G06/O

Guía de Implementación Operacional- Control de acceso

Modelo de Gestión de Documentos y Administración de Archivos (MGD) para la Red de Transparencia y Acceso a la Información (RTA)

Versión: 1.0

Fecha: diciembre de 2014

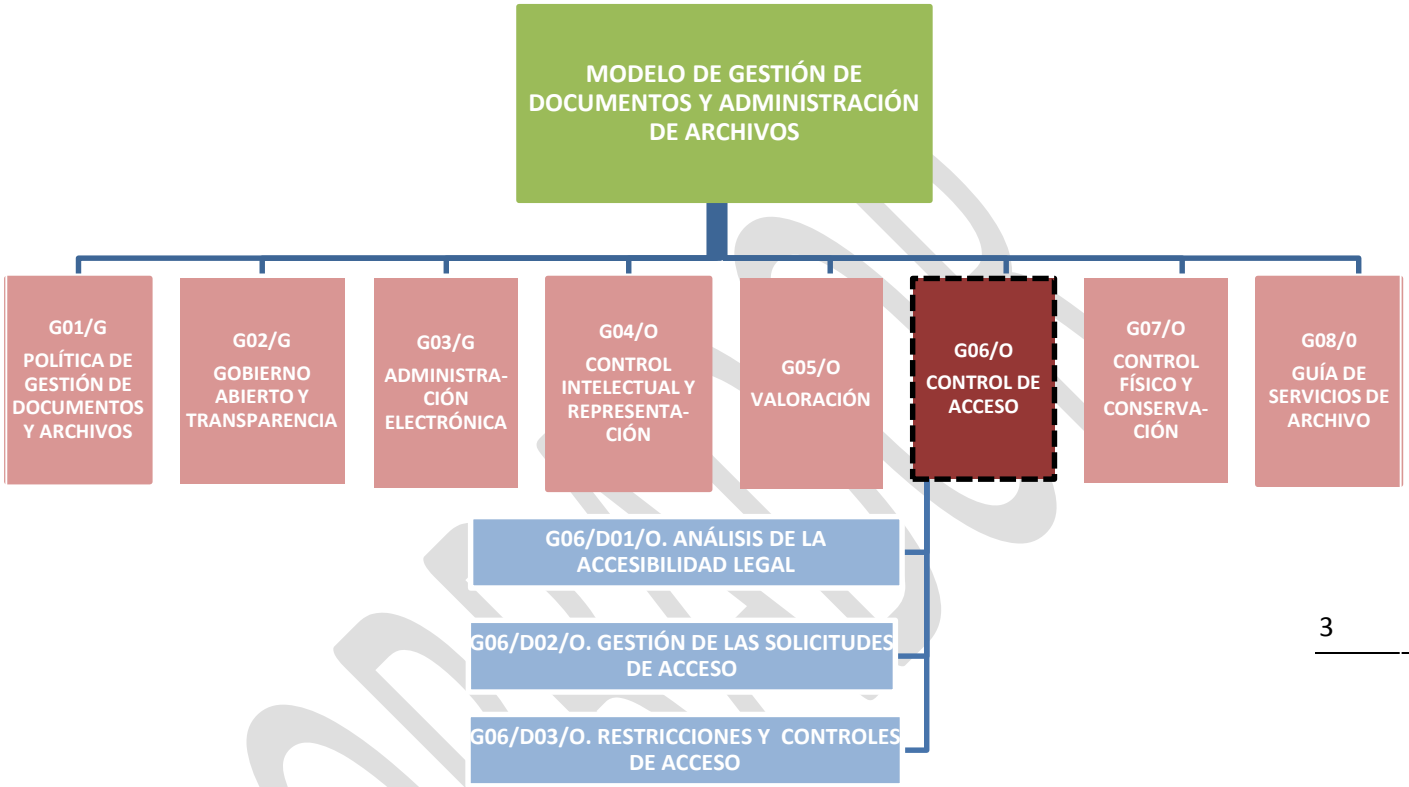
Coordinadores

Beatriz Franco Espiño
Ricard Pérez Alcázar

Equipo

Blanca Desantes Fernández
Francisco Fernández Cuesta
Javier Requejo Zalama

Esta Guía de Implementación se integra en el Modelo de Gestión de Documentos y administración de archivos (MGD) de la Red de Transparencia y Acceso a la Información (RTA) según se especifica en el siguiente Diagrama de relaciones:



1. Presentación y objetivos
    1.1. Breve presentación
    1.2. Finalidad
    1.3. Destinatarios
    1.4. Alcance y contenido
    1.5. Documentos relacionados
2. La gestión y el control del acceso a los documentos
3. Líneas de actuación
    3.1. Línea de actuación 1: Analizar las restricciones de acceso y los requisitos de seguridad de los documentos
    3.2. Línea de actuación 2: Gestionar las solicitudes de acceso a los documentos públicos
    3.3. Línea de actuación 3: Implementar las restricciones y un procedimiento de control de acceso
4. Cuadro de actuaciones
5. Términos y referencias
    5.1. Glosario
    5.2. Referencias
    5.3. Bibliografía

1. Presentación y objetivos

1.1. Breve presentación

Las Guías de implementación de procesos y controles (guías operacionales) ofrecen a los coordinadores técnicos encargados del Sistema de Gestión de Documentos en las instituciones, las líneas generales para implementar los procesos y controles técnicos del MGD de la Red de Transparencia y Acceso a la Información (RTA).

1.2. Finalidad

Este documento identifica una serie de compromisos destinados a la implementación, por parte de instituciones archivísticas, de los procesos y controles necesarios para gestionar el acceso a los documentos con eficacia, eficiencia y respeto de las debidas garantías legales establecidas tanto a favor del acceso a la información pública, como de la confidencialidad necesaria para proteger otros derechos, valores y bienes jurídicos.

1.3. Destinatarios

Las Guías de implementación de procesos u operacionales tienen como destinatarios principales a las personas designadas por la alta dirección para coordinar la implementación del MGD, tanto a nivel gerencial como operacional, y a los técnicos encargados de la implementación del Modelo, y como destinatarios secundarios a los usuarios internos de la organización.

Los destinatarios principales de esta Guía de implementación operacional son los especificados en los puntos B y C y los usuarios secundarios son los especificados en el punto D, siguiendo los códigos de destinatarios de la norma ISO 30300 (Información y documentación. Sistemas de gestión para los documentos. Fundamentos y vocabulario), que se toma como referencia para esta cuestión en este Modelo, tal y como se desarrolla a continuación:

Destinatarios principales

B. Coordinación de la implementación del Sistema de Gestión Documental (SGD): personas designadas por la alta dirección para coordinar la implementación del SGD, tanto a nivel gerencial como operacional. Ambas responsabilidades pueden concentrarse en una misma persona o grupo. Esta categoría incluye:

B.1. Representante de la alta dirección: representante específico de la dirección que lidera y se responsabiliza de la implementación del SGD (ISO 30301:2011, 5.3.2)

B.2. Representante de la gestión documental: persona designada por la alta dirección para implementar el SGD a nivel operacional (ISO 30301:2011, 5.3.3). Incluye a los responsables principales de las instituciones archivísticas.

C. Técnicos encargados de la implementación del SGD:

C.1. Profesionales de la gestión de documentos: personas encargadas de establecer las políticas, procedimientos y normas generales, e implementar los procesos y controles de la gestión de documentos (ISO/TR 15.489-2:2001, 2.3.2.b)

C.2. Profesionales con obligaciones específicas en relación con los documentos: profesionales de las áreas de gestión de riesgos, auditoría, tecnologías de la información y seguridad de la información (ISO/TR 15.489-2:2001, 2.3.2.d; ISO 30301:2011, Introducción)

Destinatarios secundarios

D. Usuarios internos

D.01. Jefes de unidades de gestión: personas responsables de garantizar que el personal a su cargo crea y mantiene documentos como parte integrante de su trabajo y de acuerdo con las políticas, procedimientos y normas establecidas (ISO/TR 15489-2:2001, 2.3.2.c)

D.02. Resto del personal: personal que crea, recibe y mantiene documentos como parte de su labor diaria, de acuerdo con las políticas, procedimientos y normas establecidas (ISO/TR 15489-2:2001, 2.3.2.e)

1.4. Alcance y contenido

Las Guías de implementación constituyen el documento en el que se definen las líneas generales de actuación que han de seguirse para implementar el modelo de gestión de documentos y administración de archivos de la Red de Transparencia y Acceso a la información (RTA). Estas líneas de actuación, fundadas en normas y buenas prácticas internacionales, se materializan a su vez en un conjunto flexible de compromisos que pueden ser asumidos por las organizaciones o instituciones según diferentes niveles de mejora.

Los compromisos incluidos en cada línea general de actuación no están concebidos para su implementación de una forma necesariamente secuencial. Pueden ejecutarse en diferentes etapas, de forma reiterada, parcial o gradualmente, de acuerdo con las necesidades de la organización, sus requisitos y los cambios que puedan operarse en su entorno y en su propio ámbito de actuación.

La guía incluye un cuadro que recoge:

- La identificación de las Líneas de actuación mediante su código numérico
- Los compromisos que se pueden alcanzar para el cumplimiento de dichas líneas de actuación. Incluye un código numérico que se utilizará en las directrices;
- Los diferentes niveles de mejora para la consecución de los citados compromisos, identificados según la siguiente leyenda:

Líneas de actuación | Nivel inicial | Nivel intermedio | Nivel avanzado

Se completa, finalmente, con un apartado que presenta documentos de referencia regionales e internacionales y bibliografía seleccionada para orientar la implementación de los compromisos señalados.

1.5. Documentos relacionados

G02/D01	Gobierno abierto y transparencia
G02/D01/G	Acceso a los documentos públicos (política)
G02/D02/G	Transparencia activa y datos abiertos
G02/D03/G	Reutilización de la información

G06/O	Control de acceso
G06/D01/O	Análisis de la accesibilidad legal
G06/D02/O	Gestión de las solicitudes de acceso
G06/D03/O	Restricciones y controles de acceso

2. La gestión y el control del acceso a los documentos

Los archivos públicos son las instituciones responsables de gestionar y conservar los documentos que testimonian la actividad de los poderes del Estado; los documentos a través de los cuales las autoridades pueden rendir cuentas a la ciudadanía; los que testimonian derechos y obligaciones de las personas, de las empresas, de las propias administraciones; los que registran, finalmente, parte esencial de la memoria escrita de una nación.

Los archivos son instituciones con vocación y tradición de servicio público, que llevan siglos satisfaciendo las necesidades de información de las autoridades a las que sirven y que en las sociedades actuales se encuentran también volcadas en poner esta información en manos de un público cada vez mayor y más heterogéneo. La implementación en la mayoría de las naciones de nuestra región de leyes de acceso a la información pública no hace sino incidir en esta función y situar a los archivos en el eje de las políticas de transparencia.

Paralela a la función primordial de los archivos públicos de garantizar el derecho de acceso a los documentos, se encuentra su responsabilidad a la hora de procurar la debida confidencialidad de la información cuando afecte a otros derechos, valores y bienes jurídicos

(la seguridad nacional, el secreto comercial y la privacidad de las personas, son tres ejemplos representativos).

Los principios de acceso a los archivos del Consejo Internacional de Archivos (ICA 2012, 10) defienden la participación de los archiveros en los procesos de toma de decisiones sobre el acceso:

> Los archiveros ayudan a sus instituciones a establecer políticas y procedimientos sobre el acceso y revisan los archivos para su posible accesibilidad en función de las leyes, directrices y buenas prácticas que estén vigentes. Los archiveros trabajan con los especialistas en Derecho y con otros especialistas con respecto a establecer un marco básico de trabajo y con respecto a la interpretación de las restricciones cuando los archiveros tengan que aplicarlas. Los archiveros conocen los archivos, las restricciones sobre acceso, las necesidades y los requisitos establecidos por las partes interesadas así como qué documentación es, de hecho, de dominio público en relación con la materia con la que los archivos está relacionada; los archiveros aplican este conocimiento cuando se han de adoptar decisiones sobre el acceso. Los archiveros ayudan a la institución a cumplir con las decisiones adoptadas y a ser coherente con las mismas, y a ser consecuente con sus resultados.
>
> Los archiveros dirigen las restricciones, revisan los archivos y eliminan las restricciones que ya no han de ser aplicadas.

En este marco, los compromisos recogidos en esta Guía pretenden profundizar en la implementación del MGD de la Red de Transparencia y Acceso a la Información (RTA) en torno a las siguientes líneas de actuación:

- Analizar las restricciones de acceso y los requisitos de seguridad de los documentos, con el objetivo de plasmarlas en una tabla de acceso y seguridad.
- Gestionar las solicitudes de acceso a los documentos públicos, esto es, llevar a cabo las tareas técnicas y administrativas necesarias para satisfacer las necesidades de información de los ciudadanos a partir de los documentos del archivo.
- Implementar las restricciones identificadas y unos procedimientos de control en los sistemas de gestión, de forma que pueda darse respuesta a las solicitudes sin menoscabo de la confidencialidad necesaria para proteger determinadas categorías de información.

3. Líneas de actuación

3.1. Línea de actuación 1: Analizar las restricciones de acceso y los requisitos de seguridad de los documentos

La gestión y el control del acceso y uso de los documentos gestionados por los archivos públicos exigen, de conformidad con la normativa técnica y las buenas prácticas internacionales sobre la materia, el análisis y sistematización de los requisitos legales de seguridad y acceso que afectan a dichos documentos. Este proceso tiene como resultado una

herramienta básica para el funcionamiento de los sistemas de gestión de documentos diseñados a partir del marco general de ISO 15489: la tabla de acceso y seguridad.

Las tablas de acceso y seguridad son el instrumento formal que contemplan las normas ISO 15489 para la identificación de los derechos de acceso y el régimen de restricciones aplicables a los documentos, y consisten en una clasificación de categorías de documentos en función de sus restricciones de acceso y condiciones de seguridad (ISO/TR 15489-2:2001, 4.2.5).

Los beneficios del análisis y definición de requisitos de seguridad y acceso de los documentos mediante tablas de acceso y seguridad son múltiples:

- Facilita la implementación y puesta en marcha de las políticas de acceso a los documentos públicos y seguridad de la información.
- Permite definir de forma racional los controles de acceso y medidas de seguridad del sistema de gestión documentos.
- Permite mejorar la eficacia y disminuir la discrecionalidad del sistema de acceso a los documentos públicos, reduciendo los plazos de respuesta.
- Permite identificar posibles mejoras en la calidad del diseño de los documentos públicos.

Compromisos a cumplir

1. Recopilar todos los instrumentos jurídicos, políticos y operativos que rigen las cuestiones de seguridad de la información y el acceso a los documentos de la organización.
2. Definir las categorías de información susceptibles de protección a tenor de las fuentes recopiladas y los plazos de acceso a cada una de ellas.
3. Identificar los requisitos de seguridad de la información que afectan a la organización, clasificarlos por niveles y vincularlos con las categorías de información definidas.
4. Identificar las categorías de información susceptibles de protección que contiene cada serie documental.
5. Asignar a cada serie unos controles de acceso y uso acordes al nivel de seguridad correspondiente a las categorías de información que contienen.
6. Fundamentar la asignación de controles en un análisis de riesgos detallado.
7. Establecer reglas de control de acceso para cada serie.
8. Aprobar la tabla de acceso y seguridad, así como los mecanismos para su revisión periódica.
9. Definir y asignar metadatos para la seguridad apropiados a cada clase de documentos.

3.2. Línea de actuación 2: Gestionar las solicitudes de acceso a los documentos públicos

Las funciones de los archivos con respecto a las solicitudes de acceso a la información pública pueden variar dependiendo de las distintas legislaciones nacionales. En general, se pueden dar tres escenarios diferentes, en función del marco jurídico que regule el acceso a los documentos custodiados por las instituciones archivísticas:

- El acceso a los documentos custodiado por instituciones archivísticas se rige por la ley general de transparencia y acceso a la información pública, pero las solicitudes se tramitan a través de oficiales o unidades administrativas ajenas a dichas instituciones (aunque dependientes de una misma autoridad pública).
- El acceso a los documentos custodiado por instituciones archivísticas se rige por la ley general de transparencia y acceso a la información pública, y dichas instituciones o alguno de sus oficiales tienen la responsabilidad de tramitar las solicitudes.
- El acceso a los documentos custodiado por instituciones archivísticas cuenta con un régimen jurídico específico, frente al general del acceso a la información pública.

Independientemente del papel concreto que reserve la legislación sobre acceso a la información pública a las instituciones archivísticas, el hecho es que habrán de participar en mayor o en menor medida en los procesos ligados a la gestión de las solicitudes de acceso.

Para alinear estos procesos con las mejores prácticas internacionales, el modelo de gestión de documentos y administración de archivos de la Red de Transparencia y Acceso a la Información (RTA) propone una serie de compromisos basados en la Ley Modelo Interamericana sobre Acceso a la Información Pública (OEA 2010a), desde el punto de vista jurídico; y en la Guía Técnica para la gestión de archivos de uso restringido del Consejo Internacional de Archivos (ICA 2014), desde el técnico-archivístico.

Compromisos a cumplir

1. Proporcionar de forma proactiva la información y los servicios necesarios para que el mayor número de personas pueda ejercer el derecho de acceso a la información pública.
2. Informar y asesorar a los usuarios en sus solicitudes de acceso.
3. Localizar los documentos necesarios para dar respuesta a una solicitud de acceso a la información en el menor plazo posible.
4. Revisar la accesibilidad legal de los documentos objeto de solicitud.
5. Facilitar la entrega de los documentos en la forma en la que fueron solicitados.
6. Documentar adecuadamente los trámites necesarios para resolver una solicitud de acceso.

3.3. Línea de actuación 3: Implementar las restricciones y un procedimiento de control de acceso

Para implementar los requisitos de seguridad y acceso identificados a través de la primera de las líneas de actuación de esta Guía, se proponen una serie de compromisos orientados, por un lado, a establecer un marco general de control de acceso en los sistemas de gestión de documentos de conformidad con la norma ISO 15489, especialmente en entornos electrónicos. Y, por otro, mediante las restricciones específicas que afectan a los propios documentos –tanto en el ámbito de los soportes tradicionales (papel, singularmente), como en entornos electrónicos-, incluyendo los mecanismos que permitan ofrecer un acceso parcial a los mismos, ocultando los datos y contenidos objeto de protección.

Compromisos a cumplir

1. Controlar y representar, por medio de los instrumentos y sistemas de descripción, los documentos de acceso restringido.
2. Retirar de la consulta pública aquellas unidades completas que sean de acceso restringido.
3. Proporcionar un acceso parcial a documentos mediante el enmascaramiento de los datos confidenciales en copias en soporte de papel.
4. Disponer de un registro de permisos de usuario.
5. Establecer un procedimiento de control de acceso conforme a la norma ISO 15489.
6. Implementar el control de acceso en el sistema de gestión de documentos electrónicos.

4. Cuadro de actuaciones

En este cuadro se recogen:

- Las líneas de actuación, identificadas mediante su código numérico
- Los compromisos a alcanzar para el cumplimiento de dichas líneas de actuación, con un código numérico que se recupera en el cuadro de compromisos de las directrices
- Los diferentes niveles de mejora para la consecución de los compromisos

Leyenda: Líneas de actuación

Nivel inicial Nivel intermedio Nivel avanzado

Línea de Actuación	Compromisos a cumplir	Nivel
1	**Analizar las restricciones de acceso y los requisitos de seguridad de los documentos**	
1.1	Recopilar todos los instrumentos jurídicos, políticos y operativos que rigen las cuestiones de seguridad de la información y el acceso a los documentos de la organización	
1.2	Definir las categorías de información susceptibles de protección a tenor de las fuentes recopiladas y los plazos de acceso a cada una de ellas	
1.3	Identificar los requisitos de seguridad de la información que afectan a la organización, clasificarlos por niveles y vincularlos con las categorías de información definidas	
1.4	Identificar las categorías de información susceptibles de protección que contiene cada serie documental	
1.5	Asignar a cada serie unos controles de acceso y uso acordes al nivel de seguridad correspondiente a las categorías de información que contienen	
1.6	Fundamentar la asignación de controles en un análisis de riesgos detallado	

Nivel inicial Nivel intermedio Nivel avanzado

Línea de Actuación		Compromisos a cumplir	Nivel
	1.7	Establecer reglas de control de acceso para cada serie	
	1.8	Aprobar la tabla de acceso y seguridad, así como los mecanismos para su revisión periódica	
	1.9	Definir y asignar metadatos para la seguridad apropiados a cada clase de documentos	
2		**Gestionar las solicitudes de acceso a los documentos públicos**	
	2.1	Proporcionar de forma proactiva la información y los servicios necesarios para que el mayor número de personas pueda ejercer el derecho de acceso a la información pública	
	2.2	Informar y asesorar a los usuarios en sus solicitudes de acceso	
	2.3	Localizar los documentos necesarios para dar respuesta a una solicitud de acceso a la información en el menor plazo posible	
	2.4	Revisar la accesibilidad legal de los documentos objeto de solicitud	
	2.5	Facilitar la entrega de los documentos en la forma en la que fueron solicitados	
	2.6	Documentar adecuadamente los trámites necesarios para resolver una solicitud de acceso	

Nivel inicial Nivel intermedio Nivel avanzado

Línea de Actuación	Compromisos a cumplir	Nivel
3	**Implementar las restricciones y un procedimiento de control de acceso a los documentos**	
3.1	Controlar y representar por medio de los instrumentos y sistemas de descripción los documentos de acceso restringido	
3.2	Retirar de la consulta pública aquellas unidades completas que sean de acceso restringido	
3.3	Proporcionar un acceso parcial a documentos mediante el enmascaramiento de los datos confidenciales en copias en soporte de papel	
3.4	Disponer de un registro de permisos de usuario	
3.5	Establecer un procedimiento de control de acceso conforme a la norma ISO 15489	
3.6	Implementar el control de acceso en el sistema de gestión de documentos electrónicos	

Nivel inicial Nivel intermedio Nivel avanzado

5. Términos y referencias

5.1. Glosario

Accesibilidad legal: posibilidad de consulta de los documentos de archivo de conformidad con la normativa vigente.

Acceso parcial: posibilidad de acceder a parte del contenido de las unidades documentales de acceso restringido mediante la ocultación de la información objeto de protección. Deberá informarse en todo caso al usuario sobre el tipo de contenidos que han sido excluidos del derecho de acceso y el motivo concreto de tal exclusión.

Acceso restringido: véase *Restricción de acceso*.

Confidencialidad: propiedad de la información por la que se garantiza que ésta es accesible únicamente a aquellas personas autorizadas para ello.

Control de acceso: esquema de mecanismos empleado por el sistema de gestión de documentos para evitar el acceso a los documentos a usuarios no autorizados.

Cuadro de acceso y seguridad: véase *Tabla de acceso y seguridad*.

Divulgación parcial: véase *Acceso parcial*.

Encubrimiento de datos: véase *Enmascaramiento de datos*.

Enmascaramiento de datos: mecanismo para proporcionar un acceso parcial a los documentos, mediante la creación de una copia o versión del documento original sobre la que se ha ocultado la información restringida. Cuando lo que se oculta son datos que permiten identificar a personas, se denomina despersonalización o anonimización.

Exclusión o retirada de documentos: mecanismo para proporcionar un acceso parcial a unidades documentales compuestas, retirando de las mismas aquéllos que contienen información restringida. Deberá informarse en todo caso al usuario sobre qué documentos han sido excluidos del derecho de acceso y el motivo concreto de tal exclusión.

Registro de permisos de usuario: categorización de los usuarios en función de sus derechos de acceso.

Requisitos de seguridad y acceso: término genérico empleado en este documento para designar al conjunto de requerimientos de la organización que permiten prevenir acciones no autorizadas sobre sus documentos (acceso, modificación, destrucción), incluyendo las restricciones de acceso.

Restricción de acceso: exclusión de determinadas informaciones del régimen general de libre acceso establecida por la normativa legal para proteger los intereses públicos y privados (seguridad nacional, privacidad, etc.). En virtud de dicha normativa, el acceso a los

documentos que contienen la información afectada se encuentra limitado –con carácter general, por un período de tiempo específico- a determinadas personas, salvo cuando se contemple la posibilidad de ofrecer un acceso parcial.

Revisión de la accesibilidad legal: proceso de valoración de las posibles restricciones al acceso que pueden afectar a los documentos objeto de una determinada solicitud, con el objetivo de informar la toma de decisiones referida a la misma. Se basa en un análisis del contenido de los documentos que recogen la información objeto de solicitud, en relación con el sistema de restricciones vigente.

Tabla de acceso y seguridad: instrumento formal que contemplan las normas ISO 15489 para la identificación de los requisitos de seguridad y acceso aplicables a los documentos, que consiste en una clasificación de categorías de documentos en función de sus restricciones de acceso y condiciones de seguridad.

Testado de documentos: véase *Enmascaramiento de datos*.

5.2. Referencias

AUSTRALIA. STATE RECORDS AUTHORITY OF NEW SOUTH WALES (SRA-NSW). 2003. *Strategies for Documenting Government Business: The DIRKS Manual* [en línea]. Revised edition: January 2007. Kingswood: State Records Authority of New South Wales. [Consulta: 15 diciembre 2014]. Disponible en: http://www.records.nsw.gov.au/recordkeeping/advice/designing-implementing-and-managing-systems/dirks-manual/dirks-manual

AUSTRALIA. STATE RECORDS AUTHORITY OF NEW SOUTH WALES (SRA-NSW). 2011. *How records management techniques and skills can contribute to information security objectives* [en línea]. Kingswood: State Records Authority of New South Wales. Advice: Information Security. [Consulta: 15 diciembre 2014]. Disponible en: http://www.records.nsw.gov.au/recordkeeping/advice/information-security/how-records-management-techniques-and-skills-can-contribute-to-information-security-objectives

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. [Consulta: 15 diciembre 2014]. Disponible en: http://www.oas.org/juridico/PDFs/mesicic4_chl_bue_acc.pdf

ESPAÑA. DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA, PROCEDIMIENTOS E IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA. 2012. *MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información* [en línea]. Versión 3.0. Madrid: Ministerio de Hacienda y Administraciones Públicas. [Consulta: 15 diciembre 2014]. Disponible en: http://administracionelectronica.gob.es/ctt/magerit

INTERNATIONAL ORGANIZATION FOR STANDARIZATION (ISO). 2001. *ISO/TR 15489-2:2001. Information and documentation - Records management - Part 2: Guidelines*. Ginebra: ISO. [Se ha empleado la siguiente versión equivalente en español: AENOR. 2006. UNE-*ISO/TR 15489-2:2006. Información y documentación. Gestión de documentos. Parte 2: Directrices*. Madrid: AENOR].

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. [Se ha empleado la siguiente versión equivalente en español: AENOR. 2012. UNE-ISO 16175-2:2012. *Información y documentación. Principios y requisitos funcionales para documentos en entornos de oficina electrónica. Parte 2: Directrices y requisitos funcionales para sistemas que gestionan documentos electrónicos*. Madrid: AENOR].

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. [Se ha empleado la siguiente versión equivalente en español: AENOR. 2012. *UNE-ISO 16175-3:2012. Información y documentación. Principios y requisitos funcionales para documentos en entornos de oficina electrónica. Parte 3: Directrices y requisitos funcionales para documentos en los sistemas de la organización*. Madrid: AENOR].

INTERNATIONAL ORGANIZATION FOR STANDARIZATION (ISO). 2013. *ISO/IEC 27002:2013. Information technology - Security techniques - Code of practice for information security controls*. Ginebra: ISO.

OPEN SOCIETY JUSTICE INITIATIVE (OSJI). 2013. *The Global Principles on National Security and the Right to Information (Tshwane Principles)* [en línea]. Nueva York: Open Society Foundations. [Consulta: 15 diciembre 2014]. Disponible en: http://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf

ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA). 2010a. *Ley modelo interamericana sobre acceso a la información pública* [en línea]. AG/RES. 2607 (XL-O/10). [Consulta: 15 diciembre 2014]. 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. [Consulta: 15 diciembre 2014]. Disponible en: http://www.oas.org/es/sla/ddi/docs/AG-RES_2841_XL-O-10_esp.pdf

ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA). 2013. *Acceso a la información pública y protección de datos personales* [en línea]. AG/RES. 2811 (XLIII-O/13). [Consulta: 15 diciembre 2014]. Disponible en: http://www.oas.org/es/sla/ddi/docs/AG-RES_2811_XLIII-O-13_esp.pdf

XXXI CONFERENCIA INTERNACIONAL DE AUTORIDADES DE PROTECCIÓN DE DATOS. 2009. *Estándares Internacionales sobre Protección de Datos Personales y Privacidad: Resolución de Madrid* [en línea]. Madrid: Agencia Española de Protección de Datos. [Consulta: 15 diciembre 2014]. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf

5.3. Bibliografía

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. [Consulta: 15 diciembre 2014]. Disponible en: http://www.palermo.edu/cele/pdf/NS-AI.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. [Consulta: 15 diciembre 2014]. Disponible en: http://unesdoc.unesco.org/images/0005/000576/057672so.pdf

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. [Consulta: 7 febrero 2014]. Disponible en: http://hdl.handle.net/10366/111529

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. [Consulta: 15 diciembre 2014]. Disponible en: http://www.metodosdeinformacion.es/mei/index.php/mei/article/view/IIMEI3-N5-153166/768

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. [Consulta: 15 diciembre 2014]. Disponible en: http://redrta.cplt.cl/_public/public/folder_attachment/55/1a/1a3b_6f48.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. [Consulta: 15 diciembre 2014]. 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.

LA TORRE MERINO, J. L.; MARTÍN-PALOMINO Y BENITO, M. 2000. *Metodología para la identificación y valoración de fondos documentales*. Madrid: Ministerio de Educación, Cultura y Deporte. Escuela Iberoamericana de Archivos: Experiencias y materiales.

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. [Consulta: 15 diciembre 2014]. Disponible en: http://www.slideshare.net/JoanSolerJimnez/com-es-fa-un-quadre-de-seguretat-i-accs

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. [Consulta: 15 diciembre 2014]. 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. [Consulta: 15 diciembre 2014]. 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). [Consulta: 15 diciembre 2014]. Disponible en: http://www.palermo.edu/cele/pdf/DatosPersonales_Final.pdf