their selection, as well as the reports that said persons submit on how those resources are used and allocated; and

m) list of public officials who have been subject to firm and/or final administrative sanctions, specifying the reason for the sanction and the provisions on which the sanction was based.

C. Financial Information

a) budget and spending plans corresponding to the current fiscal year as well as budgetary execution, breaking the information down by item, and indicating which specific projects and subsidies are intended to meet the needs of certain groups of society, including women;

b) year-end account statements corresponding to prior years;

c) description of procurement policies, guidelines and procedures, as well as contracts awarded;[12]

d) Information on public works projects and projects that use Public Funds, generated during the planning, award, contracting, execution, supervision and liquidation stages, as well as the evaluation of results;

e) Information on the beneficiaries of tax exemptions or tax incentives;

f) studies, analyses, statistics and other similar documents produced with financing from public resources;

g) financial management rules and control mechanisms;

h) audit and other reports, prepared by agencies responsible for the supervision of financial aspects, including the principal performance indicators on how the budget is executed as well as a summary of classified sections as applicable;

i) amounts assigned to expenses for any type of social communication and official publicity programs or campaigns, broken down by type of media, contract number and purpose;

j) a list of companies and persons that have breached contracts with the subject entity; and

k) Information on all outlays by the subject entity to publicize, promote, explain or defend a policy or decision.

D. Citizen Participation Mechanisms

a) description of mechanisms or general procedures for citizen participation; the forms of citizen participation that are binding and open government in nature; and mechanisms for social control, social comptrollership, social oversight or the like directed to promoting citizen participation in accountability and in combating corruption, with respect to both subject entities and guarantor bodies;

[12] Comment: To comply with this requirement, subject entities may make use of the OECD Council's "Recommendation on Fighting Bid Rigging in Public Procurement."

b) description of the results of the use and implementation of those mechanisms or procedures broken down by gender and age;

c) repository of all requests made by persons as well as the responses made to them, for which subject entities shall create, publish and maintain on their website as well as in the reception area of all their offices accessible to the public, a log of requests and disclosures of all documents disseminated in response to requests made in accordance with this Law; and

d) summary of all appeals, complaints or other actions filed by persons.

E. Needs of Specific Groups

a) relevant Information needed to promote greater gender equity[13] such as calculation of the salary gap, information on existing programs benefiting women, statistics or indicators related to labor inclusion, health, and other aspects.

b) relevant and necessary Information on social programs intended to meet the needs of other specific groups of society such as minors, seniors, afro-descendants, the lesbian, gay, bisexual, transgender and intersex (LGBTI) community and the members of indigenous community, as well as persons with disabilities.

c) detailed Information on indicators of progress and statistics that can be used to verify compliance in the implementation of gender equity, as well as on meeting the needs of other specific groups of society, including the impact generated for such groups.

d) list of subsidies granted to those sectors of society, broken down by group.

e) other indicators related to issues of social impact that, consistent with their functions, they should disseminate.

f) Information on the standards of human rights protection contained in international treaties, as well as recommendations, reports or resolutions issued by public agencies of the State or international organizations on the subject of human rights and the actions they have carried out for their implementation.

**Article 7. Responsibilities of the subject entity with regard to active transparency**

1. The subject entity should be sure to make available to those without Internet access a physical space with computer equipment and the assistance of qualified staff facilitating access to information in the entity's possession, custody or control.

2. Each subject entity shall appoint an Information Officer, who shall be responsible for complying with the active transparency requirement while adhering to the principles of gratuity, non-discrimination, timeliness, accessibility and integrity.[14]

[13] Comment: The Transparency and Access to Information Network prepared a report called "Diagnostic and Methodological Study for Incorporating the Gender Perspective in Transparency and Access to Information Policies in Latin America," which could be an important input for meeting this requirement.

[14] Comment: The gratuity principle is understood to mean the principle whereby obtaining and consulting Information should be free of cost, with requesters paying only the value, when applicable, of the materials used or shipping costs.

3. The Information Officer should ensure that the information disclosed on websites can be processed and is in selectable format,[15] meaning that data can be copied electronically for later use or processing.

4. The Information Officer shall ensure that all Information published is accompanied by the date of its latest update.

5. The Information Officer shall ensure updating, at least every (three months), unless another provision establishes a different period, of the key Information published by the subject entity, taking into consideration the production cycles of such Information.

6. The Information Officer shall ensure the annual creation and filing of a digital image of the website that contains all the key Information and information established in the publication scheme.

**Article 8. Publication schemes**

1. In addition to the key information established in Article 6, any subject entity may design, adopt and implement a publication scheme containing Information in its possession, control or custody to be disseminated proactively without any specific request.

2. When designing and implementing its publication scheme, the subject entity shall take into consideration the need to:

a) meet the citizens' most relevant needs for useful knowledge regarding that Information;

b) minimize the need for individuals to submit requests regarding the Information;

c) promote the gradual inclusion of Information, the periodic updating of these schemes, and their non-regression through the use of indicators of progress; and

d) promote equality of opportunities for all sectors of the population, through the inclusion in publication schemes of Information that is useful and relevant to their particular interests and needs, such as that relevant to minors, women, the elderly, afro-descendants, the LGBTI community, and members of indigenous communities, as well as persons with disabilities, ensuring that the latter are provided reasonable adjustments with regard to accessibility mechanisms.

3. Subject entities shall inform the Guarantor Body of their publication schemes and that body may, if it deems advisable, make appropriate recommendations that shall be binding in nature. The publication schemes shall be updated on a gradual and ongoing basis.

4. The Guarantor Body shall have the authority and competence to determine whether or not the Information contained in the publication schemes is subject to the exceptions regime.

---

The principle of non-discrimination is understood to mean that there should be no barriers to access to Information for all or any one of the reasons established in the Inter-American Convention against All Forms of Discrimination and Intolerance, adopted by the OAS in 2013.

The principle of timeliness is understood to mean that Information should be provided in the least amount of time possible, avoiding undue delays, through simple and expeditious procedures.

The principles of accessibility and integrity are understood to mean that the Information should be complete, comprehensible, useful, reliable, truthful and available in formats accessible through a simple and effective search system.

[15] Comment: *Selectable format* means a free format that allows the Information to be reused.

5. The Guarantor Body may approve model publication schemes for specific subject entities in order to harmonize such schemes, without prejudice to considering the particular characteristics and needs thereof.

### Article 9. Other laws and mechanisms

1. This Law does not affect the operation of any other legislation that:

   a) requires that the Information contained in Documents in the possession, custody or control of the subject entity be available to the public;

   b) allows anyone to access to the Documents in the possession, custody or control of the subject entity;

   c) requires the publication of Information concerning the operations of the subject entity.

2. Whenever anyone makes a request for Information pursuant to that law or administrative act, said request shall be processed in an equally favorable manner as if it had been made under this Law.

### Article 10. Previously disclosed Information

1. Subject entities shall, in the simplest way possible, guarantee and facilitate requesters' access to all previously disclosed records.

2. Requests for Information contained in logs of requests and disclosures shall be published without delay when that Information is in electronic format. If not, it shall be published no later than [three] business days following the submission of a request.

3. When the response to a request has been delivered in electronic format, it shall be made public immediately on the subject entity's website.

4. In the event the same Information is requested a second time, it shall be made public proactively on the subject entity's website, regardless of the format in which it is found.

## CHAPTER III. ACCESSING INFORMATION HELD BY PUBLIC AUTHORITIES

### Article 11. Request for Information

1. The request for Information may be filed in writing, by electronic means, verbally in person, by phone, or by any alternative means, with the relevant Information Officer. In all cases, the request shall be properly logged pursuant to Article 11.2 of this Law.

2. Unless the Information can be provided immediately, all requests shall be registered and assigned a tracking number, which shall be provided to the requester along with contact information for the Information Officer assigned to the request.

3. No fee shall be charged for making a request.

4. Requests for Information shall be registered in the order in which they are received and handled in a fair and non-discriminatory manner.

### Article 12. Requirements of requests for Information

1. A request for Information shall contain the following:

a) contact information for the receipt of notices and delivery of the Information requested;

b) a sufficiently precise description of the requested Information, in order to allow for it to be located; and

c) the preferred form in which the Information is to be provided.

2. In the event that the form in which the Information is to be provided is not specified, the requested Information shall be delivered in the most efficient and cost-effective manner for the Public Authority[16].

**Article 13. Interpretation of requests for Information**

1. The Public Authority in receipt of a request must reasonably interpret its scope and nature.

2 In the event that the receiving authority is uncertain as to the scope and nature of the requested Information, it must contact the requester for clarification. The receiving authority must make reasonable efforts to assist the requester in connection to the request, and respond accurately and completely.

**Article 14. Forwarding requests for Information**

1. If the receiving Public Authority reasonably determines that it is not the proper authority to handle the request, it must, as soon as possible and in any case within [five] working days, forward the request to the appropriate Public Authority for processing and notify the requester that his/her request has been routed to another Public Authority for processing.

3. The forwarding Public Authority must provide the requester with contact information for the Information Officer at the Public Authority where the request has been routed, in order to allow the requester to follow-up as needed.[17]

**Article 15. Third party response to notification**

Interested third parties shall be informed of the existence of a request for Information within [5] from the receipt thereof, and be given [10] days to make written representations to the receiving Public Authority either:

a) consenting to disclosure of the requested Information; or

b) stating the reasons why the Information should not be disclosed.

**Article 16. Cost of reproduction**

[16] Comment: The requester need not provide their name on the request for Information. However, insofar as the request concerns personal Information, the requester's name may be required.

[17] ALTERNATIVE: If the receiving Public Authority reasonably determines that it is not the proper authority to handle the request, it must, within the [five] business days following receipt of the request, identify the appropriate authority to the requester.

1. The requester shall only pay for the cost of reproduction of the requested Information and, if applicable, the cost of shipping, if so requested. Electronic delivery of Information shall be free of charge.

2. The cost of reproduction shall not exceed the actual cost of the material in which the Information is reproduced; cost of shipping shall not exceed the market value of same. For this purpose, the Guarantor Body shall periodically establish what they deem to be the fair market value.

3. The Public Authorities shall provide information free of all charges, including reproduction and shipping, for any low-income person as defined by the Guarantor Body.

4. The Guarantor Body will set additional rules regarding fees, which may include the possibility that the Information be provided free of charge if it is deemed to be in the public interest, or the possibility of setting a minimum number of pages to be delivered free of charge.

**Article 17. Display of Documents**

Public Authorities shall facilitate access to Documents by making the originals available for consultation in facilities suited for such purpose.

**Article 18. Information Officer**

1. The head of the Public Authority responsible for responding to requests must designate an Information Officer who shall be the focal point for implementing this law within said Public Authority. The contact information for each such Information Officer must be posted on the website of the Public Authority and made readily available to the public.

2. The Information Officer shall, in addition to any obligations specifically provided for in other sections of this Law, have the following:

a) to promote within the Public Authority the best possible practices in relation to the maintenance, archiving and disposal of Documents; and

b) to serve as a central contact within the Public Authority for receiving requests for Information, for assisting individuals seeking to obtain Information and for receiving individual complaints regarding the performance of the Public Authority in the disclosure of Information.

**Article 19. Document search**

Upon receipt of a request for Information, the Public Authority in receipt of the request must undertake a reasonable search for the Documents which best respond to the request.

**Article 20. Document management**

The [body responsible for archives] must develop, in coordination with the Guarantor Body, a Document management system which will be binding on all Public Authorities.

**Article 21. Missing Information**

When a Public Authority is unable to locate the Information responsive to a request, and records containing such Information should have been maintained, it shall be required to make reasonable efforts to gather the missing Information and deliver it to the requester.

**Article 22. Response period**

1. Each Public Authority must respond to a request for Information as soon as possible and in any event, within [twenty] working days of its receipt.

2. In the event that the request has been forwarded from one Public Authority to another, the effective date of receipt shall be that on which the appropriate authority received the forwarded request. In no event shall such date be greater than [ten] working days from the date in which the initial the request was first received by a Public Authority authorized to receive requests.

**Article 23. Extension**

1. Where a request for Information makes it necessary to search for or review a great deal of Documents, or the need to search offices physically separated from the receiving office, or the need to consult with other Public Authorities prior to reaching a determination on the disclosure of the requested Information, the Public Authority processing the request may extend the response time by up to an additional [twenty] business days.

2. In the event that the Public Authority fails to satisfy the request within [twenty] business days, or, if the conditions specified in paragraph 1 are met, the failure to respond to the request within [forty] business days shall be deemed a denial of the request.

3. In exceptional cases, involving large amounts of Information, the Public Authority may approach the Guarantor Body to request an extension greater than [forty] business days in order to respond to the request.

4. Where a Public Authority fails to meet the deadlines set forth in this article, no charge should be imposed for providing the Information. Furthermore, any Public Authority that fails to meet such deadlines must obtain prior authorization from the Guarantor Body to deny the Information or make a partial disclosure.

5. Under no circumstance may a third party notification excuse the Public Authority from complying with the terms and deadlines established in this law.

**Article 24. Notice to the requester**

1. As soon as the Public Authority has reasonable grounds to believe that satisfaction of a request will either incur reproduction charges in excess of the standards set by the Guarantor Body or take longer than [twenty] business days, it shall inform the requester and allow requester the opportunity to narrow or modify the scope of the request.

2. Public Authorities shall guarantee access to the Information in the form requested, unless this would:

a) harm the Document;

b) infringe on copyrights not held by Public Authority; or

c) be impractical because of the need to delete or redact some Information contained in the Document, pursuant to Chapter IV of this Law.

3. Where Information requested in electronic format is already available on the internet, the Public Authority may simply indicate the exact URL where the requester may access the Information.

4. Where the Information is requested in a non-electronic format, the Public Authority may not answer the request by making reference to a URL.

5. Where Information is provided to the requester, the latter shall be notified and informed of any applicable fees and/or arrangements for access.

6. In the event that all or part of the Information is withheld from a requester because it falls under the exceptions to disclosure under Chapter IV of this Law, the requester must be given:

a) a reasonable estimate of the volume of material that is being withheld;

b) a description of the precise provisions of this Law applied for the withholding; and

c) notification of the right to appeal.

## CHAPTER IV. EXCEPTIONS REGIME

### Article 25. Exceptions to disclosure

Subject entities may deny access to Public Information only under the assumptions considered in this chapter and under the following categories[18] of Information:

a) Reserved Information: that public Information that is temporarily excluded from public knowledge due to a clear, probable and specific risk of damage to public interests and in compliance with the requirements specified in this Law.

b) Confidential Information: that private Information held by subject entities to which public access is prohibited by constitutional or legal mandate due to a legally protected personal interest.

### Article 26. Supremacy of the public interest

No subject entity may refuse to indicate whether or not a Document is in its power or refuse to disclose such Document, in accordance with the exceptions contained in Articles 32 and 33 hereunder, unless the harm caused to the protected interest is greater than the public interest[19] of obtaining access to the Information.[20]

### Article 27. Human rights

[18] Comment: The list of exceptions should be exhaustive and not include any clause extending these categories to "all others that may be established by legislation."

[19] Comment: *Information of public interest* refers to Information that proves to be relevant or beneficial to society and not simply of individual interest, the disclosure of which is useful so that the public understands the activities carried out by the subject entities, such as information referring to public health, the environment, public safety, socioeconomic and political matters and transparency in public management. This definition takes up the points included in the decision of the European Court of Human Rights in the SIOUTIS v. GREECE case.

[20] Comment: Based on the principle of non-regression of public Information, a specific datum or Information of public interest that has already been disclosed in a specific format cannot cease to be made public based on a political decision.

1. The exceptions contained in Article 33 may not be applied in cases of serious violations of human rights[21] or crimes against humanity.

2. In these cases the authority competent to qualify these acts as violating human rights shall be [the Guarantor Body], at the request of the subject entities or any person.

3. The competent authority shall protect the right to privacy of victims and shall employ the methods it deems necessary for this purpose, such as redacting or other similar mechanism.

4. Information related to violations of human rights is subject to a high presumption of disclosure; in no case may it be classified by invoking reasons of national security.[22]

5. In States subject to transitional justice processes, wherein truth, justice, reparation and there are guarantees of non-repetition, the integrity of all Documents that contain such Information must be protected and preserved and the documents must be published immediately.[23]

**Article 28. Acts of corruption**

1. The exceptions contained in Articles 32 and 33 may not be invoked in the case of Information related to acts of corruption by public officials as defined by current laws and the Inter-American Convention against Corruption.

2. In these cases the authority competent to qualify the Information as related to acts of corruption shall be [the Guarantor Body] at the request of the subject entities or any person.

**Article 29. Entity responsible for classification**

1. The [supreme authority of subject entity] shall be responsible for classifying Information, except as provided in Articles 32 and 33.[24]

2. Only specifically authorized or designated officials may classify Information. When an official without this power feels that certain Information should be classified, that Information may be considered classified for a brief period of no more than [5] business days until the designated official has reviewed the recommendation on classification.

3. The identity of the person responsible for a decision on classification must be reachable or identified in the Document, so as to ensure adequate accountability.

4. Public officials designated by law may delegate their original classification power to as few hierarchical subordinates as is viable from an administrative point of view.[25]

---

[21] Comment: This connotation may be expanded to encompass cases wherein the violation has not yet been established but there is a well-founded presumption or imminent threat that it will occur.

[22] Comment: This article seeks to promote accountability for these violations, so that an effort is made to provide the victim with opportunities to gain access to effective reparations.

[23] Comment: There is a preponderant public interest with regard to disclosing Information to society as a whole on the human rights violations committed under the previous regime.

[24] Comment: A good practice is the creation of Transparency Committees, which may include the Information Officer, the heads of the Document management unit and the internal control body. Those committees meet periodically and their powers include the classification of information.

**Article 30. Generic classifications**

1. The classification of Information shall be an individual and case-based operation and subject entities shall not make generic classifications by law, decree, agreement or any other analogous instrument.

2. In no case may Information be classified before it has been generated.

**Article 31. Authority to declassify**

The Guarantor Body is empowered to order the declassification of information that does not meet the requirements set forth herein.

**Article 32. Confidential Information**

1. Subject entities may deny access to public Information when such access could harm the following private interests:

a) the right to privacy, including privacy related to life, health or safety, as well as the right to honor and to one's image;

b) personal data[26] that require the consent of their owner for their disclosure;

c) legitimate commercial and economic interests;[27] and

d) patents, copyrights and commercial secrets.

The public servants'[28] sphere of privacy is reduced according to their degree of responsibility. Consequently, public servants responsible for decision-making shall have a smaller sphere of privacy. Thus, in the event of conflict, the public interest shall prevail.

2. The exceptions in the preceding paragraph shall not apply when:

a) the individual has expressly consented to the disclosure of his personal data;

b) the circumstances of the case clearly indicate that the Information was delivered to the subject entity as part of the Information that should be subject to the disclosure regime;

c) the Information is found in public records or publicly accessed sources;

d) the Information is public in nature in accordance with this Law;

e) there is a judicial order [that seeks] and/or [authorizes its publication];

---

[25] Comment: It is considered good practice to publish the number of persons authorized to classify Information, and the number of persons who have access to classified Information.

[26] Comment: Subject entities shall disclose Information in accordance with the provisions of the *Statement of Principles for Privacy and Personal Data Protection in the Americas* adopted by the Inter-American Juridical Committee at its eightieth regular session, through resolution CJI/RES. 186 (LXXX/O-12).

[27] Comment: In cases where the Information on legitimate commercial and economic interests has been provided to the subject entity on a confidential basis, said Information shall remain exempt from disclosure.

[28] Comment: The personal data of public servants are public to the extent that such data relate to the exercise of the position or inherent to the public service provided.

f) its publication is required for reasons of national security and general safety;

g) when the Guarantor Body has ordered the declassification and disclosure of said Information;

h) when it is transmitted among subject entities and between them and the subjects of international law, in terms of treaties and inter-institutional agreements, provided the Information is used for the exercise of those entities' own powers.

3. These exceptions shall not be applicable with respect to matters related to the functions of public officials, or when more than [20] years have passed since the death of the individual in question.

4. The heads of subject entities shall have knowledge of and maintain a registry of the public servants who based on the nature of their powers have access to the files and Documents classified as confidential. In addition, they shall ensure that said public servants are knowledgeable about their responsibility in the handling of classified Information.

5. Confidential Information shall remain confidential indefinitely, unless is it declassified by the Guarantor Body, in the case of personal data and with the consent of their owner, or when expressly determined by law.

6. Once Information has been classified, the Guarantor Body is authorized and competent to verify whether the Information meets the requirements of classification; to fulfil this duty, it may view the Information. This power cannot be delegated.

**Article 33. Reserved Information**

1. Subject entities may deny access to public Information when there is a clear, probable and specific risk of significant harm. Reserved Information shall be that which:

a) disrupts the future free and frank provision of advice within and among the subject entities;

b) may undermine the conduct of international negotiations and relations;

c) imperils anyone's life, human dignity, safety or health;

d) contains opinions or recommendations that form part of the deliberative process of public servants, as long as a final decision has not been adopted;

e) affects due process rights or undermines the conduct of judicial cases or administrative procedures, as long as they have not been decided;

f) compromises the State's ability to manage the economy in the event of economic emergency decreed by law; and

g) might cause serious harm to the activities of verification, inspection, audit,[29] investigation,[30] prevention or prosecution of crimes.

2. The exceptions contained in paragraphs a) and g) shall not apply to facts, the analysis of facts, technical information and statistics.

3. The exception under paragraph g) shall not be applied to the results of a particular examination or audit, once they have been completed.

[29] Comment: Once they are completed, audits constitute key Information and their dissemination must be proactive, i.e., without need for any requests for Information.

[30] Comment: Information from completed investigations in cases that are not prosecuted shall be publicly accessible.

4. Subject entities may deny access to public Information when allowing access would constitute a violation of restricted official communications, including legal Information that should be considered privileged.

5. If a document contains parts that should be rated as classified, the subject entity shall prepare public versions, deleting what is not suitable for disclosure.

### Article 34. Defense and national security

1. The judicial branch, the legislative brand, chiefs of State and government, supervisory institutions, intelligence services, armed forces, police, and other security bodies may restrict the public's right to access Information when there are reasons of national security, but only when such restrictions comply with all the other provisions established in this Law, and the requested Information falls under one of the following categories:

a) Information on ongoing defense plans,[31] operations and issues of capacity during the period in which the Information has operational utility.[32]

b) Information on the production, capacities or use of weapons systems[33] and other military systems, including communications systems.[34]

c) Information on specific measures intended to safeguard the State's territory, critical infrastructure[35] or fundamental national institutions (*institutions essentielles*) against threats, use of force or sabotage, the effectiveness of which depends on restricting its disclosure.

d) Information intrinsic to or derived from intelligence services' operations, sources and methods, provided they concern matters related to national security.

e) Information related to matters of national security provided by a foreign State or intergovernmental agency with an express expectation of confidentiality and other diplomatic communications to the extent that they involve matters related to national security.

2. It is considered good practice for national legislation to establish an exclusive list of limited categories of information, such as the above.

### Article 35. Harm test

1. When in response to a request for Information, delivery thereof is denied on the grounds that the Information is reserved, the subject entity shall apply the harm test.

---

[31] Comment: Military operations that have already been carried out must be disclosed to third parties to ensure the right to the truth. In the event this Information has been destroyed, it shall be reconstructed by the competent authority.

[32] Comment: It should be understood that the phrase "during the period in which the Information is of operational utility" requires disclosing the Information once it is assumed that this does not mean revealing data that could be utilized by enemies to learn the State's ability to react, its capacities, its plans, etc.

[33] Comment: The States' maintenance and publication of a weapons control list is good practice encouraged by the Inter-American Convention on Transparency in Conventional Weapons Acquisition and the Arms Trade Treaty.

[34] Comment: Said Information includes data and technological innovations and Information on production, capacity and use. Information on budget items related to weapons and other military systems should be available to the public.

[35] Comment: "Critical infrastructure" refers to strategic resources, assets and systems, of such importance to the State that their destruction or incapacity would have a debilitating impact on national security.

2. The harm test must establish that the disclosure of Information may generate real, demonstrable and identifiable harm.[36]

In applying the harm test, the subject entity shall certify in writing that:

a) the disclosure of Information represents a real, demonstrable and identifiable risk of significant injury to a legally protected right clearly identified in a law. A hypothetical harm or injury may not be used as justification;[37]

b) the lack of a less harmful alternative to disclosure of the Information, to satisfy the public interest of disseminating the information;

c) the risk of harm that such disclosure would involve exceeds the public interest in the dissemination of the Information;

d) the limitation is consistent with the principle of proportionality[38] and represents the least restrictive means available for avoiding harm;

e) the restriction does not subvert the very essence of the right to Information; and

f) the concurrence of the requirements of timeliness, legality and reasonability.[39]

4. The subject entity shall in all cases indicate the specific legal provision on which it bases the reserve.[40]

---

[36] Comment: The criteria of real, demonstrable and identifiable harm should be understood as follows:
Real harm: The Information requested represents a real risk to the public interest; hypothetical harm cannot be used as a justification for secrecy.
Demonstrable harm: If said information were disclosed, it would entail greater damage to the public interest than if it were not provided.
Identifiable harm: The delivery of the Information would entail a greater impact on the parties involved in the events described above. Similarly, a public servant who improperly breaks the secrecy of proceedings or provides copy thereof or the Documents appearing in the investigation may be subject to an administrative or criminal liability procedure, as applicable.

[37] Comment: It is not enough for the subject entity to argue that there is a risk of harm; it must also provide specific and substantial reasons supporting its assertions. The issuance of certificates or another similar type of instrument by a minister or other official does not constitute sufficient arguments to demonstrate that a legal good is affected.

[38] Comment: Proportionality must be understood as the balance between harm and benefit to the public interest, so that the decision made represents a greater benefit than the harm it could cause to the population.

[39] Comment: The requirements of timeliness, legality and reasonability must be understood in the following context:

- *Timeliness*: the reserve should be established for a specific period of time so that the reserved Information does not lose its public nature and thus when the grounds for the reserve disappear, the Information must be disseminated without restriction;
- *Legality*: the subject entity must conduct an analysis of the existing legal framework and demonstrate that the limits on the exercise of the right of access to public Information are aimed at protecting rights of similar or greater importance. In other words, it must prove that the requested Information falls under one of the grounds for exception provided in this Law; and
- *Reasonability*: it is not enough for the subject entity to cite legislation that authorizes it to deny the information because it considers it reserved. It must also justify the adoption of a limitation and provide a basis for the classification. This will reduce arbitrary action by public servants who have the power to classify information and will avoid unjustified denials of access to the Information.

## Article 36. Public Interest Test

1. When invoking the existence of grounds for confidentiality in response to a request for Information, the subject entity shall apply the public interest test.

2. The public interest test should be performed based on the elements of suitability, necessity and proportionality, when there is a collision of rights.

For these purposes, the following definitions shall apply:

a) suitability: the legitimacy of the right adopted as prevailing. This must be appropriate to achieve a constitutionally valid purpose or suitable for achieving the intended purpose;

b) necessity: the lack of less harmful alternatives for opening up the Information to satisfy a public interest.

c) proportionality: the balance between the harm and benefit to the protected public interest, such that the decision represents a greater benefit to the population than the harm potentially caused by the disclosure and dissemination of the Information.

## Article 37. Generalities of classification

Classification may be established partially or completely according to the content of the Information, and shall be consistent with the principles and provisions set forth in this Law.[41]

## Article 38. Classification of Information

1. Prior to their adoption, the rules and procedures governing the classification of Information should be subject to a process of open consultation wherein people have the opportunity to express their proposals and observations.

2. The rules and procedures approved to govern classification must be broadly disseminated.

3. When the information has parts or sections that are reserved or confidential, in order to handle a request for Information, subject entities shall develop a public version in which classified parts or sections are redacted, providing a generic indication of their content and supporting and justifying their classification.

## Article 39. Declaration of confidentiality

1. Confidential Information shall be classified in accordance with the public interest test.

2. The confidential nature of the Information held by subject entities shall be declared through an administrative action that should contain the following Information at a minimum:

---

[40] Comment: In view of the burden of proof that Public Authorities have when reserved information, it is advisable to adopt rules (laws, regulations, guidelines, guides, agreements, etc.) that facilitate and specify the manner in which the harm test will be conducted, in that, on the one hand, Public Authorities would have a detailed procedure for its application and, on the other hand, individuals would have certainty regarding the elements that must be present in the reserve.

[41] Comment: Subject entities may only classify Information that exists; classification may not predate the existence of the Information.

a) date of the administrative classification action: corresponds to the date when the declaration of confidentiality was issued;

b) administrative office: the office that according to the of the subject entity's organizational chart generated or holds the confidential Information.

c) Information to be classified: individualized Information classified as confidential; indicating the case number, document, file, official letter, level, report, etc.

d) persons or agencies authorized to access that Information, preserving the confidential nature thereof, if any.

e) legal foundation: provisions of Article 32 supporting the classification.

f) justification: subject entities shall provide the motive for the classification being made, i.e., they shall specify the special reasons or circumstances that led them to conclude that the particular case falls within the assumptions provided in the Law.

g) signature of the public servant who authorizes the classification: act of the senior authority of the subject entity, of the person acting by delegation or, as applicable, the Information officer.

3. Confidential information[42] shall be labeled with the word "CONFIDENTIAL,"[43] which shall be placed in a spot visible to anyone who accesses it.

**Article 40. Declaration of reserve**

1. Information shall be classified as reserved on a case by case analysis, through the application of a harm test.

2. At the time the Information is classified, a resolution declaring the reserve must be issued, which indicates:

a) the subject entity that produced the Information;

b) the date or the event to which the reserve refers;

c) the authority that adopted the decision to reserve the Information;

d) persons authorized to access that Information;

e) distinction between the portions of the Information that are subject to confidentiality or reserve and those that are available for access by the public; and

f) the duration of the reserve.

**Article 41. Declassification of Information**

[42] Comment: If the declaration of confidentiality covers the entire Document, there will be no need to identify its individual components. If only some of its component sections are classified as confidential, that circumstance shall be noted in the declaration of confidentiality.

[43] Comment: In any case, based on the type of confidential Information involved, the subject entities may establish special labeling systems the meaning of which is comprehensible only to those who have authorized access, making identification difficult for anyone else.

Information classified as reserved shall be public when:

a) the causes that led to their classification cease to exist;

b) the classification period expires;

c) there is a resolution of the Guarantor Body or the judiciary that determines the existence of a public interest reason that prevails over the reserve of the Information; and

d) the senior authority of the corresponding administrative unit of the subject entity considers declassification appropriate, in accordance with the provisions of this Law.

**Article 42. Revision of the exceptions regime**

The Guarantor Body shall periodically revise the list of exceptions established in this Law and recommend to the Legislative Branch the exclusion of those matters that no longer merit the nature of secret or confidential information or that for other reasons it feels should be excluded as grounds for secrecy or confidentiality.[44]

**Article 43. Registry of classified Information**

1. Subject entities shall, through their Information officers, submit to the Guarantor Body every six months an index of information classified as reserved or confidential.

2. The Guarantor Body shall publish that Information in open formats on the day following its receipt. Said index shall indicate the area that generated the Information, the name of the Document, the type of classification, whether a complete or partial classification is involved, the date when classification begins and ends, its justification and, as applicable, the sections of the Information that are classified and whether an extension is in effect. In no case may the index itself be considered as classified Information.

**Article 44. Partial disclosure**

In those circumstances in which not all the information in a Document is exempt from disclosure in accordance with the exemptions indicated in Article 33, an edited version of the Document must be prepared redacting only the portions of the Document that are subject to exception. The non-exempt Information shall be made public and delivered to the requester.

The subject entity shall make a note on the Document stating the reasons why certain Information has been suppressed.

**Article 45. Maximum duration of reserve**

1. The exceptions referred to in Article 303 are not applicable to a Document that is more than [5] years old. When a subject entity wants to reserve the Information, this duration may be extended for another [5 years] with the approval of the Guarantor Body. The duration of the reserve shall start on the date when the Information is first classified.[45]

[44] Comment: this Information may be submitted in the annual report that the Guarantor Body presents to the Legislative Branch.

[45] Comment: The standard ISO15489 on Document management establishes that the assessment process falls to the producer of the information, which shall determine the period of secrecy of the Information.

2. Under exceptional circumstances, when in the judgment of the subject entity it is necessary to again extend the period of reserve of the Information, a duly founded and justified request shall be made to the corresponding Guarantor Body, applying the harm test and indicating the new period of reserve, at least three months prior to expiration of the original term.

3. Within no more than [7] business days, the Guarantor Body shall issue a resolution in which it may extend, modify or deny the requested period of reserve. The Information will continue to be reserved until the Guarantor Body makes a decision.

4. No type of Information may be reserved indefinitely.

5. In no event may the total period of secrecy exceed [10] years, including any extensions.

**Article 46. Non-Existent Information**

1. The subject entity may not refuse to deliver Information by unjustifiably alleging that it does not exist. The declaration that Information does not exist must always be proven and preceded by a properly documented search process in different administrative units.

2. The existence of Information is presumed when it pertains to the authority, duties and functions that the domestic legal framework grants to the subject entities, or to the commitments undertaken by the State at the international level.

3. Where certain powers, responsibilities or functions have not been exercised, the response must be justified based on the grounds supporting the inexistence of the Information.

4. If the requested Information is not found in the files because there is no obligation to generate it, this shall not be considered to mean that it doesn't exist but rather a lack of legal authority.

5. When declaring that the requested Information is inexistent, the subject entity shall assure the requester that it used an exhaustive search criterion, which it shall describe in its response to the requester, in addition to indicating the circumstances of time, manner and place that led to the inexistence of the Information.

6. The subject entity must duly prove the facts if the Information does not exist due to natural disasters, the commission of some crime, or if its elimination was authorized negligently or illegally. In all these cases, if the Information is of public interest, the subject entity shall do everything possible to reconstruct it.

7. The senior authority of the corresponding administrative unit shall be immediately informed of cases in which the institution for which it is responsible denies public Information by alleging the inexistence thereof, including the identification of the person or public official responsible for keeping the Information. The senior authority of the administrative unit shall in these cases:

a) analyze the case and take the necessary measures to locate the Information;

b) issue a resolution confirming that the Information does not exist;

c) ensure, provided this is materially possible, that the Information is generated or replaced (when it should exist) to the extent possible based on its powers, responsibilities or functions. With prior verification of the inability to generate the Information, there should be a well-founded and

reasoned exposition of the reasons why, in the specific case, it did not exercise those powers, responsibilities or functions, which shall be communicated to the requester; and

d) immediately notify the supervisor of the subject entity and the Guarantor Body, the internal control body or the equivalent which, as applicable, shall initiate the administrative liability or other appropriate procedure.

8. The Guarantor Body is responsible for verifying that the information does not exist by means of:

a) an on-site examination of the institutional files of the subject entity that declared the inexistence of the Information, to determine whether the Information search procedures were properly executed and confirm whether or not the Information actually exists;

b) half-yearly requests to all subject entities of cases in which Information has been denied by alleging its inexistence. Said data shall be disclosed in the annual report referred to in Article 66; and

c) requesting the responsible administrative unit to prepare a declaration of inexistence, in which the search actions are detailed.

**Article 47. Filing of appeals**

1. Anyone has the right to appeal the subject entity's decision not to deliver the requested Information by alleging one of the grounds contained in the exceptions regime.

2. This right includes the ability to challenge the declaration of reserve, made by a subject entity, before the Guarantor Body through the appeal procedure established in Chapter V of this Law.

**Article 48. Recourse against a failure to respond**

1. When the requester does not obtain a response in the established period, said requester may file a complaint with the Guarantor Body.

2. The complaint must be filed within [thirty] business days from the date in which a response should have been received by the requester; otherwise, the complaint may be rejected.

3. The Guarantor Body shall verify within a period of [five] business days whether the request for Information to the subject entity complies with the requirements of Article 12. If it does, the Governing Body shall admit the case and allow a period of [three] business days for the subject entity to justify the reasons why it did not provide a timely response to the request.

4. Once the period for the subject entity to justify its non-responsiveness has elapsed, the Guarantor Body shall verify, within [ten] business days, whether or not the requested Information is reserved or confidential. If the information is open for public access, the Guarantor Body shall issue a resolution ordering that the requester be given access to the Information.

**Article 49. Other laws**

The provisions on reserve or confidentiality of Information contained in other laws shall be consistent with the bases, principles and provisions established herein and may in no event contravene this Law.

In the event that other laws prescribe longer classification periods, those set forth in this Law shall prevail.

## CHAPTER V. APPEALS

### Article 50. Internal appeal[46]

1. A requester may file an internal appeal with the head of the Public Authority within [60] business days from the date in which the term for obtaining a response has expired, or from the date of any other breach of the rules set forth in this Law for responding to a request for Information.

2. The head of the Public Authority must issue a written and sufficiently reasoned decision within [10] business days from receipt of the notice of appeal, and deliver a copy of said decision to the requester.

3. Should the requester decide to file an internal appeal, the full term for resolution thereof must expire before an external appeal may be pursued.

### Article 51. External appeal

1. Any requester who believes that his or her request for Information has not been processed in accordance with the provisions of this Law, shall have the right to file an appeal with the Guarantor Body regardless of whether an internal appeal has been pursued.

2. Said appeal shall be filed within no more than [60] business days from the expiration of the terms for responding to a request for Information or to an internal appeal, as provided by this Law.

3. The request for an appeal shall contain:

a) the public authority with which the request was filed;

b) the contact information of the requester;

c) the grounds upon which the appeal is based; and

d) any other information that the requester considers relevant.

4. Upon receiving an appeal, the Guarantor Body may attempt to mediate between the parties with an aim to disclose the Information without exhausting a formal appeal process.

5. The Guarantor Body shall log the appeal in a centralized tracking system and inform all interested parties, including interested third parties, about the appeal and their right to participate in such process.

6. The Guarantor Body shall set clear and nondiscriminatory rules regarding the processing of appeals which ensure that all parties have an appropriate opportunity to appear in the process.

7. In the event the Guarantor Body is uncertain as to the scope and/or nature of a request and/or appeal, it must contact the appellant to clarify what is being requested and/or appealed.

[46] Comment: An internal appeal should not be mandatory, but instead optional for the requester before proceeding to the external appeals process.

### Article 52. Resolution

1. The Guarantor Body shall decide appeals, including attempts to mediate, within [60] business days and may, in exceptional circumstances, extend this timeline by another [60] business days.

2. In deciding the case, the Guarantor Body may:

a) deny the appeal; or

b) require the Public authority to take such steps as may be necessary to comply with its obligations under this Law, such as, but not limited to, providing the Information and/or reducing the fee;

3. The Guarantor Body shall serve notice of its decision to the requester, the Public Authority and any interested party. Where the decision is unfavorable to the requester, the latter shall be informed of the right to appeal.

4. If a Public Authority does not comply with the Guarantor Body's decision within the time frame set forth in said decision, the Guarantor Body or the requester may file petition the [appropriate] court to compel compliance therewith[47].

### Article 53. Judicial review[48]

1. A requester may file a case with the court only to challenge a decision of the Guarantor Body, within [60] days of notice of the adverse decision or the expiration of the term for responses provided herein.

2. The court shall come to a final decision on all procedural and substantive aspects of the case as early as possible.

### Article 54. Burden of Proof

1. The Public Authority shall have the burden of proof to establish that the requested Information is subject to one of the exceptions contained in Articles 32 and 33 above. In particular, the Public Authority must establish:

a) that the exception is legitimate and strictly necessary in a democratic society based on the standards and jurisprudence of the Inter-American System;

b) that disclosure of the Information would cause substantial harm to an interest protected by this Law; and

c) that the likelihood and gravity of that harm outweighs the public interest in disclosure of the Information.

## CHAPTER VI. GUARANTOR BODY

[47] Comment: The manner of enforcing the Guarantor Body's decisions in accordance with paragraph 4 will vary from country to country.

[48] Comment: These rules are based on the assumption that in many countries courts have all of the inherent powers needed to process these types of cases, including for example imposing sanctions on Public Authorities. Where this is not the case, these powers may need to be explicitly given to them through the access to public Information law.

### Article 55. Creation[49]

This Law creates a Guarantor Body that will promote and guarantee the right of access to public Information as well as the faithful implementation and interpretation of this Law.

### Article 56. Characteristics[50]

1. The Guarantor Body[51] shall be a body that has its own legal personality and is:
   a) established by law.
   b) autonomous and independent, with the ability to decide on the execution of its budget.
   c) specialized and impartial.
   d) authorized to impose penalties, within its areas of competence.

### Article 57. Composition

1. The Guarantor Body shall be composed of (five or more) commissioners.[52]

2. The Guarantor Body should reflect a diversity of experience and talent, as well as gender parity.

### Article 58. Requirements to be a commissioner

Commissioners must meet the following minimum requirements:

a) be a citizen in full possession of the inherent political and civil rights;
b) have knowledge and proven experience in the field covered by this Law, in order to ensure independent judgment and impartiality;
c) have a good reputation, not have been convicted of a crime involving fraud or dishonesty in the

[49] Note: Model Law 1.0 had an *Information Commission*; Model Law 2.0 considers it necessary to replace it with a newly created and more evolved *Guarantor Body*.

[50] Note: unlike Model Law 1.0, an article is created detailing the essential and non-essential characteristics with which the Guarantor Body must be created.

[51] Comment: Each State may consider the Guarantor Body to be preferably:

i) established at the constitutional level;

ii) not subordinated to any branch, body, or institution of government;

iii) collegiate, or with accountability mechanisms;

iv) independent of local transparency bodies, in the case of Federal States.

[52] Comment: It is preferable that Guarantor Bodies be composed of an odd number of commissioners greater than or equal to five (5), since a body composed of three (3) may isolate or obstruct the opinion and participation of one of the commissioners in cases where the other two are closely aligned philosophically, personally, or politically—a dynamic that is less likely to arise in a collegial body of five or more members.

Each State may consider the possibility of selecting alternate commissioners. Alternate commissioners may be those who, while not having been chosen during the selection process, have nonetheless obtained the best scores. In any case, it must be ensured that the absence/vacancy of a commissioner does not hinder the operation of the Guarantor Body.

past five years, and not have been convicted of corrupt acts as defined in the Inter-American Convention against Corruption and under domestic law.

### Article 59. Selection procedure

Commissioners shall be nominated by a majority of [two-thirds] of the members of the [Legislative Branch] and appointed by the [Executive Branch], in a process that adheres to the following principles:

a) public participation in the nomination process;

b) transparency and openness; and

c) publicity of the list of candidates considered most suitable for the position.[53]

### Article 60. Obligations of commissioners

1. Commissioners shall perform their duties on a full-time basis.

2. Commissioners may not hold any other employment, position, or commission except in academic, scientific, or philanthropic institutions.[54]

### Article 61. Term of office

1. The term of office of the commissioners shall be [5] years, renewable for a single additional term.

2. The election of commissioners must be alternated and held at staggered intervals, in order to prevent the mandate of more than two thirds of its members from expiring in the same year and to ensure the continuity of service, as well as to guarantee the autonomy and political independence of the Guarantor Body.

3. Commissioners shall remain in office until their replacements are elected.[55]

### Article 62. Removal or suspension of commissioners

1. Commissioners may only be removed or suspended from office following a process that is similar in nature to that by which they were appointed or for a situation that warrants removal from office, including:

a) a final judgment of conviction for a criminal offense or punishment for violating ethical standards of conduct;

b) infirmity that directly affects the individual's capacity to discharge his or her duties;

---

[53] Comment: In order to increase confidence in the institution, it is preferable that both the Executive and the Legislative Branches participate in the selection process; that any decision of the Legislative Branch be adopted by a qualified majority sufficient to guarantee bipartisan or multi-partisan support (e.g., 60 percent or 2/3); that the public and civil society have the opportunity to participate in the nomination process; and that the process be transparent. There are two main approaches: appointment by the Executive Branch, with the nomination and approval of the Legislative Branch; and appointment by the Legislative Branch, with the nomination or approval of the Executive Branch.

[54] Comment: It is recommended that commissioners serve on a full-time basis and that their salary be tied to an externally fixed sum in order to strengthen their independence.

[55] Comment: It is recommended that commissioners hold office for no longer than 12 years, including any re-election.

c) serious constitutional violations or breaches of this Law, or the mismanagement of Public Funds and resources;

d) refusal to comply with any of the disclosure requirements inherent to their position, such as the public disclosure of salary or benefits; and

e) negligent or bad faith disclosure or use of sensitive or confidential Information.

2. Any commissioner who has been removed or suspended from office has the right to appeal such removal or suspension to the Judicial Branch.

**Article 63. Duties and powers of the Guarantor Body[56]**

The Guarantor Body shall have all the powers necessary to perform the functions described in this Law, including the following:

I. Interpretation of the Law:

a) interpret this Law and ensure that its correct interpretation by subject entities.

II. Implementation of the law:

a) monitor and ensure *ex officio* compliance with this Law;

b) support Public Authorities in the implementation of this Law; and

c) implement a set of indicators to measure the proper application of this Law.

III. Regulations:

a) propose legislative initiatives in the area of its competence;

b) make recommendations on existing and proposed legislation in the area of its competence;

c) propose, coordinate, or, where appropriate, approve the Regulations to the Law on Access to Public Information and the internal rules necessary for the proper performance of its duties, including the design of its organizational structure; and

d) draft guidelines for the handling of public, confidential, and classified Information in the possession of subject entities.

IV. Information asset registers:

a) keep a record of requests for access to Information, responses, results, and costs of reproduction and delivery.

V. Direct internal policies:

a) provide guidance to subject entities in the design, implementation, and assessment of actions to disseminate public Information; and

b) promote the homogeneity and standardization of Information disseminated by the subject entities, through the adoption of guidelines, templates, and any means deemed appropriate.

VI. Digitalization of Information and information and communication technologies:

[56] Note: Unlike Model Law 1.0, Model Law 2.0 includes a list detailing the duties and powers of the Guarantor Body.

a) promote and guide the digitalization of public Information in the possession of subject entities as well as the use of modern and adaptable information and communication technologies.

VII. Open data:

a) ensure that key Information is increasingly disclosed in an open data format; and

b) provide technical support to reporting entities in the preparation and dissemination of Information in an open data format.

VIII. Orders:

a) issue binding decisions and orders; and

b) disclose the orders issued, particularly among the subject entities, in order to standardize the enforcement of this Law.

IX. Requests for Information:

a) promote the development and implementation by the subject entities of a modern computer system for the intake of requests through a single window; and

b) prepare forms for the submission of requests for information, which are not binding but will serve as a general guide for regulated entities and will contain the requirements established in [Article 23 of Law 1.0].

X. Dispute resolution:

a) resolve disputes relating to the classification and declassification of classified or confidential information, applying the principle of maximum openness; and

b) create and offer free and expeditious mechanisms for the resolution of disputes that may arise between subject entities and Information requesters, and mediate and/or adjudicate such disputes.

XI. National security:

a) request the cooperation of institutions in the national security and defense sector to obtain technical inputs to ensure the appropriate declassification of Information.

XII. Inspections and investigations:

a) in the context of a proceeding, to summon individuals, request searches, and receive the sworn testimony of persons deemed to be in possession of Information relevant to the performance of their functions;

b) verify and review public Information in the possession of any subject entity, through on-site inspections. This Information may include classified or confidential Information;

c) these proceedings include, *inter alia*, the supervision and observation of the request intake system of the subject entities in order to verify that they adequately respond to requests for Information; and

d) issue the appropriate preventive/precautionary measures by means of a reasoned order, *inter alia*, to request a copy of the Information in dispute, regardless of its classification; notify the offender's supervisor of the alleged conduct and the existence of the proceeding before the Guarantor Body; and request that the head of the regulated entity take special measures to safeguard and back up the Information in question.

XIII. Compliance lists:

a) adopt the necessary guidelines for monitoring compliance with this Law, including the periodic publication of the list of subject entities that comply/fail to comply with the provisions of this Law, including the incorporation of a gender perspective; and

c) publish a list identifying the subject entities against which the highest number of complaints was received.

XIV. Reports of violations:

a) refer cases of suspected administrative or criminal misconduct to the competent bodies.

XV. Penalties and enforcement measures:

a) establish and carry out enforcement measures, including public and private reprimands, fines, and others.

XVI. Legal Recourse:

a) serve as a second instance for persons who are dissatisfied with the resolutions of the subject entities;

b) in the case of Federated States, serve as a second instance in the event of denial by local bodies;

c) resolve individual complaints, which may be filed at any time under the legally established guidelines and procedures;

d) hold oral and public hearings to determine the classification or declassification of Information, as appropriate;

e) call witnesses and produce evidence in the context of an appeal; and

f) as the result of an appeal, the Guarantor Body may, *inter alia*, order the declassification of Information and consequently its release.

XVII. Training:

a) promote and implement training and awareness programs directed at subject entities, in particular public servants, and provide any technical support they may require on matters within their competence.

XVIII. Public awareness:

a) hold workshops, conferences, seminars, and other similar activities to publicize the importance of the right of access to public Information as a tool to ensure transparency;

b) sign cooperation agreements with all kinds of public and private organizations that promote access to public Information; and

c) disseminate this Law and promote its understanding among the general public through the publication and dissemination of guides and other similar resources on the relevance of the right of access to Information and its practical application, taking into account accessibility criteria for groups in situations of vulnerability.

XIX. Constitutional challenges:

a) bring unconstitutionality actions in matters within its competence to challenge federal or state laws as well as international treaties signed by the Executive Branch and ratified by the Legislative Branch that violate the right of access to public Information.

XX) International conventions:

a) ensure compliance with the obligations undertaken by the State in international conventions, specifically regarding access to public Information, including the Inter-American Convention against Corruption and the United Nations Convention against Corruption.

XXI. Coordination with national archives:

a) cooperate with the entity in charge of the national archives in the creation and use of the criteria for cataloguing and conserving Documents, in the organization of the archives of the agencies and entities subject to this Law, as well as in other areas of mutual interest.

### Article 64. Budget[57]

1. The Legislative Branch must approve the budget of the Guarantor Body, which must be sufficient for it to properly discharge its duties.

2. The creation of new bodies shall guarantee the provision of sufficient human, budgetary, and material resources for them to perform their duties, as this is the only way to guarantee sufficient conditions for the proper application of this Law.

### Article 65. Reports of subject entities [58]

1. Subject entities shall submit annual reports to the Guarantor Body detailing the activities they carry out to comply with this Law. This report shall include, at a minimum, information on:

a) number of requests for Information received, granted in whole or in part, and of requests denied, disaggregated by gender where possible, as well as any other Information related to indigenous groups, economically disadvantaged persons, women, persons with disabilities, Afro-descendants, and others, for purposes of evaluating the implementation of this Law. In order to collect this Information, reporting entities may use Information request forms[59] with minimum fields to be completed by the requesters;

b) number of requests responded extemporaneously, including justification for any delay;

c) details of the sections of this Law that were invoked to deny, in whole or in part, requests for Information and the frequency with which they were invoked;

d) response time to requests for Information;

e) number of appeals filed to contest the denial of Information, disaggregated by gender;

f) fees charged for the reproduction and delivery of the requested Information;

g) activities undertaken to meet the obligation to disclose key Information and those undertaken to implement the open State policy;

h) activities carried out to implement proper document management;

i) activities to provide training and education to public servants; and

j) gender-disaggregated statistics and information demonstrating compliance with this Law.

---

[57] Note: Model Law 2.0 introduces a specific article on the budget of the Guarantor Body.

[58] Note: Model Law 2.0 details the information that both the report of the Guarantor Body and the report of the subject entities should contain.

[59] Comment: The omission of the requirement to complete the information request forms shall not be grounds for invalidating such request.

k) difficulties observed in complying with the Law.

2. The Guarantor Body may gradually expand the above list as it deems advisable to verify compliance by the subject entities with the provisions of this Law. To this end, the Guarantor Body will issue the guidelines it deems necessary.

**Article 66. Reports of the Guarantor Body**

The Guarantor Body shall publish annual reports on its activities and on the implementation of the Law. Said report shall include at least the following:

a) a systematized summary of the Information received from subject entities in compliance with this Law;

b) the number of appeals filed, disaggregated by gendered including those from the various public authorities, their grounds, results, and status;

c) number of penalty proceedings filed and their current status;

d) list of public servants penalized for failure to comply with this Law; and

e) disaggregated statistical Information that makes it possible to identify and define inequalities that require the adoption of differentiated measures and the measures and proposals that will be undertaken in order to narrow the gaps between different sectors of society. Criminal and Civil Responsibility

**Article 67. Civil and criminal liability**

1. No one shall be subjected to civil or criminal action, or to any employment detriment, for any action taken in good faith in the exercise, performance or purported performance of any power or duty in terms of this Law, as long as they acted reasonably and in good faith.

2. It is a criminal offense to willfully destroy or alter Documents after they have been the subject of a request for Information.

**Article 68. Administrative offenses**

1. It is an administrative offense to willfully:

a) obstruct access to any Document in contravention of Chapter II of this Law;

b) prevent the performance by a Public Authority of its duty under Chapters II and III of this Law;

c) interfere with the work of the Guarantor Body;

d) fail to comply with provisions of this Law;

e) fail to create a Document either in breach of applicable regulations and policies or with the intent to obstruct access to Information; and

f) destroy Document without authorization.

2. Anyone may make a complaint about an administrative offense as defined above.

3. Administrative sanctions shall be governed vt the administrative law of the State and may include a fine [of up to x times the minimum wage], a suspension of a period for [x] months/years, termination, or a separation or restriction from service for [x] months/years].

4. Any sanctions ordered shall be posted on the website of the Guarantor Body and the respective Public Authority within five days of the imposition thereof.

## CHAPTER VII. PROMOTIONAL AND COMPLIANCE MEASURES

### Article 69. Monitoring and compliance

1. The [legislative body] should regularly monitor the operation of this Law, in order to determine whether changes and improvements are necessary to ensure all Public Authorities comply with the text and spirit of the Law, and to ensure that the government is transparent, remains open and accessible to its citizens, and guarantee the fundamental right of access to Information.

### Article 70. Training

1. The Information Officer shall ensure the provision of appropriate training for the officials of the Public Authority on the application of this Law.

2. The guarantor Body shall assist Public Authorities in providing training to officials on the application of this law.

### Article 71. Formal Education

1. The [Ministry of Education] shall ensure that core education modules on the right to Information are provided to students in each year of primary and secondary education.

## CHAPTER VIII. TRANSITORY PROVISIONS

### Article 72. Abbreviated title and entry into force

1. This Law may be cited as the Access to Public Information Law of [year].

2. This Law shall be effective on the date of its promulgation by [insert name of relevant official such as President, Prime Minister], regardless of which it shall become effective automatically [six] months after its approval in the absence of a promulgation.

3. The Guarantor Body shall have up to 6 months from the date in which this Law becomes effective to appoint its personnel, establish its internal processes, disseminate information proactively and carry out any other action needed for its full operation.

### Article 73. Regulations

1. This Law must be properly regulated within [1] year of its entry into force, with active involvement of the Guarantor Body.

****

ADDENDUM A: MODEL INTER-AMERICAN LAW ON DOCUMENT MANAGEMENT

ADDENDUM B: IMPLEMENTATION GUIDE FOR THE MODEL INTER-AMERICAN LAW ON DOCUMENT MANAGEMENT

# MODEL INTER-AMERICAN LAW ON DOCUMENT MANAGEMENT

## INTRODUCTION AND PURPOSE

Document management and file administration in government entities are some of the most important aspects for the effective implementation of a country's law on access to information and transparency. The inability to locate the information may become an obstacle in managing information requests, while inappropriate file management may delay compilation of requested information.

Therefore, it is fundamental to ensure that Document and file management policy is consistent with policies on information access policies, transparency, open government, and open data.

The success of transparency and access to public information initiatives depends 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, adequate archive management controls with effective standards and procedures, allow members of the public and public officials to trust not only 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. These Documents constitute a legacy 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.

Said Documents contain information that constitutes a valuable resource and an important asset for the subject entity. They are important not only 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. Therein lies the importance of a standardized Document management policies and procedures that ensures that they are accorded the proper attention and protection, while enabling their probative value and information content to be preserved and retrieved more efficiently and effectively through the use of standard practices and processes based on good practice.

Document and archive management is a crosscutting process in all institutions, making it an integral part of all the processes carried out in an institution's different areas. 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.

## MODEL INTER-AMERICAN LAW ON DOCUMENT MANAGEMENT

### CHAPTER 1. DOCUMENT MANAGEMENT POLICY

### Article 1. Documents and files

1. In the context of this law, "Document" shall mean any written information, regardless of its form, origin, date of creation, or official nature; whether or not it was created by the obligated entity that has possession of it; whether or not it is classified as confidential, and regardless of its medium or technology platform.

2. For the purposes of this law, "Archive service" means the service responsible for the functions of Document management, conservation, and administration.

3. Documents and Archive Services must be properly organized and well managed to ensure the quality and integrity of public information, as well as to meet established response times to the public and the subject entity itself.

4. Documents and archives must be managed with adequate controls and standards, as well as with effective procedures, so that members of the public and public officials alike 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 the subject entities.

### Article 2. Implementation of Document management policy

1. Every obligated entity shall define a Document and archive management policy as a declaration of intent that includes lines of action and objectives that it wishes to achieve as an institution in relation to the Documents that it produces or receives in the performance of its functions and activities.

   Comment: *The implementation of a Document management policy at the core of institutions is a democratic obligation of our administrations that should be aligned with other high-level strategic policy goals, such as transparency, access to public information, good governance, and accountability, since Documents constitute the basis and foundation of open government as well as underpinning the principles of transparency, civic participation, and partnership.*

2. The Document and archive management policy will govern the practices of those responsible for their management and of anyone else who generates or uses Documents in the course of their activities, including:

a. Establishment of standards and good practices.

b. Design of procedures and deadlines.

c. Provision of services related to their management and use.

d. Integration of the Document management system with the systems and processes of the obligated entity or institution.

e. Oversight and audit for accountability.

### Article 3. Appointment of an authority to lead the management policy

1. All regulated entities shall establish a unit or agency for the formulation and leadership of Document management policy, which will guarantee that Document management decisions, actions, and activities conform to the legal framework and are duly Documented.
2. The senior management of the obligated entity must appoint a specific representative who, aside from their other responsibilities, should ensure that the Document management policy and system are established, implemented, and maintained in accordance with the necessary requirements.

### Article 4. Document management processes

1. The Document management policy of the obligated entity comprises the different Document management processes addressed herein below.
2. The Document management policy shall implement a system of regular oversight and evaluations—at intervals agreed upon within the obligated entity—of all or part of its Document management processes, as a commitment to quality and continuous movement.

## CHAPTER 2. DOCUMENT IDENTIFICATION, CLASSIFICATION, AND DESCRIPTION

### Article 5. Archive identification

1. For the purposes of this law, "Identification" shall mean the Document management process used to review and study the actions carried out within an institution that provide knowledge of every aspect of the Documentation that the institution manages and keeps.

   Comment: *The fundamental objective of Identification is to gain a thorough knowledge of the institution producing, creating, or receiving the Documents in the exercise of its competencies, its organizational evolution over time, the administrative processes with which it has been operating, and all the provisions and regulations that affect the formal procedures it carries out. With that thorough knowledge, it will be possible to define the Document series that are the essential building blocks for developing all the other Document management processes in an institution*.

### Article 6. Document classification

1. For the purposes of this law, "Document Classification" shall mean a Document management process based on the systematic structuring of activities, institutions, or the Documents they generate into categories according to conventions, methods, or standards of procedure, all logically organized and represented in a Document management system.

   Comment: *Document Classification is used to design all Document management actions and strategies within an institution, since its result provides essential added value for planning and determining numerous subsequent actions, such as the establishment of Documentary conservation periods, the information access procedure, and the possibilities of recovering information and Documents from among all those managed by the subject entity.*

2. The tool resulting from Document Classification is the regulated entity's Document Classification chart, to be used for correct classification of all Documents generated by the subject entity.

3. It is the institution's responsibility to prepare a Document Classification chart in collaboration with the units responsible for Document creation and/or management, and to code that chart so that it includes all the activities carried out in the subject entity and their Documentary record.

### Article 7. Document description

1. In the context of this law, the main aim of description is to represent Documents in a comprehensible manner, providing information about the context of their creation, their organization, and their content, as well as to facilitate access to them.

   Comment: *Archival description is directly linked to the prior processes of Identification 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. A fond cannot be properly appraised, conserved, and disseminated if its contents, institutional provenance, and the functions that prompted its creation and use—i.e., its context—are not known.*

2. Institutions should develop a gradual plan for Document description. This plan should ignore the medium in which Documents are stored and the stage in their lifespan.

## CHAPTER 3. DOCUMENT APPRAISAL, TRANSFER, AND DISPOSAL

### Article 8. Document Appraisal

1. For purposes of this law, "Appraisal" shall mean the 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 Disposal, whether total or partial.

   Comment: *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.*

2. Appraisal procedures, which include Document selection, Disposal, and Transfer, should be designed to avoid arbitrary destruction of Documents as well as their needless accumulation.

3. Documents may never be disposed of as long as they have administrative force and continue to have probative value of rights and obligations.

   Comment: *It is essential to guarantee the information needed to know what activities institutions have carried out and to conserve that which is necessary, at first, for institutional management purposes, and subsequently, for research and history*.

   It would be desirable for Appraisal to occur not only when Documents enter archives, but also as early as the Document production stage. If we begin with rationalizing Document production and use, we can standardize procedures, and the production of useless Documents can be avoided; at the same time control and regulation of access to them can be defined, as can the time frames for Transfer, Disposal, or conservation.

4. Each subject entity shall establish an institutional Appraisal committee. This committee will be responsible for approving Document Appraisal tables or retention calendars.

5. Documents necessary for the normal operation of institutions and the services they provide or that serve as support for and recognition of rights and/or obligations, whether institutional or individual, should not be disposed of.

6. In some cases, serious economic sanctions and sometimes even criminal proceedings may result from the irregular destruction of Documents

7. All decisions taken and reports issued by Appraisal committees shall be Documented to provide evidence that they were permitted and authorized under the relevant law and norms.

8. The Appraisal and Disposal process shall be framed within a transparent and reliable system that is consistent with quality assurance systems and integrates the archive with the institution's management systems.

**Article 9. Document Transfer**

1. For the purposes of this law, "Transfer" shall means the usual procedure for entering material in an archive by transferring fractions of Document series once they have reached the time limit set by the rules established in the Appraisal for each stage of the lifespan of Documents.

   Comment: *Document Transfer shall be a process included in the Document management policy of the obligated entity. Its purpose is to ensure that Documents are properly processed in the most appropriate archive for that purpose. Thus, the accumulation of Documents in different centers and units is avoided, as are the adverse effects of that accumulation, while the most appropriate service is provided for each phase of the Documents' lifespan.*

2. All obligated entities shall establish a Transfer calendar, understood as a management instrument that governs the physical Transfer of Documents to the storage areas managed by the archive. Under this calendar, each unit shall have an assigned period for effecting the Transfer of Documents.

3. All Document Transfers are to be accompanied by a delivery report or form which should provide the necessary information about the Documents being transferred.

4. In the case of the Transfer of electronic Documents, provision shall be made for the compatibility of formats and media.

5. Electronic Document Metadata should be transferred along with the Document in order to enable its identification, authenticity, and any conservation procedures that may be necessary in the future.

6. The Documents shall be accompanied by other supplementary Documentation, such as indications of use and access privilege procedures; procedures to prevent, correct, and discover losses of or alterations to information; and indications of conservation procedures in connection with deterioration of the media and/or technological obsolescence.

7. Documents to be transferred shall be adapted to a durable format.

**Article 10. Document Disposal**

1. For purposes of this law, "Disposal" shall mean 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 purposes.

2. All Document Disposal shall be based on a decision regulated and authorized by the Appraisal Committee and at the highest level of the obligated entity, and shall be set forth in an express authorization by the management of the regulated entity that includes the type of Document to be disposed of and the time period that the reviewed Documentation is to be conserved.

3. Disposal shall ensure the impossibility of the disposed-of Document's reconstruction or subsequent use.

   Comment: *Strip-cut or cross-cut shredding is the most appropriate method for disposing of paper Documents. Paper is shredded into strips or particles whose size is chosen based on the level of protection required for the information contained in the Documents to be destroyed. In the case of Documents containing especially sensitive information, shredding into small particles is recommended.*[1]

4. If the Documentation to be disposed of is stored on computer media, the Appraisal Committee shall decide if it is to be securely wiped, understood as the procedure for the Disposal of data or files from a medium or set of media that enables those media to be reused (by means of overwriting, demagnetization, cryptographic wiping, etc.); or destroyed, meaning the process of rendering storage media containing electronic Documents physically unusable (by breaking into pieces, crushing, melting, shredding, etc.). The decision will depend on the medium or system of storage and the type of information it contains.

5. Documents shall be disposed of securely, with the same level of security as they had throughout their life cycle.

6. Disposal shall be done under proper supervision, in the presence of a responsible party of the regulated entity, who will attest to the action, and with control of the work to ensure the quality and relevance of said processes.

7. If the Disposal is done by an externally contracted company, the entity shall monitor compliance with all agreed Disposal requirements.

8. The Disposal shall be Documented in a Disposal record that contains all essential data to attest to said Disposal. That record shall be signed by the Appraisal Committee.

9. The Appraisal Committee of each institution shall coordinate the Appraisal and Disposal of Documents with the General Archive of the Nation or its equivalent, in order to prevent the destruction of information of historical value, as established in the respective national laws.

## CHAPTER 4. INFORMATION ACCESS AND SECURITY

[1] The particles of material for Documentation containing especially sensitive information are recommended to have a surface area of < 2000 $mm^2$ or strips of indeterminate length and width of < 12 mm, as recommended in ISO Standard BS EN 15713:2010 *Secure Destruction of Confidential Materials. Best practices code.*

**Article 11. Access to public Documents**

1. Access to public information is the fundamental right of persons to consult information in the possession, custody, or control of public authorities in the exercise of their functions. To the extent that such information is recorded in the form of Documents, one may also speak of the right to access public Documents.

2. The archive of media and Documents shall be done so as to guarantee proper conservation of their location and consultation, and to allow the right of access to public information to be realized.

3. The policy on access to public information shall be approved at the highest level of responsibility, together with guidelines for its implementation.

4. At a minimum, the Document setting out that policy should contain:

    a. The obligated entity's declaration of principles regarding access to public Documents and a list of its commitments, which shall 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 on existing restrictions, the reasons for them, and their legal and juridical bases.

    c. Clear information on the necessary administrative procedure, if any, for requesting access to Documents.

5. The policy on access to public information shall be evaluated periodically, including the level of compliance therewith, and mechanisms shall be established to correct its shortcomings or make improvements to it. This task shall include identification of indicators on the exercise of the right of access to public information.

6. The policy on access to public information shall be publicly disseminated and available to users at all times.

**Article 12. Analysis of legal access to Documents**

1. Analysis of legal and regulatory access is a technical process that entails the identification, for each Document series, of categories of content that may warrant a restriction on access to Documents as recognized by law, and the determination, in accordance with said law, of the legal time limits on access, as appropriate, that may apply.

2. Appropriate security measures shall be implemented that guarantee confidentiality in cases where it is required.

3. Possible means of facilitating total or partial access to Documents shall be made available.

4. Access and security tables or charts shall be prepared as an instrument in which rights of access and the system of applicable restrictions are identified.

**Article 13. Management of Document access requests**

1. The subject entity shall provide reference information on its Documents—including those subject to any type of restriction—and the procedure for requesting access to them.

2. The obligated entity shall provide direct access to public information without the need for any kind of procedural formalities; to information or Documents classified as unrestricted on the basis of the accessibility analysis process; and to internal users or those legally authorized to access restricted-access Documents
3. The obligated entity shall make available to the public standardized access request forms with clear instructions for their completion, that are in line with the provisions of the access to public information law.

**Article 14. Access restrictions and control**

1. Public authorities shall implement, in relation to their Document and archive management systems, the necessary security measures and access controls to prevent, in accordance with the legally established rights and restrictions, unauthorized access to confidential information.
2. Public authorities shall establish the necessary mechanisms to allow partial access to Documents or conceal certain data—with users advised in advance of that fact—through data masking, de-personalization or anonymization, partial access to files, or other similar mechanisms.
3. The security measures and controls on Document access should be established in accordance with the law, applicable technology, and, in particular, the obligated entity's information security policy.
4. A user permissions register shall be established as one of the main access control instruments.
5. Controlling access to Documents shall consist of applying the appropriate access conditions to each Document and to allow each user to access and use Documents according to those conditions and the permissions assigned to them in the user permissions register.
6. The necessary measures shall be instituted to control physical access to premises where Documents or the equipment and systems used to store them are located, in order to prevent unauthorized entry.
7. A monitoring system shall be implemented to supervise Document access, use, or handling, by means of tracing mechanisms (Document access log, audit trails, etc.).

**Article 15. Minimum security measures for Documents containing personal data**

1. Public authorities shall adopt measures to protect the security of personal data and prevent their unauthorized alteration, loss, transmission, or access.
2. Obligated entities shall assign one or more security officers responsibility for coordinating and controlling the application of security measures.
3. The duties and obligations of each user or user profile with access to personal data and information systems shall be clearly defined and Documented.
4. 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.
5. The copying or reproduction of Documents containing personal data should only be done under the supervision of personnel authorized by the security officer.

6. A register shall be established that logs access and identifies which authorized person has accessed Documentation containing personal data, and on what date. In instances where such Documentation has been loaned, the return date for the Documentation shall be logged.
7. Procedures shall be implemented to ensure the integrity of Documentation, such as a Document index or sequential numbering of its pages.
8. A security Document shall be drawn up that sets out the measures, standards, action protocols and rules for ensuring the level of security ; as well staff duties and obligations in relation to Document access.
9. For password-based authentication mechanisms, there should be an assignment, distribution, and storage procedure that ensures password confidentiality and integrity.

**Article 16. Exercise of the rights of access, rectification, cancellation, and objection of personal data**

1. The owners of personal data or their accredited representatives are entitled to request obligated entities 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 deletion of information that concerns them.
2. The obligated entity shall respond to the requests that it receives and set a maximum time limit for issuing and notifying a decision in the rights protection procedure.
3. Where a decision approves a request, the obligated entity shall ensure that the rights are effectively exercised and set down the manner of their realization in writing.

**Article 17. Information security**

1. Public authorities shall 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.
2. Public authorities shall manage information security within the institution and shall maintain the security of resources and information assets that are accessible by staff or external personnel.
3. All staff accessing information should be aware of and accept their responsibility with respect to security. Public authorities shall provide staff with the necessary training to perform that task properly.
4. Infrastructure and repositories must be protected by means of access control mechanisms.
5. Any system should consider the security requirements of Documents for their entire lifespan.
6. A plan of action shall be developed to minimize the effects of a catastrophe, in order to safeguard the integrity, availability, and preservation of information.
7. Public authorities shall ensure that their staff maintain professional secrecy, not divulge restricted information, and respect confidentiality where appropriate.

**Article 18. Reuse of information**

1. For the purposes of this law, reuse of public sector information means the use by natural or legal persons, whether for-profit or non-profit, of information in the possession, custody, or control of the obligated entity, for purposes other than the ones that those Documents originally had in the public service mission for which they were produced.

2. The reuse of public sector information offers significant economic potential and added value, as it facilitates the development and creation of new products, services, and markets.

3. A consistent legal framework shall be created with an objective and subjective sphere of application, as shall 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.

4. That legal framework shall include limitations compatible with the Access to Public Information Law; that is, it shall list those public Documents or categories of Documents not amenable for reuse of public-sector information (e.g., Documents and information that affect the security of the State, Documents protected by copyright or industrial property rights, etc.) in accordance with standards in force.

5. The conditions for reuse shall include such aspects as the guarantee that Documents will not be altered or their information falsified or distorted, that the source be stated, etc.

## CHAPTER 5. DOCUMENT CONSERVATION AND CONTINGENCY MANAGEMENT

### Article 19. Preparation of an integrated Document conservation plan

1. For the purposes of this law, 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.

2. Institutions shall ensure the security and integrity of Documents over time through procedures set down in internal regulations or process manuals.

3. The obligated entity shall design and implement a conservation plan for the Document fonds in its custody.

4. All the staff in the various units of each obligated entity shall be trained in good practices and preventive conservation, especially those with responsibilities in archives.

5. Each facility should have an officer in charge to ensure that archive depositories or rooms where equipment and systems on which Documents are stored fulfill the necessary requirements to enable their normal operation.

6. Electronic Documents must be conserved, as must analog Documents, as evidence of acts for responsibility and memory purposes, while maintaining their authenticity, reliability, integrity, and availability. This conservation should involve information technology specialists, Document managers, and archivists.

### Article 20. Custody and control of facilities

1. The obligated entity shall 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.
2. In order to ensure the correct design and construction of an archive building, the obligated entity shall provide the architects or engineers all the necessary information in relation to environmental guidelines, security features, disaster prevention, secure Document transportation, and use of appropriate furniture to ensure the success of the project.
3. Archive Document repositories should be separate from other offices and not be in a high-traffic area. If possible, they should also be situated well away from places with high temperature and hygroscopic variations (such as walls and attics) or areas vulnerable to flooding (such as basements).
4. Documentation circuits must not be interfered with by staff who do not belong to the obligated entity or unauthorized public officials. All exits shall be appropriately signed to facilitate evacuation and intervention in an emergency.
5. The obligated entity shall ensure that it selects appropriate archive furniture to contribute to the better preservation of the fonds in its custody. That selection must also include high-density storage systems to minimize the space needed for the fonds in its custody.
6. Archives with electronic Documents in their custody shall employ digital preservation strategies and tools to address the challenges of media durability and technological obsolescence. Depending on the medium and the type of information it contains, consideration shall be given to the most appropriate preservation option: media renewal, information migration to durable formats, information Transfer between technology platforms, information system emulation, etc.

**Article 21. Environmental control**

1. Archives shall comply with national standards on occupational risk prevention.
2. An evaluation shall be done of environmental factors that could affect Documents. To that end, there shall be monitoring of humidity and temperature fluctuations, intensity and length of Document exposure to light, the presence of dust and pollution in archive repositories, insect population, and periodic inspections to check for signs of pest activity.
3. Inspection routines shall be developed for rooms and repositories to check for the presence of micro-organisms in response to biodegradation; biocide misuse shall be monitored, and a healthy environment shall be ensured through maintenance and cleaning of humidification, dehumidification, and ventilation equipment in archive repositories.
4. Conservation standards and appropriate handling techniques for overall hygiene maintenance shall be observed.

**Article 22. Preparation of a contingency management plan**

1. Each obligated entity shall design a contingency management plan for institutional archives, which shall be considered one of the pillars of the general preventive conservation plan.

2. The obligated entity shall be responsible for providing instruction to the members of contingency committees, contingency teams, and salvage brigades for safeguarding the Document fonds in the custody of those authorities.

3. At a minimum, the contingency management plan shall include information about the building, essential Documents, evacuation routes, chains of communication to be activated in emergencies, basic instructions and action protocols, and damage assessment forms.

### Article 23. Risk assessment

1. A risk assessment shall be done to identify the protection strengths and weaknesses of each center. To that end, the following variables shall be assessed:

    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 fonds.

2. The information compiled in the risk assessment shall be materialized in a risk map that serves as a guide for establishing and monitoring inspection routines. The risk map must be kept current and enable action priorities to be established.

## CHAPTER 6. AWARENESS RAISING AND USER ASSISTANCE SERVICES

### Article 24. Awareness raising and gender policy

1. The obligated entity shall raise awareness of the Documents in its possession.

2. The obligated entity shall develop an awareness program, taking into account the type of user being targeted, as well as analyzing needs in terms of media and awareness-raising actions to be carried out (exhibits, guided tours, publications, social media accounts, educational services, etc.)

3. The obligated entity shall disseminate information of interest to women, particularly concerning gender discrimination and violence, and shall produce, based on the information in its possession, custody or control, statistics on violence and discrimination against women and other related qualitative and quantitative information.

4. The obligated entity shall have a budget with which to operate that service properly.

### Article 25. Assistance to the administration by archive services

1. The archive shall keep permanently available for the administration the Documents that the latter has generated and transferred to it.

2. The archive must be able to answer queries and manage through a regulated procedure administrative loans of any Document to the administration that produced the Document series in its custody.

### Article 26. Public assistance

1. The archives of public authorities must have 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. It will be in charge of:
    a. Addressing requests for archival information
    b. Providing access to Documents
    c. Document reproduction
2. The range of public assistance services offered by the archive shall be available in writing and publicly disseminated.
3. In general, such services shall be free of charge and equally accessible to all without restriction. However, in certain circumstances, they may or must be subject to restrictions where the law so requires.
4. A multichannel service shall be established 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).
5. On-site access to Documents should occur on suitable premises, by the appropriate means, and with sufficient technical and administrative staff.
6. The conditions on the use of the contents of the archive's digital objects available online or of copies obtained or provided shall be clearly set out and stated to users in writing.

## CHAPTER 7. ELECTRONIC MANAGEMENT

### Article 27. Interoperability

1. The information systems and supported procedures of public authorities must have the ability to share data and enable the exchange of information and knowledge with each other. This capacity of information and communication technology (ITC) systems and the business processes they support to exchange data and enable the exchange of information and knowledge is known as interoperability.
2. Interoperability should have a threefold dimension: organizational, semantic, and technical. A fourth dimension, the temporal, is also included, which requires the obligated entity to guarantee access to information throughout the lifespan of electronic Documents.
3. Interoperability should be an instrument that simplifies the organizational complexity of the obligated entity.
4. The obligated entity should strive to be technology neutral, ensuring a free choice of alternatives for people and avoiding any kind of technological discrimination.

### Article 28. Metadata

1. The purposes of this law, “Metadata” shall mean those data that describe the context, content, and structure of electronic Documents and files and their management over time.
2. Public authorities should ensure the availability and integrity of the Metadata of the information in their possession, custody, and control.
3. Electronic Document management Metadata should be articulated in Metadata schemes that match the particular characteristics and management needs of each obligated entity.
4. The Metadata that the obligated entity identifies as necessary for its Document management processes should be incorporated in the electronic Document management systems.

**Article 29. Digitization**

1. Minimum requirements must be established for electronic images produced by digitization, which should be defined by standardizing the basic parameters for those processes.
2. The digitization process should cover format standardization, quality levels, technical conditions, and the associated Metadata.
3. The electronic image obtained from digitization should be true to the original content and ensure its integrity.
4. A necessary part of the digitization process is preventive maintenance and routine checks to ensure the quality of the image and its Metadata.

## CHAPTER 8. STAFF PROFILES AND DOCUMENT MANAGEMENT TRAINING

**Article 30. Senior management**

1. The senior management of the subject entity shall define the overall orientation of the Document and archive management policy in order to:
    a. Give coherence to all the operations of the entire obligated entity in the area of the management.
    b. Require staff to adopt the inherent requirements and duties of Document management and custody.
    c. Ensure that the processes of the obligated entity and the Documents it generates are transparent and comprehensible.
    d. Ensure for the benefit of external interested parties (law courts, regulators, auditors, members of the public, etc.) that Documents are appropriately managed.
2. Although senior management may delegate responsibility for Document management and custody to the rest of the institution’s staff, it shall retain ultimate responsibility with respect to accountability.
3. Should the complexity of the obligated entity so require, senior management shall appoint a Document and archive management representative at the operational level, whose role, responsibilities, and competencies must be clearly defined.

**Article 31. Middle management**

1. The heads of management units are responsible for ensuring that the personnel under their supervision create, maintain, and protect Documents as an integral part of their work, in accordance with previously established policies, procedures, and norms.
2. Middle managers shall encourage and hold regular interdisciplinary meetings including staff who create and have custody of Documents as part of their responsibilities, IT technicians, and archive technicians of the obligated entity, in order to develop, implement, review, and improve management systems in their spheres of action as well as to create, safeguard, and process authentic, complete, and available Documents.

**Article 32. Archive technicians**

1. The technical personnel qualified in the area of archives and Document management are responsible for every aspect of archival processing and correct Document management in the obligated entity, including the design, implementation, and maintenance of the Document management system and its operations.
2. Archive technicians are a crosscutting, highly qualified human resource, essential for the obligated entity in the areas of communication, awareness, advisory services, and training of personnel in archive and Document management throughout the obligated entity.
3. Archive technicians must work in collaboration with ICT technicians on the design, implementation, and improvement of the management system, on information architecture, on information security, and on information access and recovery.

**Article 33. Communication plan**

1. The communication plan shall ensure that the procedures and benefits of Document and archive management are understood throughout the obligated entity. It shall clearly explain the Document management guidelines and situate the procedures and processes in a context that enables the reasons for the need for Document management to be understood.
2. The communication plan shall articulate procedures to ensure that the Documents related to the obligated entity's Document and archive management policy are accessible to and reach all its members, and it is advisable to make a package of Documents with information on strategic responsibilities and procedures readily accessible.

**Article 34. Work team awareness**

1. The obligated entity must ensure the awareness and buy-in of all the personnel and that they are mindful of:
    a. The importance of each of their individual activities and how they help to achieve the objectives of the Document and archive management system.
    b. The main aspects of the Document and archive management system associated with their work and the benefits of their improved performance.
    c. The importance of carrying out the obligated entity’s policy and Document and archive management procedures.
    d. The risks and consequences of failure to adhere to established procedures.

**Article 35. Continuing education plan**

1. One of the strategies of the obligated entity shall be to design a continuing education plan and appoint a person with the appropriate seniority to have responsibility for the program, provide it with the necessary resources, and be in charge of its design and execution.
2. Education shall be given to all personnel of the obligated entity who generate, maintain, or have custody of Documents (as well as executive officers and senior management), external contractors, volunteers, and anyone else who is in charge of all or part of an activity in which Documents are created and incorporated in the obligated entity's Document management systems, taking into account their duties and responsibilities.
3. The training needs analysis shall be based on periodic personnel surveys, personnel performance evaluations, and analyses of weaknesses, risks, or gaps in Document and archive management in the obligated entity.
4. The training must be periodically evaluated and reviewed through:

    a) Measurement of its performance

    b) Audits

    c) Contrasting staff competency levels with the objectives of the education program.

5. Periodic reviews will be done, both of the education contents, and of its orientation, in order to ensure its effectiveness and adequacy to changes that may occur in the context (legal, social, administrative, etc.) in which the obligated entity is situated and in the internal Document and archive management system itself.
6. The necessary adjustments shall be made to the education plan to achieve ongoing improvement, and mechanisms shall be designed so that personnel who have already received education can benefit from the improvements introduced in new activities.
7. The level of satisfaction of persons who have participated in education activities shall be evaluated (for example, by means of satisfaction surveys).

**Article 36. Miscellaneous provisions**

With its entry into force, this law derogates all other norms of equal or lesser rank that oppose or contradict the provisions of this law.

# APPLICATION GUIDE
# MODEL INTER-AMERICAN LAW
# ON DOCUMENT MANAGEMENT

## TABLE OF CONTENTS

## CHAPTER 1. 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.*

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

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 probably 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.

## CHAPTER 2. DOCUMENT ANALYSIS, CLASSIFICATION, AND DESCRIPTION

**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.*

**2.1. Archive identification**
**2.2. Document classification**
**2.3. Document description**

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.

## CHAPTER 3. DOCUMENT APPRAISAL, TRANSFER, AND ELIMINATION



### 3.1 Document appraisal

**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.*

**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.

## CHAPTER 4. INFORMATION ACCESS AND SECURITY



### 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 fonds.

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.
    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.

[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.

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.

## CHAPTER 5. CONSERVATION AND CONTINGENCY MANAGEMENT



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 fonds.

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.

## CHAPTER 6. AWARENESS RAISING AND USER ASSISTANCE SERVICES

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

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 fonds, document-producing 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.

### 6.4. 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.

## CHAPTER 7. ELECTRONIC ADMINISTRATION

**7.1. Interoperability**
**7.2. Metadata**
**7.3. Document digitization**

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.

## CHAPTER 8. STAFF PROFILES AND DOCUMENT MANAGEMENT TRAINING



**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.

### 8.4. Communication plan
### 8.5. Work team awareness

**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.

### 8.6. 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.archivogeneral.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/publiventa/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 I: 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.; TILLETT, 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
- 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 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 *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 I: 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/POLITICA%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.archivogeneral.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


- ALBERCH I 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: *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.
- 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 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 *G02/G. Guía de Implementación Gerencial: Gobierno Abierto y Transparencia. G02/D01/G. Directrices: Acceso a los documentos públicos. G02/D03/G. Directrices: Reutilización 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 STANDARIZATION (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 STANDARIZATION (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 STANDARIZATION (ISO). 2016. *ISO 15489-1:2016: Information and documentation - Records management - Part 1: Concepts and principles*. Ginebra: ISO.
- INTERNATIONAL ORGANIZATION FOR STANDARIZATION (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: *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.
- 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 Arquivos Municipais: Políticas, Sistemas e Instrumentos nos Arquivos 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 universitaris de Biblioteconomia 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.agendadigital.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. DOCUMENT 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 Operacional: 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.minhafp.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 CLAVAÍN, J. 2008. *La conservación en archivos y bibliotecas: prevención y protección*. Madrid: Ollero y Ramos.

- TACÓN CLAVAÍN, 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://archivofsierrapambley.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 Documentación 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 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 *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 ORGANZATION. 2010a. *ISO 16175-1:2010. Principles and functional requirements for records in electronic office environments. Part 1: Overview and statement of principles.*
- INTERNATIONAL STANDARDS ORGANZATION. 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 ORGANZATION. 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. Sustentabilidad. 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 Conected Europe. Disponible en: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/About+CEF+building+blocks
- COMISIÓN EUORPEA. 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://cevifaiprivada.ifai.org.mx/swf/cursos/archivos/introduccin.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