G06/D01/O

Directrices – Requisitos de seguridad y 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

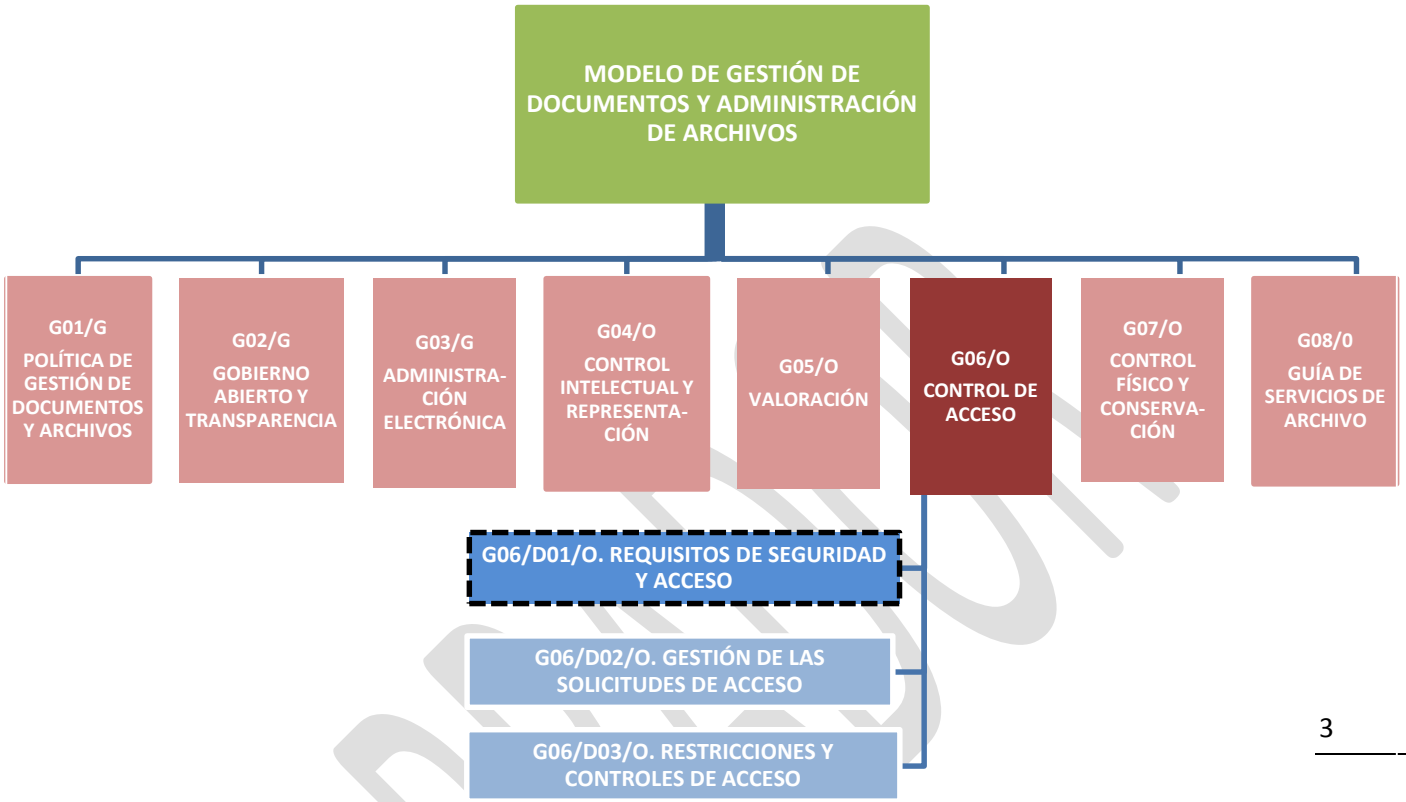
Coordinadores

Beatriz Franco Espiño
Ricard Pérez Alcázar

Equipo

Blanca Desantes Fernández
Francisco Fernández Cuesta
Javier Requejo Zalama

Estas Directrices se integran en el MGD según se especifica en el siguiente Diagrama de relaciones:



1. Presentación y objetivos
    1.1. Finalidad
    1.2. Alcance y contenido
    1.3. Documentos relacionados
2. Requisitos de seguridad y acceso: metodología para su análisis y sistematización
    2.1. Cuestiones preliminares
    2.2. Recopilación de los instrumentos que gobiernan el acceso y la seguridad de la información
    2.3. Clasificación de las categorías de información susceptibles de protección y las cuestiones de seguridad vinculadas a las mismas
    2.4. Vinculación de los requisitos de acceso y seguridad con las series documentales
    2.5. Plasmación en las herramientas funcionales del sistema. Aprobación de la tabla de acceso y seguridad, y mecanismos de revisión
3. Cuadro de compromisos de cumplimiento
4. Términos y referencias
    4.1. Glosario
    4.2. Referencias
    4.3. Bibliografía

1. Presentación y objetivos

1.1. Finalidad

La finalidad de estas Directrices es proporcionar recomendaciones técnicas y metodológicas sobre el proceso de análisis de las restricciones de acceso y los requisitos de seguridad que afectan a los documentos y su sistematización mediante tablas o cuadros de acceso y seguridad, en el marco del Modelo de Gestión de Documentos y administración de archivos de la Red de Transparencia y Acceso a la Información (RTA).

1.2. Alcance y contenido

Paralela a la primordial función de los archivos públicos de garantizar el derecho de acceso a los documentos, se encuentra su responsabilidad 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 muy representativos).

En estas Directrices se propone una metodología básica para analizar y sistematizar los requisitos de seguridad y acceso que afectan a los documentos gestionados por la institución archivística, en un proceso que –en el marco de los sistemas de gestión de documentos diseñados a partir del marco general de ISO 15489- tiene como propósito brindar la herramienta principal –junto con los correspondientes permisos de usuario- del subsistema de control de acceso y uso: el cuadro o tabla de acceso y seguridad, si bien los requisitos identificados pueden incorporarse a otras herramientas del sistema, como los instrumentos de descripción.

Los beneficios de la definición de requisitos de seguridad y acceso de los documentos mediante esta metodología de análisis, y su presentación en forma de tablas de acceso y seguridad son múltiples:

- **Facilita la implementación y puesta en marcha de las políticas de acceso a los documentos públicos y de seguridad de la información**. Cuando la organización carece de dichas políticas, la puesta en práctica de este proceso constituye un punto de partida esencial para el diseño de las mismas desde el punto de vista de la gestión de documentos. De forma similar, constituyen un eficaz complemento a otras políticas, planes y programas de la institución archivística, como los programas de documentos vitales o esenciales.
- **Permite definir de forma racional los controles de acceso y medidas de seguridad del sistema de gestión de documentos**, adaptándose a las necesidades de cada tipo de contenidos, y cumplir de forma eficiente con las exigencias legales y los códigos de buenas prácticas internacionales. Todo ello puede redundar, además, en un aumento de la confianza en el servicio de archivo, en el sistema de transparencia y en las instituciones públicas en general.
- **Permite mejorar la eficacia y disminuir la discrecionalidad del sistema de acceso a los documentos públicos, reduciendo los plazos de respuesta**. Esta metodología permite diferenciar a primera vista las series documentales de acceso libre, de aquéllas que

pueden presentar algún tipo de restricción. Y, en estos casos, proporciona a la autoridad responsable un conocimiento preliminar sólido del tipo de contenidos susceptibles de protección presentes en los documentos objeto de solicitud, por lo que facilita la revisión de accesibilidad concreta que informe la toma de decisiones al respecto (véase el apartado correspondiente en las Directrices *G07/D02/O – Gestión de las solicitudes de acceso*).

- **Por último, este proceso puede permitir identificar y proponer mejoras en la calidad del diseño de los documentos públicos**. Al ampliar y profundizar los análisis de identificación de las series, se puede advertir la existencia de datos susceptibles de protección excesivos o irrelevantes para documentar adecuadamente la actividad o proceso que evidencian.

Ha de advertirse que la seguridad de la información es un proceso transversal (no exclusivo de la gestión de documentos) y complejo, que pretende, en último término, la preservación de la confidencialidad, la integridad y la disponibilidad de la información.

A nivel gerencial, el MGD de la Red de Transparencia y Acceso a la Información (RTA) recoge unas recomendaciones generales (*Directrices G03/D02/G – Seguridad de la información*) sobre seguridad de la información, incluyendo la necesidad de adoptar una política específica al respecto.

A nivel operativo, los documentos asociados a la *Guía G07/O - Control físico y conservación* presentan criterios y medidas específicas para el control físico de los documentos, las instalaciones y los equipos, orientados a preservar su integridad y disponibilidad.

En este marco, el presente documento se centra principalmente en proporcionar orientación para identificar los requisitos de confidencialidad necesarios para dar cumplimiento a las exigencias legales y políticas de la organización, al tiempo que se procura facilitar el ejercicio del derecho de acceso por parte de los ciudadanos. Se complementa con las Directrices *G06/D03/O - Restricciones y controles de acceso*, en la que se definen controles y métodos para dar cumplimiento a los requisitos de confidencialidad identificados.

1.3. Documentos relacionados

G02/G	**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**

G03/D02/G	**Seguridad de la información**

G06/O	Control de acceso
G06/D02/O	Gestión de las solicitudes de acceso
G06/D03/O	Restricciones y controles de acceso

G07/O	Control físico y conservación
G07/D01/O	Plan integrado de conservación
G07/D02/O	Custodia y control de las instalaciones
G07/D03/O	Gestión de contingencias

2. Requisitos de seguridad y acceso: metodología para su análisis y sistematización

2.1. Cuestiones preliminares

Las tablas de acceso y seguridad son el instrumento formal que contempla la norma 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).

En estas Directrices se propone una metodología básica para la elaboración de tablas o cuadros de acceso y seguridad, tanto en el marco del diseño e implementación de un sistema de gestión de documentos (con un enfoque global, sobre el conjunto de los documentos), como de forma progresiva (enfocándose cada vez en una/s agrupación/es documental/es determinada/s), a través del tratamiento archivístico de fondos acumulados o pendientes de tratamiento. De esta forma, la tabla se irá completando progresivamente, a la par que el cuadro de clasificación y el calendario de conservación.

La definición de los requisitos de seguridad y acceso de los documentos en forma de estas tablas o cuadros no es, por tanto, un proceso aislado, sino que ha de incorporarse a las tareas de análisis (identificación) propias de los procesos de clasificación y valoración. No en vano, para su correcta ejecución se requiere un conocimiento profundo del contenido y el contexto de producción y uso de los documentos: las funciones que lleva a cabo la organización, cómo y por qué se ejecutan, qué agentes están involucrados en las mismas, así como la forma en que se documentan. Del mismo modo, resulta especialmente útil aprovechar los análisis y documentos que se generan en el diseño e implantación de políticas y sistemas de gestión de la seguridad de la información -la familia de normas ISO 27000 constituye la principal referencia internacional en este sentido-, siendo tal circunstancia un contexto ideal para acometer un proyecto de elaboración de la tabla de acceso y seguridad.

Teniendo en cuenta estas cuestiones, la metodología que se propone a través de estas Directrices, consta de las siguientes fases, no necesariamente lineales:

- Recopilar las fuentes jurídicas y políticas que han de gobernar el acceso y la seguridad de la información presente en los documentos de la organización
- Definir las categorías de información susceptibles de protección y los plazos de acceso a cada una de ellas a tenor de las fuentes recopiladas, así como los requisitos de seguridad de la información que afectan a la organización
- Identificar las categorías de información susceptibles de protección que contiene cada serie documental y asignar a cada una de ellas los controles de acceso y uso acordes al nivel de seguridad correspondiente a dichas categorías
- Aprobar la tabla de acceso y seguridad y plasmar sus requisitos en las herramientas del sistema.

2.2. Recopilación de los instrumentos que gobiernan el acceso y la seguridad de la información

El primer paso de la metodología que se expone consiste en recopilar los distintos instrumentos jurídicos, políticos y operativos que rigen las cuestiones de seguridad de la información y el acceso a los documentos de la organización.

En particular, se atenderá a las siguientes fuentes:

- **Normas legales y reglamentarias**. Los requisitos habrán de fundamentarse básicamente en aquellas normas que establecen el régimen jurídico de la información pública, en especial, la regulación del ejercicio del derecho de acceso por parte de los ciudadanos y los requisitos legales necesarios para proteger determinadas categorías de información en atención a distintos intereses públicos y privados. Por tanto, se recopilarán la leyes y normas de desarrollo relativas a:
  - transparencia y acceso a la información pública;
  - secretos de Estado e información clasificada;
  - secretos especiales o sectoriales (secreto fiscal, bancario, fiduciario, comercial, industrial);
  - propiedad intelectual;
  - privacidad y protección de datos de carácter personal;
  - seguridad de la información; y
  - gestión de documentos públicos y archivos del Estado.
- **Órdenes y disposiciones judiciales**. Ello incluye las órdenes sobre secreto judicial en procesos específicos y, sobre todo, la jurisprudencia encargada de interpretar la aplicación de las restricciones al acceso.
- **Políticas y normas internas**. Especialmente, se tendrán en cuenta los documentos adoptados por la organización referidos a:
  - políticas institucionales de gobierno abierto y transparencia; en especial, la política de acceso a los documentos públicos;

- políticas y normas internas de seguridad de la información y protección de datos de carácter personal, incluidas las normas técnicas y códigos de buenas prácticas adoptados por la institución;
- planes y programas de conservación, documentos esenciales o vitales y gestión de contingencias, en lo que se refiere a la identificación de activos estratégicos, análisis de riesgos y controles de seguridad para garantizar la integridad de los documentos; y
- políticas, reglamentos internos, manuales de procedimientos e instrumentos internos que gobiernan la gestión de los documentos y la administración de los archivos de la organización.

- **Acuerdos con los propietarios de archivos privados**. Cuando la institución administra archivos y colecciones privadas ingresadas por donación, compra, comodato o cualquier otra fórmula que permita el acceso por parte de terceros, se tendrán en cuenta aquellas disposiciones contractuales que lo regulen.

2.3. Clasificación de las categorías de información susceptible de protección y las cuestiones de seguridad vinculadas a las mismas

Los objetivos de esta tarea son, por un lado, identificar y clasificar las distintas categorías de información susceptibles de protección a tenor de las normas y políticas que afectan a la organización, las restricciones de acceso vinculadas a las mismas y su plazo de prescripción; por otro, identificar las cuestiones de seguridad establecidas en las fuentes establecidas y asociarlas, cuando así esté establecido, con las categorías específicas de información.

Esta fase requiere el análisis exhaustivo de las fuentes recopiladas anteriormente. Así mismo, y como recomiendan las mejores prácticas internacionales, “las áreas de la organización pertinentes deberían ser consultadas a la hora de desarrollar las categorías de restricción de acceso” (ISO/TR 15489-2:2001, 4.2.5.2).

Tomando como base las excepciones a la divulgación que contempla la Ley Modelo Interamericana sobre Acceso a la Información Pública (en adelante LMI), podrían encuadrarse las distintas categorías de información susceptible de protección en tres grupos principales, que se van a identificar, a su vez, con un código de dos letras:

- **Información de acceso restringido y susceptible de protección por razones de interés público (PU)**: bajo esta denominación se engloban aquellas categorías de información cuya divulgación genere un riesgo claro, probable y específico de un daño significativo a la seguridad nacional, a la correcta ejecución de las leyes y las políticas públicas y a cualquier otro interés público protegido de forma explícita por la legislación vigente.

  Mención especial merecen las categorías referidas a **información clasificada de interés para la seguridad nacional** que recogen muchas leyes y acuerdos internacionales sobre esta materia. Ateniéndose a las categorías de información que legítimamente pueden mantenerse en secreto que recoge el principal referente internacional de

buenas prácticas en esta materia, los Principios Globales sobre Seguridad Nacional y Derecho de Acceso a la Información (Principios de Tshwane) de la Open Society Justice Initiative (2013, pp. 19-20), se puede distinguir:

a) Información sobre planes militares en vigor, operaciones en curso y capacidades militares, por el tiempo en que dicha información tiene utilidad operativa.

b) Información sobre la producción, características o uso de armamento y otros sistemas militares, incluyendo los sistemas de comunicación.

c) Información sobre medidas específicas para salvaguardar el territorio del Estado, infraestructuras o institucionales nacionales cruciales contra amenazas, uso de la fuerza o sabotaje, cuya efectividad dependa de su confidencialidad.

d) Información concerniente o derivada de las operaciones, fuentes y métodos de los servicios de inteligencia, en tanto que afecte a cuestiones de seguridad nacional.

e) Información relativa a cuestiones de seguridad nacional, proporcionada por un Estado extranjero o una institución intergubernamental con una advertencia explícita de confidencialidad, y otras comunicaciones diplomáticas en tanto y cuanto afecten a cuestiones de seguridad nacional.

Cuando el ordenamiento nacional contemple algún tipo de categorías o niveles de clasificación para este tipo de contenidos –establecida en función de su mayor o menor "sensibilidad" (así, por ejemplo, algunas normas distinguen entre información "secreta", "reservada" y "confidencial")-, que pueda vincularse directamente con actividades y los documentos que son testimonio de las mismas a tenor de la normativa, se emplearán dichas categorías o niveles, ya que a cada una de ellas, le suele corresponder unas medidas de protección y unos plazos o procedimientos de desclasificación concretos.

Con carácter general, los estándares y marcos de referencia en materia de acceso a la información pública suelen contemplar unos plazos de prescripción de la restricción (bien de aplicación automática, bien previa decisión al respecto de la autoridad competente). En este sentido, la LMI (art. 42) propone un plazo general de 12 años a partir de la fecha de los documentos.

- **Información de acceso restringido y susceptible de protección por razones de interés privado (PR)**: bajo esta denominación se pueden agrupar aquellas categorías heterogéneas de información cuyo acceso pueda afectar a bienes y derechos privados legalmente reconocidos y protegidos. Para identificar este tipo de categorías puede resultar necesario analizar la normativa que regula el sector específico de actividad de la organización. En cualquier caso, la legislación sobre acceso a la información suele contemplar este tipo de excepciones al mismo, incluyendo las referidas a intereses comerciales y económicos legítimos, propiedad intelectual e industrial, etc.

- **Información de acceso restringido y susceptible de protección por contener datos de carácter personal**: se trata de un subconjunto de la información restringida por razones de interés privado, que responde al derecho fundamental a la privacidad y la protección de datos personales. En la actualidad, no existe un referente regional equivalente a la LMI (aunque sí algunas leyes nacionales), por lo que la Organización de Estados Americanos está impulsando la elaboración de "un proyecto de Ley Modelo

sobre Protección de Datos Personales, tomando en cuenta los estándares internacionales alcanzados en la materia" (OEA 2003). Entre estos, se pueden destacar los aprobados en la denominada "Resolución de Madrid" por la XXXI Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (2009), denominados precisamente *Estándares internacionales sobre protección de datos y privacidad*.

Uno de esos estándares es el que identifica una categoría de datos personales susceptibles de una especial protección: los denominados "**datos sensibles**". Suelen considerarse como sensibles aquellos datos de carácter personal que afecten a la esfera más íntima del interesado, o cuya utilización indebida pueda dar origen a una discriminación ilegal o arbitraria, o conllevar un riesgo grave para el interesado. En particular, la Resolución de Madrid considera sensibles "aquellos datos de carácter personal que puedan revelar aspectos como el origen racial o étnico, las opiniones políticas o las convicciones religiosas o filosóficas; así como los datos relativos a la salud o a la sexualidad". Es necesario identificar estas categorías de datos sensibles, así como aquellas otras que establezca la legislación nacional aplicable, ya que suele corresponderles unas condiciones adicionales para su tratamiento y unas medidas de seguridad más estrictas. Por el contrario, y con carácter general, no habrán de tenerse en cuenta como susceptibles de protección los datos de funcionarios y cargos públicos en lo que se refiere exclusivamente con sus actividades públicas.

La limitación del acceso por razones de protección de los datos personales no suele prescribir en una fecha determinada, sino que suele perdurar durante toda la vida de las personas afectadas. Incluso, se puede prolongar más allá, para proteger la memoria de la persona difunta o el honor y la intimidad familiar, especialmente cuando se trata de datos sensibles. Así, la LMI prolonga la protección hasta cumplidos 20 años de la defunción del individuo en cuestión.

La tabla de acceso y seguridad es una herramienta que facilita el control apriorístico del acceso a los documentos (la resolución a procedimientos de acceso a documentos concretos requerirá la revisión de las unidades en cuestión). Por tanto, únicamente se tendrán en consideración los plazos de acceso generales, que tomen como referencia la fecha de los documentos. En el mismo sentido, tampoco se habrán de tener en cuenta las restricciones que no se refieran estrictamente al contenido de los documentos sino a circunstancias variables sobre su tramitación (en ocasiones, previas a su captura en el sistema de gestión de documentos) o su uso con fines de investigación y persecución de delitos. Por ejemplo, siguiendo con el ejemplo de la LMI, se podrían excluir de la tabla las categorías referidas a:

- La información resultado de tareas de asesoramiento interno e interinstitucional (salvo la referida a hechos, análisis de hechos, informaciones técnicas y estadísticas) cuya difusión pueda alterar el correcto transcurso del proceso deliberativo de las autoridades del Estado (LMI, art.40.b.3).
- La información necesaria para la elaboración o desarrollo efectivo de políticas públicas (LMI, art.40.b.4), hasta que la política pública se haya aprobado.

- La información requerida circunstancialmente para la ejecución de la ley o la prevención, investigación y persecución de delitos (LMI, art.40.b.6).
- Los exámenes y auditorías, y procesos de examen y de auditoría (LMI, art.40.b.9), hasta que éstos hayan concluido.

Por otro lado, resulta conveniente también, de cara a una correcta definición de cada una de las categorías, identificar y tener en cuenta los distintos contenidos que son o han de ser objeto de publicidad activa por disposición expresa de la ley. En este sentido, la LMI llama la atención sobre estos supuestos para modular la aplicación de las restricciones al acceso por razones de interés privado (art. 40.a).

Finalmente, habría que identificar, a partir de las fuentes recopiladas en la fase anterior, las **cuestiones de seguridad de la información** que afectan a la organización y establecer, en la medida de lo posible, una vinculación inicial entre los requisitos identificados y las categorías de información definidas. En concreto, en este momento se deberán definir:

- Unos requisitos de seguridad básicos, aplicables al conjunto de documentos gestionados por la institución.
- Reglas, controles y requisitos de mayor nivel, para proteger los activos más "sensibles" de la organización.
- En relación con esto último, se realizará, para cada una de las categorías de información definidas, una primera vinculación con un nivel de seguridad determinado. En este sentido, se tendrán en cuenta los requisitos o controles especiales que la normativa vigente aplicable asocia específicamente a determinadas categorías, como la información clasificada o los datos personales sensibles.

Un ejemplo básico de definición de categorías de información susceptibles de clasificación se presenta, a continuación, en la Tabla 1. Se han obviado las referencias a las cuestiones de seguridad al depender del marco normativo, político y de actividad de cada organización.

Tabla 1. Propuesta básica de categorización

CÓDIGO	CATEGORÍA DE INFORMACIÓN	PLAZO	NORMA
PU01	Seguridad pública y defensa nacional	12 años	LMI, art.40.b.1 y 2
PU02	Relaciones internacionales e intergubernamentales	12 años	LMI, art.40.b.5
PU04	Actividades del Estado para manejar la economía	12 años	LMI, art.40.b.7
PU05	Intereses financieros de la autoridad pública	12 años	LMI, art.40.b.8
PU07	Otros intereses públicos susceptibles de protección	12 años	-
PR01	Intereses comerciales y económicos legítimos	NA	LMI, art.40.a.2
PR02	Patentes	NA	LMI, art.40.a.3

PR03	Derechos de autor	NA	LMI, art.40.a.3
PR04	Secretos comerciales	NA	LMI, art.40.a.3
PR05	Otros intereses privados susceptibles de protección	NA	-
DP01	Datos personales sensibles	NA	LMI, art.40.a.1
DP02	Otros datos de carácter personal protegidos	NA	LMI, art.40.a.1

2.4. Vinculación de los requisitos de acceso y seguridad con las series documentales

El eje central de esta metodología lo constituye el análisis del contenido de las series desde la perspectiva de los requisitos de acceso y seguridad, identificando las categorías de información susceptibles de protección que recoge cada una de ellas y estableciendo al efecto los controles de seguridad apropiados.

Para aplicar a los documentos los requisitos de confidencialidad identificados en la fase anterior, se tomará como unidad básica de análisis la serie documental. Cuando el sistema contemple agrupaciones documentales de nivel inferior a la serie (subseries) que presenten diferencias significativas en lo referido al contenido informativo susceptible de protección, se emplearán dichas agrupaciones menores. La vinculación de los requisitos de acceso y seguridad con series documentales determinadas requiere un conocimiento exhaustivo de las mismas, por lo que será necesario acudir a los repertorios o inventarios de series (La Torre y Martín-Palomino 2000, p. 22; Serra 2013, p. 4) o cualquier otro instrumento que recoja el análisis de identificación (véanse las *Directrices G05/D01/O – Identificación y clasificación*) o información descriptiva pormenorizada de cada serie documental, así como cuando sea necesario, a la propia documentación. Dichos instrumentos se enriquecerán, a su vez, con los resultados de este proceso. Así mismo, se tendrán en consideración los análisis de series paralelas o con contenidos equivalentes elaborados por otras organizaciones del mismo contexto legal y reglamentario.

Este análisis se puede descomponer en las siguientes tareas:

- **Identificar las categorías de información susceptibles de protección que aparecen en los documentos** que componen la serie, de conformidad con la clasificación establecida en la fase anterior. Esta identificación ha de realizarse siempre a nivel de unidad documental compuesta (expediente) y, cuando la profundidad del análisis realizado durante la identificación de la serie lo permita, a nivel de cada uno de los tipos documentales que componen el expediente tipo.

  Se describirán de forma somera los distintos contenidos de cada categoría, así como la frecuencia de su aparición, distinguiendo entre los muy frecuentes (que abundan en la mayor parte de las unidades que componen la serie); frecuentes (suelen aparecer en bastantes documentos de buena parte de las unidades de la serie); o excepcionales (pueden aparecer en algún documento de determinados expedientes). Por ejemplo,

ante una serie de expedientes personales, se podrían identificar las siguientes categorías de datos.

Serie: Expedientes personales		
Categoría	**Descripción**	**Frecuencia**
DP01	Datos sobre la salud: enfermedades padecidas, discapacidades	Frecuentes
DP01	Datos sobre infracciones y sanciones administrativas	Excepcionales
DP02	Datos de identificación: nombre y apellidos, fecha y lugar de nacimiento, fotografía, número de la seguridad social	Muy frecuentes
DP02	Datos económicos: cuantía de las retribuciones ordinarias y extraordinarias	Frecuentes
DP02	Datos de filiación y estado civil: cónyuge, nombre de los padres, datos de identificación de sus descendientes	Frecuentes
DP02	Datos académicos y de capacitación: titulaciones, formación recibida	Frecuentes

- **Asignar a cada serie unos controles de acceso y uso acordes al nivel de seguridad** correspondiente a las categorías de información que contienen. Cuando una serie contenga categorías de información a las que, por prescripción legal, les corresponda un determinado nivel de seguridad, se les asignará dicho nivel por defecto, sin perjuicio de que puedan asignárseles niveles de seguridad más altos tras una evaluación de impacto y análisis de riesgos. Dichos **análisis de riesgos** resultan especialmente útiles para determinar los requisitos y controles necesarios para cada serie, en especial cuando estos no vengan definidos legal o reglamentariamente.

  Los análisis de riegos son una tarea fundamental en la implantación de sistemas de gestión de la seguridad de la información. En palabras de Gómez y Andrés (2012, p. 46), constituyen “una tarea crucial y, en muchos casos, la más laboriosa, por cuanto exige valorar una gran cantidad de parámetros desde múltiples puntos de vista, y suele implicar a multitud de personas que deben llegar a un consenso en sus valoraciones”. Existen diversas metodologías o marcos de trabajo para el análisis de riesgos en seguridad de la información –por ejemplo, en los países de habla hispana se encuentra ampliamente difundido MAGERIT, en la actualidad por su tercera versión (España 2012)-. En general, todas ellas parten de una evaluación de los activos de información, para proponer “una lista de posibles amenazas, unas vulnerabilidades que habrá que considerar y unos baremos para ponderar la probabilidad y el impacto que ocasionaría en la organización que la amenaza se convirtiera en realidad”. A partir de estos parámetros, se pueden obtener unos valores de riesgo de los distintos activos de información (en nuestro caso, de las series documentales) con los que “conseguiremos una imagen dónde radican los mayores riesgos en nuestra organización y, por lo tanto, en qué puntos hay que incrementar el esfuerzo, dónde tendremos que aplicar medidas o mejorar las existentes” (Gómez y Andrés 2012, p. 47). Se recomienda que los modelos avanzados o con un alto grado de madurez asignen los niveles de seguridad (y, con ellos, los controles pertinentes) a partir de análisis de riesgos.

A un nivel más básico, se pueden definir a partir de una evaluación básica del nivel de impacto. Un punto de partida para esta evaluación es el que se propone a continuación:

- Para cada categoría de contenidos de una misma serie, se calculará un nivel de impacto a partir de la siguiente fórmula:

Nivel de impacto = Nivel de confidencialidad X Nivel de frecuencia

- Cuando la serie en cuestión tenga asociadas varias categorías de información susceptible de protección, se tomarán los valores más altos de cada grupo general de contenidos (PU, PR y DP) y se sumarán.
- El Nivel de confidencialidad se puede obtener de un baremos como el que se propone en la Tabla 2:

Tabla 2. Nivel de confidencialidad

Nivel de confidencialidad	Valor	Categorías de información
Muy alto	4	Información clasificada, datos personales sensibles
Alto	3	Información restringida por razones de interés público
Medio	2	Información restringida por razones de interés privado, resto de datos de carácter personal
Básico	1	Resto de contenidos

- El Nivel de frecuencia se obtiene a partir de la siguiente tabla, teniendo en cuenta que el nivel excepcional no ha de aplicarse ante niveles de confidencialidad muy alta.

Tabla 3. Nivel de frecuencia

Nivel de frecuencia	Valor
Muy frecuente	2
Frecuente	1
Excepcional*	0,5

- El Nivel de impacto resultante habrá de confrontarse en una baremos como el que recoge la Tabla 4, para asignar un nivel de seguridad apropiado:

Tabla 4. Niveles de seguridad

Nivel de impacto	Nivel de seguridad
≥ 4	Alto
>1 y <4	Medio
≤ 1	Bajo

- Esta propuesta simplista y deliberadamente conservadora que se propone como punto de partida puede enriquecerse considerablemente si se introducen otros parámetros modificadores en función de otros criterios (por ejemplo, el volumen de la serie, su carácter vital o esencial, su antigüedad en el caso de series cerradas, etc.) en función de las características de la organización. En cualquier caso, los resultados se entenderán provisionales hasta que se basen en un análisis de riesgos detallado.

- **Establecer reglas de control de acceso**: por último, se establecerán para cada serie unas reglas que definan "qué usuarios (agrupados en grupos y roles) pueden realizar

acciones sobre los documentos, y qué tipo de acciones pueden realizar" (Serra 2013, p. 6). Estas reglas permitirán vincular la tabla de acceso y seguridad con el registro de permisos de usuario, definido en las *Directrices G07/D03/O - Restricciones y controles de acceso*. De esta forma, la gestión del proceso de acceso consistiría, básicamente, "en aplicar a cada documento las condiciones de acceso correspondientes a su clase de acuerdo con la tabla de acceso y seguridad; y permitir a cada usuario el acceso y uso de los mismos de acuerdo con dichas condiciones y los permisos que tienen asignados en el registro de permisos de usuario" (Fernández 2011, p. 170).

2.5. Plasmación en las herramientas funcionales del sistema. Aprobación de la tabla de acceso y seguridad, y mecanismos de revisión

Los resultados del análisis han de reflejarse en las herramientas funcionales del sistema, principalmente a través de la tabla de acceso y seguridad, que será aprobada desde el nivel más alto de decisión, previo proceso de participación pública.

Como ya se ha señalado, 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). Es decir, que supone vincular los requisitos identificados en la fase anterior con cada serie representada en el cuadro de clasificación de la organización.

La metodología propuesta permite documentar progresivamente las distintas tareas necesarias. Se considera una buena práctica hacer transparente el proceso, fomentando su difusión para el conocimiento general y, en especial, por parte de la comunidad profesional y los usuarios potenciales. En el mismo sentido, se considera también una buena práctica el establecimiento de mecanismos de comunicación y participación por parte de dichas comunidades, durante la ejecución o la validación de este proceso o, a posteriori, para su revisión. Estos mecanismos pueden ser tanto formales (en especial, a través de comisiones de valoración) como informales (comentarios públicos a través de la web). El cuadro o tabla de acceso y seguridad deberá, finalmente, ser aprobado al más alto nivel posible de la organización, que se encargará también de definir los mecanismos para su revisión periódica y actualización.

Una vez aprobada la tabla, los contenidos de la misma se pueden plasmar en otras herramientas del sistema. En este sentido, las normas internacionales de descripción archivística contemplan elementos destinados a informar sobre la accesibilidad de los documentos de archivo y sus agrupaciones: por ejemplo, los elementos *3.4.1. Condiciones de acceso* y *3.4.2. Condiciones de reproducción* de la norma ISAD (G). En entornos electrónicos, ello supone la asignación de metadatos para la seguridad de los documentos (ISO 23081-1:2006, 9.2.4), tanto en el momento de la creación de los documentos en el seno de sistemas de soporte de procesos de negocio o de su incorporación en el sistema de gestión, como con posterioridad. En el modelo general de metadatos propuesto en las normas ISO 23.081, los

metadatos referidos a los requisitos de acceso y seguridad forman parte del grupo o categoría de metadatos de uso (ISO 23081-2:2009, 9.3).

Ha de tenerse en cuenta, finalmente, que tanto la relación de las distintas categorías de protección como las medidas asociadas a la misma son elementos dinámicos, que varían en función de la consideración social de los mismos, los cambios legislativos o reglamentarios, y el avance en su definición por parte de la doctrina jurídica, los precedentes administrativos y la jurisprudencia. El seguimiento continuo de estas cuestiones permite la actualización de los distintos instrumentos en que se plasman los resultados del análisis de accesibilidad legal y reglamentaria y los controles derivados de los mismos, garantizando, con ello, un cumplimiento óptimo de las obligaciones legales y compromisos éticos del archivo.

3. Cuadro de compromisos de cumplimiento

Este cuadro identifica los compromisos recogidos en la línea de actuación sobre requisitos de seguridad y acceso de la Guía de Implementación de Control de acceso y unas recomendaciones sobre cómo cumplir con los mismos.

El número representado es el mismo con el que se identifica dicho compromiso en la Guía de Implementación.

Nº	Compromisos	Cómo cumplir con los compromisos
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	Identificar y reunir todas aquellas leyes, reglamentos, órdenes y disposiciones judiciales, políticas y normas internas y acuerdos con los donantes que afectan al acceso a los documentos gestionados por el archivo y a la seguridad de la información contenida en los mismos
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	A partir del análisis de las fuentes jurídicas, políticas y operativas recopiladas, se deben identificar las categorías de información susceptible de protección y los plazos de acceso que podrían existir para cada una de ellas Se recomienda agruparlas en tres bloques, referidos a las categorías restringidas por razones de interés público; a las restringidas por razones de interés privado; y a aquellas que contienen datos personales o sobre la privacidad de las personas
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	Reunir, a partir de las fuentes recopiladas, los requisitos legales, políticos y operativos de seguridad de la información que afecten a la organización Clasificar los requisitos identificados en niveles de seguridad, partiendo de un nivel básico, aplicable al conjunto de documentos gestionados por la institución, hasta alcanzar un nivel de seguridad alto, destinado a proteger los documentos más “sensibles” de la organización Posteriormente, establecer una vinculación inicial entre los requisitos identificados y las categorías de información definidas. Esta vinculación será provisional hasta que no se base en los resultados de un análisis de

		riesgos específico
1.4	Identificar las categorías de información susceptibles de protección que contiene cada serie documental	Analizar el contenido de las series desde la perspectiva de los requisitos de acceso y seguridad. Este análisis se realizará sobre los repertorios, inventarios de series o cualquier otro instrumento que recoja un análisis de identificación o información descriptiva pormenorizada de cada serie documental, así como, cuando sea necesario, sobre la propia documentación. Así mismo, se tendrán en consideración los análisis de series paralelas o con contenidos equivalentes elaborados por otras organizaciones del mismo contexto legal y reglamentario Se indicarán las categorías presentes en cada serie, describiéndose de forma somera los distintos contenidos de cada categoría, así como la frecuencia de su aparición
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	Vincular cada serie documental con los controles definidos para el nivel de seguridad correspondiente a las categorías de información que contienen, de conformidad con los requisitos legales y políticos establecidos Para realizar la asignación deberá tenerse en cuenta el valor para la organización de la información que se quiere proteger y el impacto que supondría una brecha de la confidencialidad
1.6	Fundamentar la asignación de controles en un análisis de riesgos detallado	Escoger una metodología de análisis de riegos (por ejemplo, MAGERIT) y actualizar la asignación de controles a partir de los resultados de la misma
1.7	Establecer reglas de control de acceso para cada serie	Definir para cada serie qué grupos y roles de usuarios pueden acceder y realizar acciones sobre los documentos, así como el tipo de acciones que puede realizar cada uno de ellos
1.8	Aprobar la tabla de acceso y seguridad, así como los mecanismos para su revisión periódica	Elevar la tabla para su aprobación por parte de la dirección de la organización Se recomienda someter previamente sus

		contenidos a un proceso de participación que permita incorporar el conocimiento de las distintas partes interesadas
1.9	Definir y asignar metadatos para la seguridad apropiados a cada clase de documentos	Definir los metadatos necesarios para representar las condiciones y requisitos de acceso y uso de los documentos Asignar dichos metadatos en el momento de la incorporación de los documentos en el sistema, a través de la tabla de acceso y seguridad

4. Términos y referencias

4.1. Glosario

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

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

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.

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.

4.2. 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

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]

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

4.3. 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.

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: 15 diciembre 2014]. Disponible en: http://hdl.handle.net/10366/111529

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