G06/D03/O

Directrices – Restricciones y controles 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

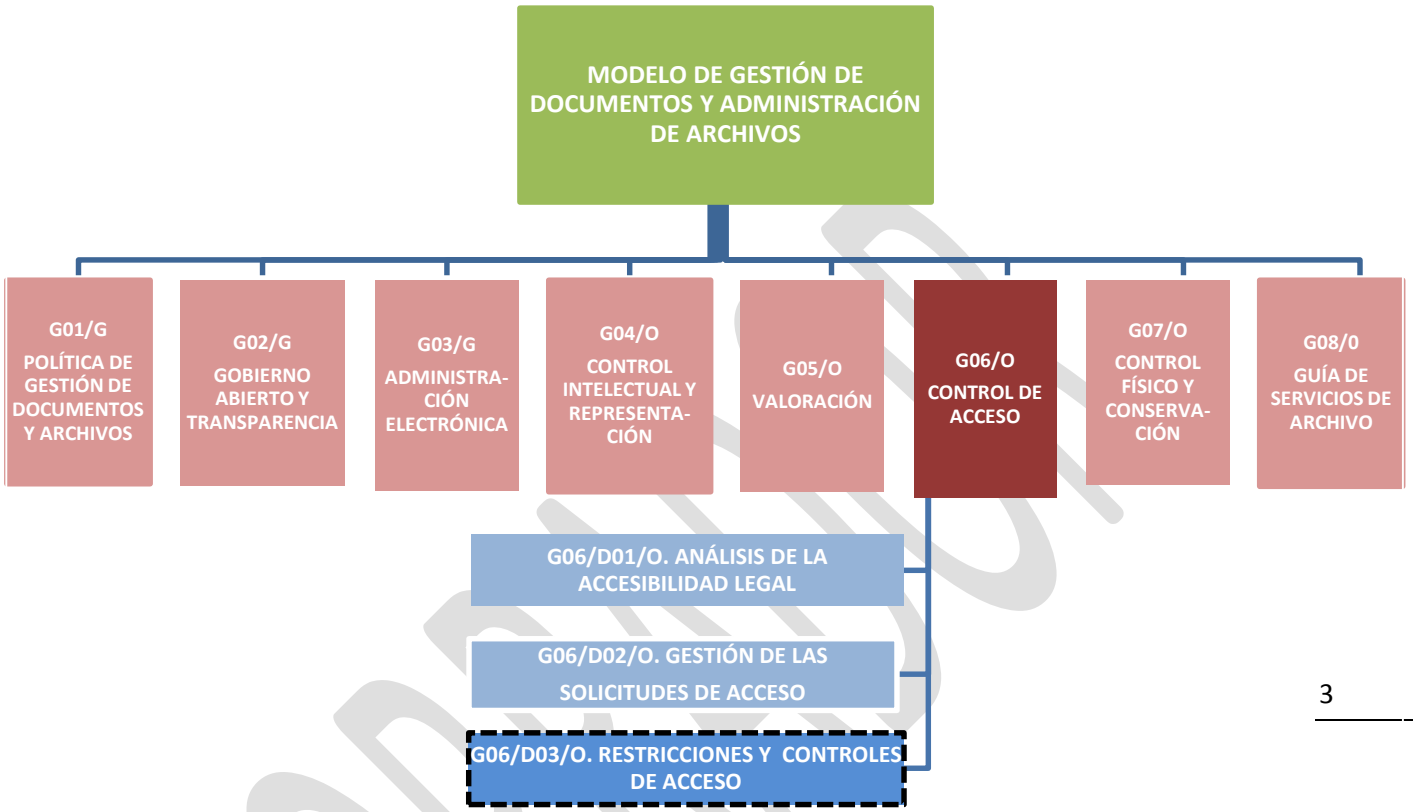
Coordinadores

Beatriz Franco Espiño
Ricard Pérez Alcázar

Equipo

Blanca Desantes Fernández
Francisco Fernández Cuesta
Javier Requejo Zalama

Estas Directrices se integran en el Modelo de Gestión de Documentos y administración de archivos 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. Finalidad

Enmarcadas en el Modelo de Gestión de Documentos y administración de archivos de la Red de Transparencia y Acceso a la información (RTA), estas Directrices pretenden proporcionar una orientación básica sobre la implementación de los requisitos y controles de acceso necesarios para garantizar la confidencialidad de los documentos, cuando así lo establezca la legislación.

1.2. Alcance y contenido

En las Directrices G07/D01/O se propone una metodología para identificar los requisitos de seguridad y acceso que afectan a los documentos gestionados en los archivos públicos. En este documento, en cambio, se recoge una serie de orientaciones sobre la implementación de dichos requisitos a través de dos vías complementarias:

- En primer lugar, mediante el marco general del **control de acceso** de los sistemas de gestión de documentos. Se podría definir el control de acceso como el esquema de mecanismos empleado por el sistema de gestión para evitar el acceso a los documentos a usuarios no autorizados. En este documento se explicará el funcionamiento general de este control de acceso tal y como se plantea en la norma ISO 15489, y se enunciaran los requisitos funcionales que han de contemplar los sistemas que pretendan implementar el control de acceso a documentos electrónicos.
- En segundo lugar, mediante la implementación de las **restricciones de acceso** en 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.

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

G07/O	Control de acceso
G07/D01/O	Requisitos de seguridad y acceso
G07/D02/O	Gestión de las solicitudes de acceso
G07/D03/O	Restricciones y controles de acceso

2. El control de acceso en los sistemas de gestión de documentos

2.1. El acceso a los documentos en las normas ISO 15489

De acuerdo con las normas ISO 15489, entre las funcionalidades que debe contemplar un sistema de gestión de documentos se encuentran las medidas para controlar el acceso, la identificación del usuario, la destrucción autorizada y la seguridad, con la finalidad de evitar el acceso, la destrucción, la modificación o la eliminación de documentos sin autorización (ISO 15489-1:2001, 8.2.3), y poder cumplir los derechos y restricciones establecidos.

> El acceso a los documentos puede estar restringido para proteger: la información personal y la intimidad; los derechos de propiedad intelectual y el secreto comercial; la seguridad de los bienes(físicos o financieros); la seguridad pública; y los privilegios legales y profesionales. Igual importancia revisten los derechos de acceso legalmente reconocidos en virtud de las normas de buen gobierno, la libertad de información, la protección de la intimidad, el ordenamiento jurídico y la legislación archivística (ISO/TR 15489-2:2001, 4.2.5.2).

Los controles de acceso apropiados se garantizan mediante la asignación de un nivel de acceso tanto a los documentos como a los individuos (ISO 15489-1:2001, 9.7). Para ello, las normas técnicas contemplan dos herramientas fundamentales:

- En primer lugar, el **cuadro o tabla de acceso y seguridad**: se trata de una de las principales herramientas de la gestión de documentos, junto con el cuadro de clasificación y el calendario de conservación, y constituye el instrumento formal de identificación de los derechos de acceso y del régimen de restricciones aplicables a los documentos (ISO/TR 15489-2:2001, 4.2.5.1). Las Directrices *G07/D01/O - Requisitos de seguridad y acceso* recogen una propuesta metodológica para su elaboración.

- En segundo lugar, el **registro de permisos de usuario**, que supone una categorización de los usuarios en función de sus derechos de acceso:

  > Un sistema de gestión de documentos ha de gestionar permisos de usuario que le son propios. Puede utilizarse el registro general de empleados y de permisos de usuario de la organización, pero en los casos que no exista, se tendrá que concebir uno propio. Este registro distingue los permisos de usuario para el acceso, la modificación o eliminación de los documentos, de los […] de aquellos de sólo lectura (ISO/TR 15489-2:2001, 4.2.5.2).

  Aunque la norma no establece una metodología específica para su elaboración, sí apunta una secuencia de procesos:

  - identificar las necesidades de acceso de las distintas áreas funcionales de la organización;
  - identificar distintos perfiles de usuario;
  - identificar los usuarios que tienen acceso a grupos concretos de documentos;
  - asignar perfiles de usuario, teniendo en cuenta que "las restricciones de acceso pueden aplicarse tanto dentro de la organización como a usuarios externos" (ISO 15489-1:2001,9.7); y
  - asignar permisos de usuario de acuerdo con los distintos perfiles y los derechos de acceso específicos de los usuarios.

En este marco, la gestión del proceso de acceso debería garantizar que (ISO 15489-1:2001, 9.7):

a) los documentos se dividen en categorías de acuerdo con su nivel de acceso en un momento dado;

b) los documentos sólo se entregan a aquellas personas que estén autorizadas a verlos;

c) los documentos encriptados pueden leerse cuando así se requiera y autorice;

d) los procesos y las operaciones relacionados con los documentos sólo son realizados por quienes están autorizados; y

e) las unidades de la organización responsables de una función concreta atribuyen los permisos de acceso a los documentos de su área de responsabilidad.

Los procesos de control de acceso de conformidad con las normas ISO 15489 consisten, básicamente, en aplicar a cada documento o grupo de documentos las condiciones y requisitos 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.

2.2. Requisitos funcionales para sistemas electrónicos

La norma ISO 16175-2:2011 ha articulado un conjunto de requisitos funcionales para sistemas que gestionan documentos electrónicos, que incluye requisitos específicos sobre controles de acceso y seguridad.

Adaptándolo al esquema apuntado en el apartado anterior, podrían agruparse dichos requisitos de la siguiente manera:

- **Mantener un registro de permisos de usuario, gestionado únicamente por el administrador del sistema**. En este sentido, el sistema de gestión de documentos electrónicos debe:

92	Permitir sólo a los administradores establecer perfiles de usuario y asignar a los usuarios a un grupo.
93	Permitir al administrador limitar a usuarios especificados o grupos de usuarios el acceso a documentos, agrupaciones y a metadatos de gestión de documentos.
95	Permitir únicamente al administrador la posibilidad de cambios de los atributos de seguridad de grupos o usuarios (como derechos de acceso, nivel de seguridad, prerrogativas, asignación y gestión de contraseña inicial).
96	Permitir sólo al administrador adscribir al perfil de usuario atributos que determinen a qué características, campos de metadatos de gestión de documentos, documentos o agrupaciones tiene acceso al usuario. Los atributos del perfil: 1. prohibirán el acceso al sistema que gestiona documentos electrónicos sin un mecanismo de autenticación aceptado atribuido al perfil del usuario, 2. restringirán al usuario el acceso para documentos o agrupaciones específicos,

	3. restringirán al usuario el acceso de conformidad con la autorización dada al usuario, 4. restringirán al usuario el acceso a determinadas características (por ejemplo, lectura, actualización y/o borrado de campos específicos de metadatos de gestión de documentos), 5. denegarán el acceso después de la fecha especificada, y 6. asignarán al usuario un grupo o grupos.
97	Proporcionar las mismas funciones de control por roles y por usuarios.
98	Poder establecer grupos de usuarios que estén asociados con una agrupación.
99	Permitir que un usuario sea miembro de más de un grupo.
110	Permitir la asignación de categorización de seguridad de los permisos de acceso: 1. al nivel de grupo (poder establecer grupos de acceso a agrupaciones específicas, seguridad por clases de documentos o niveles de autorización); 2. por rol organizativo, 3. al nivel de usuario, y 4. en combinación de lo anterior.

- **Establecer categorías de seguridad a los documentos y sus agrupaciones, de conformidad con las tablas de acceso y seguridad y las decisiones sobre la accesibilidad legal de documentos concretos**

94	Permitir al administrador modificar la categoría de seguridad de documentos individuales.
102	Permitir al administrador […] modificar la categoría de seguridad de todos los documentos de una agrupación en una sola operación. El sistema que gestiona documentos electrónicos debe facilitar un aviso si las clasificaciones de seguridad de cualquier documento disminuyen y esperar confirmación antes de completar la operación.
103	Permitir al administrador cambiar la categoría de seguridad de agrupaciones […].
104	Registrar, con todo detalle, cualquier cambio en la categoría de seguridad en los metadatos de gestión de documentos de los documentos, volúmenes o agrupaciones afectadas.
108	Permitir la asignación de clasificaciones de seguridad a los documentos.
109	Permitir la selección y asignación de clasificaciones de seguridad al nivel de sistema para: 1. todos los niveles de agrupaciones de documentos (incluyendo volúmenes), y 2. documentos individuales o entidades documento.
111	Permitir la asignación de una categoría de seguridad: 1. en cualquier nivel de agrupación de documentos, 2. después de un periodo de tiempo especificado o de un evento, y 3. a un tipo de documento.
112	Permitir la aplicación automática por defecto del valor: “No confidencial/no protegido” para una agrupación o documento no asignado a ninguna categoría de seguridad.
114	Poder determinar la categoría de seguridad más alta de cualquier documento en cualquier agrupación por medio de una simple consulta.
115	Permitir revisiones rutinarias programadas de las clasificaciones de seguridad.
117	Poder impedir que una agrupación electrónica tenga una clasificación de seguridad más baja que la de cualquier documento en esa agrupación.

- **Gestionar, de conformidad con los controles establecidos (y documentar),el acceso por parte de los usuarios a los documentos**:

105	Proporcionar una de las siguientes respuestas (a seleccionar en el momento de la configuración) siempre que un usuario solicite acceso o busque un documento, división o agrupación para las que no tengan derecho de acceso: 1. mostrar título y metadatos de gestión de documentos, 2. mostrar la existencia de una agrupación o documento (esto, es, mostrar su número de expediente o de documento), pero no el título u otros metadatos de gestión de documentos, o 3. no mostrar ninguna información del documento ni indicar su existencia de ninguna forma.
106	No incluir nunca, en una lista de texto completo u otros resultados de búsqueda, ningún documento para el que el usuario no tenga derecho de acceso.
107	Anotar todos los intentos no autorizados de acceso a agrupaciones (y sus volúmenes) o documentos en sus correspondientes metadatos únicos.
116	Restringir el acceso a agrupaciones/documentos electrónicos que tengan una clasificación de seguridad más alta que la autorización de seguridad de un usuario.

2.3. El control de acceso como elemento crucial de la seguridad de la información

El modelo establecido en las normas técnicas de gestión de documentos y archivos que se ha definido en los apartados anteriores constituye un marco idóneo para implementar controles y medidas generales de seguridad de la información.

Las *Directrices G03/D02/G – Seguridad de la información* recogen una serie de recomendaciones en materia de seguridad de la información destinadas a su adopción e impulso desde el nivel gerencial de las organizaciones, que se basan en las buenas prácticas establecidas en la norma ISO/IEC 27002. Tanto las organizaciones más avanzadas en esta materia –aquellas que cuentan con una política y un sistema integral de gestión de la seguridad de la información (SGSI) diseñado de conformidad con la familia de normas ISO/IEC 27000- como las que desean implementar de forma progresiva distintos controles y medidas de seguridad de la información, han de contemplar como un elemento crucial el control de acceso a sus activos de información. En este sentido, las mencionadas Directrices recogen los siguientes aspectos a tener en cuenta:

- **Requisitos del negocio para el control del acceso**. Garantía del acceso a la información. Los requisitos de la organización marcarán y serán la base del acceso a la información. Las pautas de control del acceso respetarán la política de divulgación del propio organismo.

- **Gestión del acceso de los usuarios**. Garantía de un acceso autorizado a los sistemas de información y control ante el acceso no autorizado. Cabrán procedimientos formales para controlar los derechos de acceso. Dichos procedimientos abarcarán todo el ciclo del acceso, desde el registro de nuevos usuarios hasta el borrado de aquéllos que ya no requieren acceso. Se tenderá a minimizar el acceso restringido a la información confidencial.

- **Responsabilidades del usuario**. Garantía de control ante accesos no autorizados y vigilancia ante el peligro que corre la información en su tratamiento. Cabrá concienciar a los usuarios autorizados de lo importante de su cooperación en la consolidación de la seguridad de la información. Los usuarios deben ser responsables parciales de la efectividad de los controles, por ejemplo mediante el correcto uso de sus claves secretas, personales e intransferibles, y una correcta atención de los equipos.

- **Control de acceso de red**. Garantía de control ante el acceso no autorizado a los servicios de las redes, internas y externas. El acceso autorizado a las redes no comprometerá la seguridad de los servicios, por lo que se vigilará de:
  a. Existencia de interfaces apropiadas
  b. Aplicación de mecanismos de autenticación adecuados
  c. Obligación del control de acceso del usuario a la información

- **Control de acceso del sistema operativo**. Garantía de control ante el acceso no autorizado a los sistemas operativos. Se considerará el uso de medios de seguridad para restringir el acceso a usuarios no autorizados. Estos medios deben ser capaces de:
  a. Autenticación de usuarios autorizados, según política de control de acceso definida.
  b. Registro de intentos, fallidos y exitosos, de autenticación del sistema.
  c. Registro del uso de privilegios especiales del sistema.
  d. Emisión de alarmas ante la violación de las políticas de seguridad del sistema.
  e. Proporcionar los medios de autenticación apropiados.
  f. Restricción, en su caso, del tiempo de conexión de los usuarios.

- **Control de acceso a las aplicaciones y a la información**. Garantía de control ante accesos no autorizados a la información de las aplicaciones. Se considerará el uso de medios de seguridad para la restricción del acceso a la información y a las aplicaciones. Las aplicaciones deberán estar capacitadas para:
  a. Control del acceso del usuario a la información y a las aplicaciones, según la política de control de acceso definida.
  b. Proporcionar protección ante accesos no autorizados al software del sistema de operación y de software malicioso que supere los controles del sistema.
  c. No comprometer a otros sistemas con los que se comparten recursos.

- **Teletrabajo y movilidad**. Garantía de la seguridad de la información ante el uso de medios móviles. La protección será proporcional al riesgo de estos modos de trabajo, como puedan ser los ambientes desprotegidos, en el caso de la movilidad, y la protección específica del lugar, en el caso del teletrabajo.

La normativa técnica y las mejores prácticas internacionales sobre seguridad de la información recogen mecanismos específicos para el control de acceso en estos ámbitos. Los sistemas de gestión de documentos deberían garantizar, en los niveles avanzados de implementación del MGD de la RTA, la alineación y conformidad de sus procedimientos y mecanismos de control de acceso con las políticas, normas (en especial, la familia ISO/IEC 27000) y buenas prácticas en materia de seguridad de la información.

3. Implementar y revisar las restricciones de acceso

Implementar las restricciones de acceso en los documentos supone, como señala la Guía Técnica para la gestión de archivos de uso restringido del Consejo Internacional de Archivos, el aseguramiento por parte de los archiveros de que el expediente o documento que contiene la información (o una parte de la unidad que pueda ser separada fácilmente del resto) ha sido retirado de los materiales disponibles al público (ICA 2014, I.40).

Se considera una mala práctica sustituir las restricciones por la firma de compromisos de confidencialidad o mecanismos a posteriori referidos al uso de la información: como señala la mencionada Guía Técnica (ICA 2014, J. 41), algunas instituciones archivísticas que no quieren restringir el acceso a los materiales físicos, pero quieren mantener el control sobre el uso final de la información, requieren a los usuarios la firma de un acuerdo de no divulgación o la presentación del borrador de su investigación para su aprobación antes de su publicación. Esto no es una buena práctica, ya que genera un riesgo sustancialmente mayor de que se produzca una divulgación no autorizada de información, sobre todo si se permite a los investigadores obtener copias de materiales restringidos.

Tampoco se considera una buena práctica, con carácter general, retirar las referencias a documentos y agrupaciones de acceso restringido de los instrumentos y sistemas de descripción disponibles. La Guía técnica del ICA recomienda, por el contrario, que estén "incluidos en los instrumentos de descripción aquellos materiales recibidos que no han sido procesados aún, o aquellos que no son de libre acceso" (ICA 2014, A.3), siempre que no se vulneren otros derechos y bienes dignos de protección -principalmente, la privacidad y el derecho a la protección de los datos personales- (ICA 2014, F.27):

> Por ejemplo, si la identidad de una persona es el elemento restringido, el nombre de la persona en el título original del expediente debería reemplazarse con palabras que indiquen que el nombre está restringido y se ha eliminado, por ejemplo, "Denuncias sobre la actividad criminal de [nombre restringido]". Si todas las palabras del título estuvieran restringidas, el resto de elementos de información sobre el expediente (número, fechas extremas, etc.) deberían seguir apareciendo, reemplazándose el título por una expresión del tipo "el título de este expediente está restringido".

Así mismo, se informará adecuadamente, a través de los elementos de descripción destinados a informar sobre la accesibilidad de los documentos de archivo y sus agrupaciones –elementos *3.4.1. Condiciones de acceso* y *3.4.2. Condiciones de reproducción* de la norma ISAD(G)- sobre las circunstancias específicas de una determinada unidad de descripción.

La implementación de las restricciones de acceso incluye, además, la ocultación de la información objeto de protección cuando las leyes permitan un acceso parcial a los documentos. Esta ocultación puede realizarse a través de dos tipos de mecanismos:

- **Enmascaramiento o encubrimiento de datos**: son aquellos mecanismos en los que se genera una copia o versión del documento original, sobre la que se ha extraído u 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**: aquellos casos en que se permite el acceso a determinados documentos de una unidad concreta, pero no a otros, informándose al usuario, en la medida de lo posible, sobre los documentos que han sido excluidos del derecho de acceso y el motivo concreto de tal exclusión.

3.1. Restringir el acceso a los documentos en soporte papel

La Guía Técnica del ICA (2014, I.44) no considera una buena práctica el acceso parcial mediante la ocultación de la información restringida en sobres (esto es, la colocación de las unidades restringidas en sobres cerrados, pero instalados en su expediente de procedencia), ya que los sobres añaden volumen de instalación y su cerramiento puede soltarse o ser retirado con facilidad por los usuarios, exponiendo de esta manera la información confidencial.

En su lugar, propone (ICA 2014, I.43 y 48), cuando el acceso a una unidad documental haya de restringirse en su totalidad o la política de la institución consista en retirar de la consulta pública unidades completas al ser tanta la información restringida que la parte accesible puede resultar engañosa o ininteligible, que el archivero retire la unidad de su emplazamiento original, insertando en su lugar una hoja de testigo (*withdrawal sheets*). Si son muchos los documentos de un mismo expediente (o los expedientes de una misma unidad de instalación) que han de retirarse, puede valer con un único testigo al principio del mismo, en el que se haga relación de todas las unidades retiradas. Al cumplimentar la hoja de testigo, habrá de tenerse cuidado de no revelar la información restringida. Por su parte, los materiales originales retirados se instalarán en unidades de instalación paralelas, almacenadas en un área separada. Este sistema reduce la posibilidad de que la información restringida llegue a manos de los usuarios no autorizados y, según la mencionada Guía, facilita también la eventual reintegración de los artículos.

Por lo que se refiere al enmascaramiento o encubrimiento, se considera una práctica no aceptable cualquier operación que se realice mediante la colocación de cualquier elemento sobre el contenido de documentos originales o cualquier operación que pudiera alterar o dañar la integridad de los documentos.

Si parte de un documento en papel es accesible, ha de realizarse una versión del documento de la que se elimine la información restringida (copia A) y, posteriormente, realizar una copia de uso (copia B) de la anterior. Ha de asegurarse que esta copia de uso muestra claramente dónde, por qué y con qué legitimidad se ha eliminado la información. El uso de papel de color para la copia B puede ayudar tanto a usuarios como a archiveros a distinguirla de otras copias. Entre los métodos para eliminar la información confidencial de la copia A, la Guía técnica destaca (ICA 2014, I.45) los siguientes:

a. recortar la información restringida de la copia A (el efecto “rollo de pianola”), anotar en la copia la legitimidad de las restricciones, y fotocopiar o escanear la página. Resulta útil cubrir el reverso de la página recortada con un papel inconfundiblemente marcado o coloreado al realizar la segunda copia, de manera que los agujeros sean fáciles de ver en la copia B destinada al usuario. Las partes retiradas serán destruidas por medios seguros;

b. tachar la información restringida sobre la copia A con tinta gruesa, anotar la página con la legitimidad de las restricciones, y hacer la copia B (puede que el tachón no tape completamente la información restringida, por lo que puede resultar necesaria una segunda copia);

c. para bloques de texto, colocar un pedazo de papel sobre el bloque restringido de la copia A, anotar la página con la autoridad de las restricciones, y hacer la copia B;

d. escanear la página, eliminar la información confidencial por medios electrónicos, anotar la página, y poner a disposición esta copia electrónicamente, a través de un sitio de acceso público, o mediante copia impresa (la copia impresa puede ser a su vez escaneada para hacerla accesible electrónicamente, eliminando así la posibilidad de que la información redactada puede ser restaurada electrónicamente por el usuario).

3.2. Restringir el acceso a documentos electrónicos

En entornos electrónicos, resulta indispensable representar y controlar la accesibilidad a través de 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 23081, 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).

Las posibilidades de proporcionar un acceso parcial a los documentos han de ser previstas en los requisitos funcionales de los documentos electrónicos y los sistemas de gestión de los mismos. Como señala la Guía técnica del ICA (2014, I. 49), requiere un buen conocimiento técnico de las propiedades del software, que asegure que la supresión de información no puede ser invertida y que dicha información suprimida no se puede recuperar a partir del fichero electrónico proporcionado al usuario. La versión de uso ha de mostrar claramente la eliminación de contenidos. Por ejemplo, en el caso de documentos en forma paginada (un documento textual en pdf.), los datos borrados han de ser reemplazados por marcas que ocupen la misma cantidad de espacio que el texto original para que el usuario pueda comprender el alcance de la eliminación. Si la unidad solicitada está estructurada en forma de base de datos y una fila o columna deben ocultarse, deberá hacerse constar este hecho, informando sobre el tipo de elemento que se ha restringido.

Si el software a disposición de la institución archivística no permite las condiciones expresadas en el párrafo anterior, habrá de disponerse un medio alternativo para el acceso parcial, como la impresión del material en papel (o un extracto del si la solicitud es para un segmento de datos estructurados), empleando cuando resulte necesario alguna de las técnicas señaladas para los documentos en soporte papel y digitalizando esta versión impresa parcial.

3.3. La revisión de las restricciones

Las restricciones al acceso no han de ser, en ningún caso, perpetuas. Resulta indispensable establecer mecanismos que permitan revisar la vigencia de las restricciones existentes y remover, en su caso, los obstáculos que se oponen al libre acceso a la información pública.

Como recoge el décimo de los Principios de Acceso a los Archivos del ICA (2012), "los archiveros dirigen las restricciones, revisan los archivos y eliminan las restricciones que ya no han de ser aplicadas". La revisión de las restricciones supone, por tanto, revertir los procedimientos llevados a cabo, en su caso, para implementarlas. Ello habrá de realizarse:

- Tras el transcurso de plazos legalmente establecidos y recogidos en la correspondiente tabla de acceso y seguridad.
- Como resultado de una decisión administrativa o judicial relativa a una determinada solicitud de acceso. El quinto principio de acceso a los archivos del ICA recuerda que si una decisión autoriza el acceso a documentos previamente restringidos, "éste ha de ser concedido a todo el público en los mismos términos y condiciones". Las decisiones administrativas y judiciales relativas al acceso constituyen una fuente fundamental para la definición de la política de acceso y el sistema de restricciones y pueden resultar útiles para determinar la accesibilidad de categorías de información y agrupaciones documentales más amplias (véanse las Directrices *G07/D01/O - Requisitos de seguridad y acceso*).

Todas las acciones y decisiones llevadas a cabo en relación con la revisión deberán documentarse adecuadamente. En este sentido, la Guía Técnica del ICA defiende su incorporación al denominado registro de control de acceso (véanse las Directrices *G07/D02/O - Gestión de las solicitudes de acceso*), en el que se documentan las acciones y decisiones relativas al acceso a la información contenida en una determinada unidad documental. De esta forma, debería registrarse (2014, 60): la razón de la apertura de la información restringida, la legitimación de la misma y la fecha de tal apertura.

4. Cuadro de compromisos de cumplimiento

Este cuadro identifica los compromisos recogidos en la línea de actuación sobre gestión de solicitudes de 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
3.1	Controlar y representar por medio de los instrumentos y sistemas de descripción los documentos de acceso restringido	Incorporar en los instrumentos y sistemas de descripción aquellos materiales recibidos que no han sido procesados aún o que no son de libre acceso, de forma que no se vulneren otros derechos y bienes dignos de protección -principalmente, la privacidad y el derecho a la protección de los datos personales- Se deberán cumplimentar, además, los elementos de las descripciones destinados a informar sobre la accesibilidad de los documentos de archivo y sus agrupaciones
3.2	Retirar de la consulta pública aquellas unidades completas que sean de acceso restringido	Retirar la unidad (documento, expediente) de su emplazamiento original, insertando en su lugar una hoja de testigo Los materiales retirados de consulta pública se instalarán en otras unidades de instalación, custodiadas en un área separada del resto
3.3	Proporcionar un acceso parcial a documentos mediante el enmascaramiento de los datos confidenciales en copias en soporte de papel	Realizar una copia en soporte de papel del documento (sea originalmente un documento en este soporte o un documento electrónico cuyo contenido pueda imprimirse) de la que se elimine la información restringida (copia A) y, posteriormente, realizar una copia de uso (copia B) de la anterior Sobre esta copia se anotará claramente dónde, por qué y con qué legitimidad se ha eliminado la información. El uso de papel de color para la copia B puede ayudar tanto a usuarios como a archiveros a distinguirla de otras copias

3.4	Disponer de un registro de permisos de usuario	Los registros de permisos de usuario son una categorización de los usuarios en función de sus derechos de acceso. Puede utilizarse el registro general de empleados y de permisos de usuario de la organización, pero en los casos que no exista, se tendrá que concebir uno propio Para ello, se llevarán a cabo las siguientes tareas: - identificar las necesidades de acceso de las distintas áreas funcionales de la organización; - identificar distintos perfiles de usuario; - identificar los usuarios que tienen acceso a grupos concretos de documentos; - asignar perfiles de usuario, teniendo en cuenta que las restricciones de acceso pueden aplicarse tanto dentro de la organización como a usuarios externos; y - asignar permisos de usuario de acuerdo con los distintos perfiles y los derechos de acceso específicos de los usuarios
3.5	Establecer un procedimiento de control de acceso conforme a la norma ISO 15489	Los procesos de control de acceso de conformidad con la norma ISO 15489 consisten, básicamente, en aplicar a cada documento o grupo de documentos las condiciones y requisitos 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. El sistema de gestión de documentos habrá de contar con tales instrumentos, y un procedimiento definido para su aplicación.
3.6	Implementar el control de acceso en el sistema de gestión de documentos electrónicos	Implementar en el sistema de gestión de documentos electrónicos los requisitos funcionales sobre controles de acceso y seguridad establecidos en la norma ISO 16175-2:2011, y que incluyen: - mantener un registro de permisos de usuario, gestionado únicamente por el

		administrador del sistema; - establecer categorías de seguridad a los documentos y sus agrupaciones, de conformidad con las tablas de acceso y seguridad y las decisiones sobre la accesibilidad legal de documentos concretos; y - gestionar, de conformidad con los controles establecidos, el acceso por parte de los usuarios a los documentos (incluyendo la capacidad de documentar cada instancia de acceso) Así mismo, se deberán definir los metadatos necesarios para representar las condiciones y requisitos de acceso y uso de los documentos, y asignar dichos metadatos en el momento de la incorporación de los documentos en el sistema, a través de la tabla de acceso y seguridad

5. Términos y referencias

5.1. Glosario

Acceso parcial: acceso a una 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*.

Anonimización: véase *Enmascaramiento de datos.*

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.

Despersonalización: véase *Enmascaramiento de datos.*

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.

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 autorizadas, salvo cuando se contemple la posibilidad de ofrecer un acceso parcial.

Testado de documentos: véase *Enmascaramiento de datos*.

5.2. Referencias y bibliografía

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

INTERNATIONAL COUNCIL ON ARCHIVES (ICA). 2012. *Principios de Acceso a los Archivos* [en línea]. Trad. de Esther Cruces Blanco. París: ICA. [Consulta: 15 diciembre 2014]. Disponible en: http://www.ica.org/download.php?id=2728

INTERNATIONAL COUNCIL ON ARCHIVES (ICA). 2014. *Guía técnica para la gestión de archivos de uso restringido* [en línea]. París: ICA. [Consulta: 15 diciembre 2014]. Disponible en: http://www.ica.org/download.php?id=3324
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. [Consulta: 15 diciembre 2014]. Disponible en: http://www.ica.org/download.php?id=3164

INTERNATIONAL ORGANIZATION FOR STANDARIZATION (ISO). 2001. *ISO 15489-1:2001: Information and documentation - Records management - Part 1: General*. Ginebra: ISO. [Se ha empleado la siguiente versión equivalente en español: AENOR. 2006. *UNE-ISO 15489-1:2006. Información y documentación. Gestión de documentos. Parte 1: Generalidades*. Madrid: AENOR].

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). 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). 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].