MODELO DE REQUISITOS
PARA LA GESTIÓN DE REGISTROS ELECTRÓNICOS

ESPECIFICACIÓN MoReq

Esta especificación ha sido preparada
por Cornwell Affiliates plc.
para el programa IDA
de la Comisión Europea

Marzo 2001

MODELO DE REQUISITOS
PARA LA GESTIÓN DE REGISTROS ELECTRÓNICOS

ESPECIFICACIÓN MoReq

Esta especificación está disponible en formato electrónico en las siguientes direcciones:

- http://www.europa.eu.int/ispo/ida
- http://www.dlmforum.eu.org
- http://cornwell.co.uk/moreq

Marzo 2001

Marzo 2001

ÍNDICE

1 INTRODUCCIÓN

1.1 Contexto

El foro DLM fue el primero en abordar, en uno de los diez puntos de acción surgidos de su reunión de 1996[1], la necesidad de establecer una especificación exhaustiva de los requisitos de la gestión de los registros electrónicos. Con posterioridad, la DG Empresa de la Comisión Europea encargó el desarrollo de este modelo de especificación como parte del programa de intercambio de datos entre administraciones (IDA).

Tras la celebración de una licitación abierta en 1999, en 2000 comenzó el trabajo en este ámbito, que concluyó a principios de 2001. De su desarrollo se ocupó un pequeño equipo de consultores especialistas de la empresa Cornwell Affiliates plc, que contó con el apoyo y la orientación de un grupo de expertos de varios países, así como con la ayuda de organizaciones de validación pertenecientes tanto al sector público como al privado.

En el anexo 2 se explica con más detalle la metodología aplicada.

1.2 Objetivos y alcance de esta especificación

Esta especificación describe un Modelo de Requisitos para la gestión de registros electrónicos (MoReq) e incide especialmente en los requisitos funcionales de la gestión de registros electrónicos mediante un sistema de gestión de registros electrónicos (SGRE).

La especificación se ha concebido de forma que pueda aplicarse en todas las organizaciones públicas y privadas que deseen introducir un SGRE o bien quieran evaluar la capacidad que ya poseen en tal sentido.

Si bien es cierto que la especificación se centra en los requisitos funcionales, también reconoce la importancia de los atributos no funcionales en la eficacia de un SGRE, como sucede con cualquier otro sistema de información. No obstante, tales atributos no funcionales presentan grandes variaciones según el entorno. Por consiguiente, se procede a su identificación, pero la descripción que de ellos se realiza es muy somera.

También se abordan otros requisitos muy ligados a éstos, tales como la gestión de documentos y la gestión electrónica de registros físicos (p. ej., documentos en

[1] DLM es un acrónimo de la expresión francesa «Données Lisibles par Machine», en español «datos de lectura automática». El foro DLM tiene su base jurídica en las conclusiones del Consejo Europeo, de 17 de junio de 1994, sobre una mayor cooperación en el ámbito de los archivos (94/C 235/03).

papel o microfilm), aunque en menor profundidad. Así, la especificación incluye directrices sobre los requisitos de la gestión de registros físicos, pero no se ocupa con detalle de las funciones relativas al control de los emplazamientos físicos, los códigos de barras, etc. Otras cuestiones relacionadas, como la digitalización y otros medios de creación de documentos electrónicos, escapan al alcance de la especificación. De igual modo, tampoco se pretende abordar la implementación práctica de un SGRE.

Esta especificación se ha concebido partiendo de la premisa de que los usuarios del SGRE no serán solamente los administradores y responsables de archivos, sino también el personal de oficina y operativo que utilice este sistema en su trabajo cotidiano para crear, recibir y recuperar documentos.

Dado que esta especificación se refiere a los requisitos «tipo», se ha concebido con un carácter exclusivamente genérico y no aborda ninguna cuestión específica de una plataforma o sector. Por su naturaleza modular, las comunidades de usuarios pueden reforzar su funcionalidad con características concretas que satisfagan las necesidades de su actividad (para más información sobre la utilización y personalización de esta especificación, véanse la sección 1.6 y el Anexo 3).

1.3 ¿Qué es un SGRE?

La gestión de registros electrónicos es compleja y exige la correcta aplicación de una gran variedad de funciones. Es obvio que el sistema –un SGRE– que colme tales necesidades precisa software especializado, que puede consistir en un módulo especializado, en varios módulos integrados, en software desarrollado a la medida del usuario o en una combinación de varios tipos de programas informáticos. En todos los casos, siempre tendrán que existir procedimientos y políticas que complementen la gestión de forma manual. La naturaleza del SGRE variará según la organización. La presente especificación no presupone la naturaleza de las soluciones individuales de los SGRE. Los usuarios de la especificación tendrán que decidir cómo llevar a la práctica la funcionalidad de un SGRE de forma que responda a sus necesidades.

1.4 ¿En qué casos se puede aplicar esta especificación?

La especificación MoReq se ha concebido para que la utilicen:

- **Los posibles usuarios del SGRE,** como punto de partida en la preparación de una licitación.
- **Los usuarios de SGRE,** en la auditoria o evaluación de un sistema ya existente.

- **Las organizaciones dedicadas a la formación,** como documento de referencia en la preparación de cursos de gestión de registros o bien como material de trabajo en sus cursos.
- **Las instituciones académicas,** como instrumento docente.
- **Los proveedores y creadores de SGRE,** como directriz que guíe el desarrollo de sus productos, destacando las funcionalidades necesarias.
- **Los proveedores de servicios de gestión de registros,** como orientación sobre la naturaleza de los servicios que prestan.
- **Los posibles usuarios de servicios externos de gestión de registros,** como referencia a la hora de especificar los servicios que van a contratar.

La especificación insiste en la facilidad de uso del sistema. Así, el principio director de todo el proyecto ha sido la creación de una especificación que resulte útil en la práctica.

1.5 Puntos fuertes y limitaciones de esta especificación

La especificación MoReq se ha llevado a cabo teniendo siempre en mente el pragmatismo y la facilidad de uso. En principio, se ha concebido como instrumento práctico de ayuda a las organizaciones para satisfacer las necesidades propias de su actividad de gestión de los registros, tanto electrónicos como impresos en papel. Aunque en su desarrollo se han tomado en consideración las disciplinas tradicionales de gestión de archivos y registros, éstas se han interpretado de forma acorde a los entornos electrónicos. Por consiguiente, en la elaboración del modelo de requisitos se han tenido presentes las necesidades de los administradores de los registros físicos y electrónicos.

Si los requisitos incluidos en esta especificación MoReq llegan a aplicarse en la práctica, deberán dar lugar a un sistema que gestione registros electrónicos con el grado de confianza e integridad deseados, aunando las ventajas del método de trabajo electrónico con la teoría clásica de administración de registros. Algunos ejemplos de este enfoque pragmático comprenden la incorporación de requisitos sobre gestión de documentos, flujos de tareas, metadatos y otras tecnologías similares.

Tal y como se explicaba al comentar el alcance del sistema, esta especificación pretende abarcar una amplia gama de requisitos que abarca varios países, industrias y tipos de registro. La amplitud del enfoque es deliberada, pero conlleva una limitación importante: una única especificación no puede aportar unos requisitos que coincidan con los ya existentes de forma exacta, sin necesidad de modificación. En cada país existen tradiciones, perspectivas y exigencias normativas propias en materia de gestión de registros. En ciertos casos, habrá que tomar estas cuestiones en consideración a la hora de aplicar esta especificación MoReq, sobre todo cuando se utilicen en el desarrollo de un nuevo sistema.

Por otra parte, este proyecto no aborda los aspectos prácticos de la gestión de registros. Se ha optado por que la especificación trate únicamente las capacidades necesarias para la gestión de registros electrónicos mediante programas informáticos, eludiendo la discusión de temas como la filosofía de la gestión de registros, las teorías archivistas, la toma de decisiones o el control de la gestión. De tales asuntos se ocupan otras publicaciones, algunas de las cuales hemos enumerado en el Anexo 1. Por citar un ejemplo concreto, la especificación menciona en varias ocasiones que ciertas funciones se han de reservar a un administrador. Ello no significa que los administradores hayan de adoptar decisiones sobre la política de gestión, sino que deben ser los únicos usuarios a los que la organización conceda la facultad de llevarlas a la práctica por medio del SGRE.

Por último, en un esfuerzo por centrar la especificación en el usuario, se utiliza, en la medida de lo posible, la terminología habitual entre quienes trabajan con registros electrónicos. Así, en aras de una mejor comprensión, la especificación describe los ficheros electrónicos como «contenedores» de registros, si bien en sentido estricto tales ficheros no contienen ningún elemento. Para más detalles, véase la sección 2.2.

1.6 Uso de la especificación

Los requisitos detallados en esta especificación se han concebido para ser tomados como modelo. No son prescriptivos en todas las aplicaciones posibles de sistemas de gestión de documentación electrónica, pues en ciertos entornos algunos de ellos no resultan pertinentes. Los distintos sectores empresariales, entornos o tipos de organización, entre otros elementos, impondrán también sus requisitos específicos adicionales. Por consiguiente, antes de proceder a su uso, conviene personalizar la especificación.

Esta especificación se ha preparado de forma que pueda ser utilizada tanto en papel como en versión electrónica. Se ha elaborado con Microsoft Word 97 y Word 2000. Su utilización en la modalidad electrónica presenta una serie de ventajas que se detallan en el Anexo 3.

1.7 Estructura de la especificación

La especificación se ha organizado en capítulos que a su vez se dividen en secciones.

En el capítulo siguiente se ofrece una descripción general de algunos de los requisitos más importantes, comenzando con la terminología clave.

Los capítulos 3 a 11 estudian con detenimiento los requisitos del SGRE. En cada uno de ellos, los requisitos funcionales se agrupan según un criterio lógico. No

obstante, dada la naturaleza de la materia, ha sido imposible evitar cierto solapamiento entre capítulos.

Todos los requisitos se detallan conforme a un patrón establecido, tal y como se indica a continuación.

Los requisitos se presentan en forma de tabla, con un requisito por fila, como ilustra la siguiente figura.

Ref.	**Requisito**
13.1.1	El SGRE debe proporcionar …

Cada requisito tiene asignado un número y se expresa en lenguaje natural.

En el capítulo 12 se identifican los elementos de los metadatos necesarios para satisfacer tales requisitos, exponiéndolos en relación con éstos.

En el capítulo 13 se expone un modelo formal de referencia de SGRE tal y como se concibe en la presente especificación. Dicho modelo se puede utilizar para entender cuestiones clave de la especificación, como las definiciones formales de los términos (por ejemplo, fichero, volumen, nivel) y las relaciones existentes entre ellos (por ejemplo, «qué puede almacenarse en un fichero electrónico»).

En los anexos se pueden consultar detalles sobre documentos administrativos y de referencia, así como otros datos útiles.

1.8 Requisitos preceptivos y requisitos facultativos

En esta especificación:

- El verbo «deber» indica que un requisito se puede considerar preceptivo en la aplicación de la mayoría de los SGRE.
- El verbo «convenir» indica que un requisito se puede considerar facultativo en la aplicación de la mayoría de los SGRE.

1.9 Comentarios sobre la especificación

Si bien no resulta factible entablar correspondencia al respecto, el lector puede enviar sus comentarios y observaciones sobre la presente especificación a la siguiente dirección de correo electrónico:

dlm-forum@cec.eu.int

2 DESCRIPCION GENERAL DE LOS REQUISITOS DE LOS SISTEMAS DE GESTIÓN DE REGISTROS ELECTRÓNICOS (SGRE)

El presente capítulo comienza con la definición de algunos términos de interés (sección 2.1), sigue con una exposición de ciertos conceptos esenciales (sección 2.2) y, por último, presenta un diagrama de relaciones entre entidades que ilustra el modelo en que se basa la especificación (sección 2.3).

2.1 Terminología clave

En esta especificación resulta esencial precisar el significado de ciertos términos. En la medida de lo posible, el significado se corresponde con el que se le confiere en el uso corriente, o con el generalmente admitido en la comunidad de quienes se dedican a la gestión de documentación. Todos los términos se definen en el Glosario (sección 13.1); sin embargo, en esta parte se repiten ciertas definiciones básicas para facilitar su consulta.

Los términos en *cursiva* se definen en el Glosario.

captura

Registro, *clasificación*, adición de *metadatos* y almacenamiento de un *registro* en un sistema que gestiona *registros*.

clase

(sólo en esta especificación) Parte de una jerarquía representada por una línea que va desde cualquier punto del sistema jerárquico de clasificación a todos los ficheros que quedan por debajo.

Nota: Este término se puede corresponder, en la terminología clásica, con una «clase primaria», un «grupo» o una «serie» (o bien una subclase, un subgrupo, una subserie, etc.) de cualquier nivel del sistema de clasificación.

clasificación

Identificación y estructuración sistemáticas de las actividades empresariales o los *registros* en categorías, de acuerdo con convenciones, métodos y normas de procedimientos organizados de forma lógica y representados en un sistema de clasificación.

Fuente: ISO 15489 (proyecto de norma internacional; véase la referencia [9] del Anexo 1).

documento

Información u objeto registrado que se puede tratar como una unidad.

Fuente: ISO 15489 (proyecto de norma internacional; véase la referencia [9] del Anexo 1).

Nota: Un documento puede estar en papel, en microfilm o en un soporte magnético o electrónico de cualquier otro tipo. Puede incluir cualquier combinación de texto, datos, gráficos, sonido, animaciones o cualquier otra clase de información. Un solo documento puede estar formado por uno o varios objetos de datos.

Nota: Los documentos se diferencian de los *registros* en varias cuestiones esenciales. Véase *registro*.

fichero electrónico

Conjunto de *registros electrónicos* relacionados entre sí.

Fuente: Especificación funcional de «fichero electrónico» de la Public Record Office (véase la referencia [2] del Anexo 1).

Nota: Este término se emplea a menudo en sentido amplio para designar los *volúmenes electrónicos*.

metadatos

(en el contexto de gestión de registros) Información estructurada o semiestructurada que permite la creación, la gestión y la utilización de registros a lo largo del tiempo, tanto dentro de los mismos ámbitos en que se crearon como entre ellos.

Fuente: Definición de trabajo del Archiving Metadata Forum (http://www.archiefschool.nl/amf).

Nota: La distinción entre datos y metadatos puede resultar algo confusa. Así, por lo general parece evidente que los datos esenciales utilizados en la indexación de un registro (título, fecha, etc.) forman parte de los metadatos del registro; en cambio, la pista de auditoría de un registro y el calendario de conservación se pueden considerar tanto datos como metadatos, dependiendo del contexto. Por ejemplo, se pueden definir distintos tipos de metadatos en relación con la indexación, la conservación, la reproducción, etc. Estas características del uso de los metadatos quedan dentro del ámbito de aplicación de la especificación MoReq.

registro

Documento o documentos elaborados o recibidos por una persona u organización en el curso de su actividad y conservados por esa persona u organización.

Fuente: Adaptado de la especificación funcional de la Public Record Office (referencia [2] del Anexo 1).

Nota: También se pueden aplicar definiciones nacionales locales.

Nota: Un registro puede constar de uno o varios *documentos* (como sucede cuando un documento tiene anexos) y estar en cualquier soporte y formato. Además del contenido del documento o los documentos, debe incluir información contextual y, cuando proceda, estructural (esto es, información que describa los componentes del registro). Una característica esencial de un registro es que no se puede modificar.

registro electrónico

Un *registro* en soporte *electrónico*.

Nota: Puede estar en soporte electrónico porque ha se ha creado mediante un programa informático de aplicación o bien porque se ha digitalizado, esto es, se ha escaneado un documento en papel o microfilm.

SGRE

Sistema de gestión de registros electrónicos.

Nota: El SGRE difiere del *sistema de gestión electrónica de documentos (EDMS, por sus siglas en inglés)* en varios puntos clave. Para más detalles, véase la sección 10.3.

sistema de clasificación

Véase clasificación.

Fuente: Definición de «Sistema de clasificación» en ISO 15489 (proyecto de norma internacional; véase la referencia [9] del Anexo 1).

Nota: Los sistemas de clasificación se suelen representar como jerarquías.

volumen

Subdivisión de un *fichero electrónico* o *en papel*

Fuente: Definición de «parte» en la especificación funcional de la Public Record Office (referencia [2] del Anexo 1).

Nota: Las subdivisiones se establecen para facilitar la gestión del contenido de los ficheros mediante la creación de unidades que no resulten demasiado grandes o difíciles de manejar. Las subdivisiones se realizan en función de criterios más mecánicos (por ejemplo, basadas en el número de registros, en series de números o en lapsos de tiempo) que intelectuales.

2.2 Conceptos esenciales

La comprensión de esta especificación exige el dominio de ciertos conceptos esenciales:

- Registro y registro electrónico
- Fichero y volumen electrónico
- Sistema de clasificación
- Clase
- SGRE
- Captura de registros
- Perfil del usuario

Registro y registro electrónico

La Guía de la información electrónica del foro DLM (sección 2.4 de la referencia [6] del Anexo 1) sugiere que los registros se consideren elementos formados por:

- Contenido
- Estructura
- Contexto
- Presentación

El contenido está presente en uno o más documentos físicos o electrónicos que transmiten el mensaje del registro y se almacenan de un modo que permite a los futuros usuarios entender los registros y su contexto. Por ello, un registro incluye, además del contenido de sus documentos, información sobre el contexto y la estructura del documento. La presentación depende tanto de los contenidos de los registros como de su estructura y, cuando se trata de registros electrónicos, del software empleado en su representación.

La gran mayoría de los registros físicos están en soporte papel y se guardan en ficheros, constituidos físicamente por uno o más volúmenes de registros introducidos en carpetas de papel. Los controles de procedimientos deben impedir que los usuarios modifiquen los registros o su posición dentro de los ficheros.

Cuando se trata de registros electrónicos, se aplican conceptos similares. Un registro está formado por uno o más documentos electrónicos, que pueden ser documentos elaborados con un procesador de textos, mensajes de correo electrónico, hojas de cálculo, imágenes fijas, animaciones, ficheros de audio o cualquier otro tipo de objeto digital. Los documentos se convierten en registros cuando se seleccionan, esto es, cuando se «capturan» en el SGRE. Una vez capturados, los registros se «clasifican», lo que quiere decir que se les asignan códigos que se corresponden con la clase del sistema de clasificación a la que pertenecen, con lo cual se pueden manejar dentro del SGRE.

Ficheros y volúmenes electrónicos

Los registros en papel se acumulan en ficheros en papel, guardados en carpetas también de papel. En un SGRE, éstos se pueden gestionar como si se acumulasen en ficheros electrónicos y se almacenasen en carpetas electrónicas. En sentido estricto, los ficheros y carpetas electrónicos no precisan una existencia real, son virtuales, pues en realidad no «contienen» nada: no son más que los atributos de los metadatos asociados a los registros que se han colocado en ellos. Además, en muchos casos no es preciso que en el sistema electrónico exista una distinción real entre fichero y carpeta. No obstante, el usuario del SGRE no suele ser consciente de tales sutilezas: el software de aplicaciones que gobierna el sistema permite que los usuarios vean y manejen las carpetas como si éstas guardasen los documentos físicos asignados lógicamente a los ficheros. En la presente especificación se

adopta este enfoque centrado en el usuario. Por consiguiente, en aras de una mejor comprensión, el resto de la especificación describe los ficheros electrónicos como «contenedores» de registros. Téngase en cuenta, no obstante, que, si bien la especificación aporta los requisitos funcionales de la gestión de los ficheros electrónicos, no indica cómo se debe aplicar el concepto de fichero electrónico.

En ocasiones, los ficheros se dividen «mecánicamente» en volúmenes conforme a criterios predeterminados. Con el término «mecánicamente» queremos expresar simplemente la adherencia a tales convenciones, que no se basan en el contenido intelectual de los ficheros sino en su tamaño, el número de registros que contienen o sus ciclos vitales. Esta práctica surgió en la gestión de los ficheros de papel con el propósito de restringir su tamaño y su peso a valores manejables y se puede seguir aplicando cuando se trata de ficheros electrónicos, con objeto de limitar su tamaño a valores asequibles para la evaluación, la transferencia o cualquier otro procedimiento relacionado con su gestión.

Aunque la distinción entre ficheros y volúmenes de ficheros parece evidente, sus implicaciones resultan menos obvias. Ello se debe a que las consecuencias de la elección de una división de ficheros en volúmenes varían en función de las necesidades del sistema. Las diferencias surgen cuando:

- Se cierran ciertos ficheros transcurrido un intervalo de tiempo limitado, de modo que la unidad utilizada en la gestión es el fichero (si bien un fichero puede estar formado por varios volúmenes). Como ejemplos podemos citar un fichero de una contratación concreta de pequeña magnitud o bien el fichero de un proyecto.

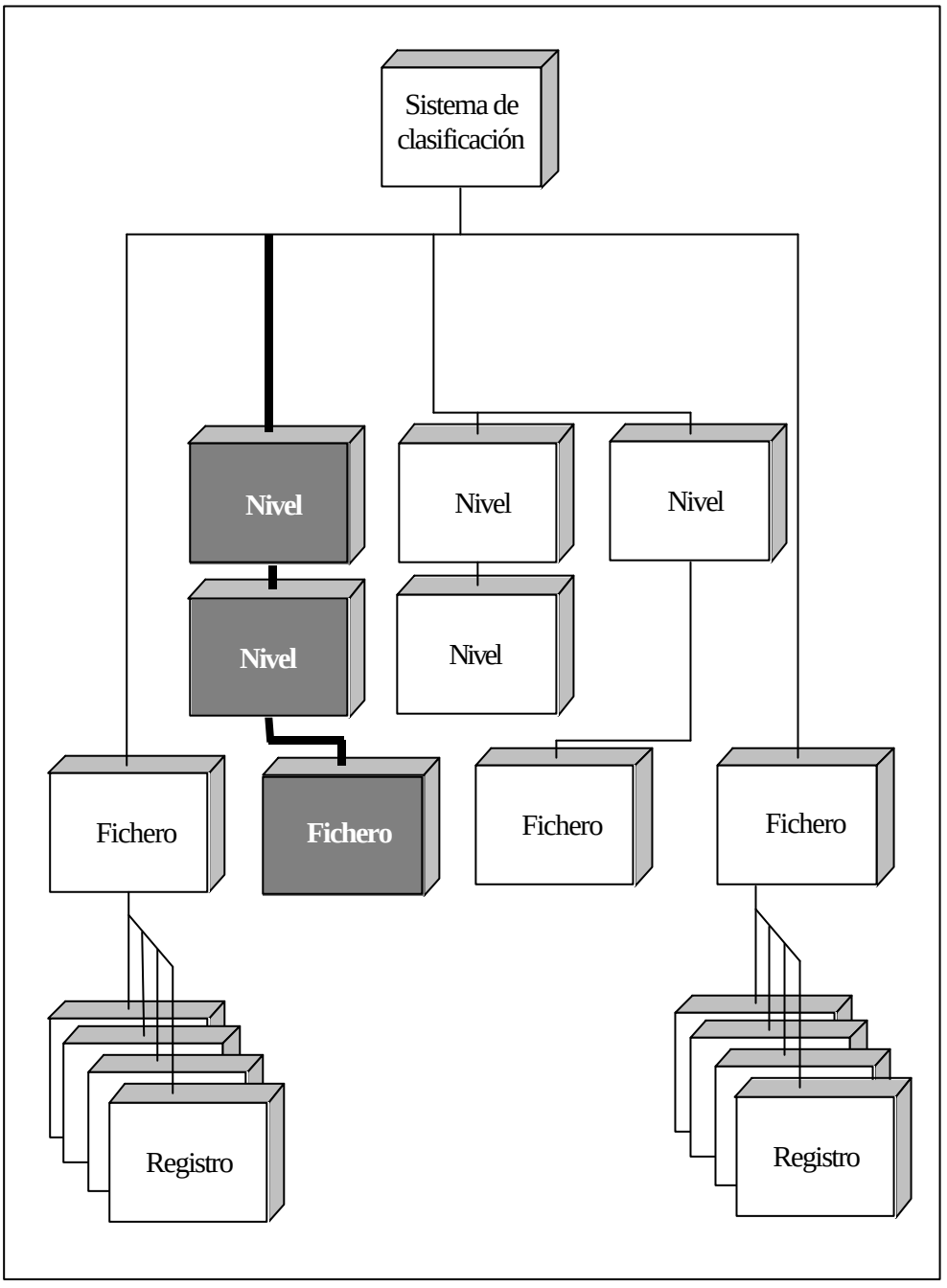
- Algunos ficheros tienen un ciclo vital ilimitado o casi ilimitado, de modo que la unidad empleada en la gestión es el volumen. Como ejemplos podemos citar un fichero de registros sobre una región geográfica o un fichero que trate de una materia en la que no influya el transcurso del tiempo, como sucede con ciertas políticas, o bien un fichero de facturas, en el que cada año comienza un nuevo volumen.

Sistema de clasificación

Con la gestión de registros, los ficheros se añaden respetando una estructura que, de acuerdo con las buenas prácticas, debería reflejar las funciones de la actividad en cuestión. La representación de esta agregación se denomina «sistema de clasificación». En general, el sistema de clasificación consiste en una jerarquía, si bien podría apoyarse en un tesauro y no poseer una naturaleza jerárquica. El resto de la presente especificación se centra en el enfoque jerárquico.

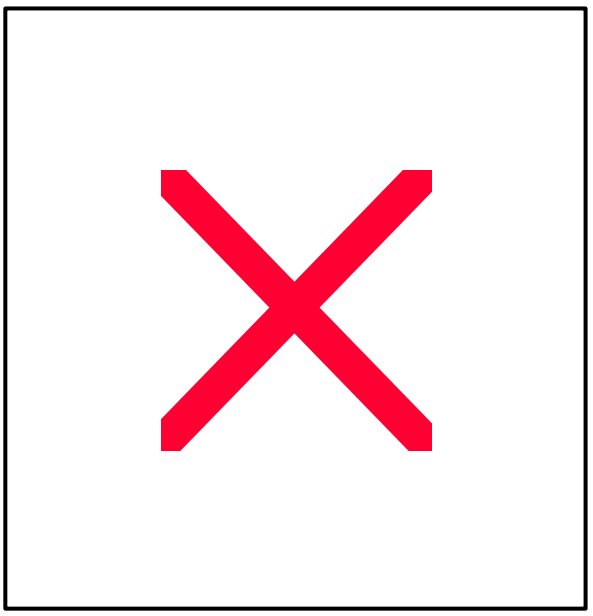
Del mismo modo que los ficheros parecen tener una existencia real aun cuando no son más que una mera acumulación de registros, los niveles más altos de la jerarquía del sistema de clasificación también parecen reales, pese a ser solamente una simple agregación de ficheros o niveles inferiores. Tal y como sucedía con los

ficheros, la presente especificación fija unos requisitos en relación con la jerarquía, pero sin intervenir en el modo en que se aplican.



Los ficheros pueden estar presentes en cualquier nivel de la jerarquía, como se observa en la figura anterior, adaptada de la norma ISAD (G) (referencia [7] del Anexo 1).

Téngase en cuenta que este gráfico sólo pretende mostrar ciertas relaciones potenciales entre niveles, ficheros y registros, y no refleja todos los niveles ni todas las disposiciones posibles.



Clase

Esta especificación utiliza el término «clase» para referirse a la porción de una jerarquía representada por una línea que va desde cualquier punto de la jerarquía a todos los ficheros que quedan por debajo de ella. Por consiguiente, el término «clase» corresponde a lo que en algunos textos se denomina «grupo» o «serie» (o subgrupo, subserie, etc.).

En términos visuales, una clase de una jerarquía corresponde a una rama de un árbol, de modo que puede incluir otras clases, tal y como las series contienen subseries y subsubseries. Las casillas sombreadas y las líneas gruesas del diagrama de la derecha constituyen un ejemplo de clase.

La presente especificación no pretende establecer un método de preparación de un sistema de clasificación. Esta cuestión se trata en otras publicaciones, como el trabajo del proyecto UBC-MAS (referencia [8] del Anexo 1).

Sistema de gestión de registros electrónicos (SGRE)

A grandes rasgos, un SGRE es una aplicación destinada a la gestión de registros electrónicos, si bien también se puede utilizar en la gestión de registros físicos. Esta especificación se centra expresamente en la gestión de los registros electrónicos.

Un SGRE suele estar estrechamente integrado en un sistema de gestión electrónica de documentos. En términos técnicos, un SGRE gestiona registros, mientras que un EDMS se ocupa de documentos (que no son registros). No obstante, puede resultar difícil delimitar su funcionalidad, sobre todo cuando se utilizan como instrumentos que facilitan el trabajo cotidiano. Este tema se trata con mayor profundidad en la sección 10.3, sobre cuestiones relacionadas con la Gestión de documentos.

Captura de registros

Los documentos elaborados o recibidos en el curso de la actividad se convierten en registros cuando se seleccionan, esto es, «se capturan» en el SGRE. En esta captura, se «clasifican», es decir, se les asignan códigos que hacen referencia a la

clase a la que pertenecen, lo que permite que el sistema los gestione. También se les asigna un identificador único.

En muchos casos los documentos seleccionados o capturados se convierten en registros cuando se vinculan a un proceso empresarial, tal y como sucede, por ejemplo, con un flujo de tareas. Así, cuando se genera una factura se tendría que producir de forma automática la captura de un registro. En otros casos puede existir una política por la que cualquier documento relacionado con un asunto de la empresa tenga que convertirse en un registro, aun cuando no intervenga de manera oficial en un proceso empresarial. Y en otras circunstancias, será el usuario el que inicie de forma selectiva el proceso de captura. La determinación de los documentos que deberían capturarse en el sistema de registros se tendría que basar en un análisis del entorno normativo, de los requisitos de contabilidad y de la actividad de la empresa, así como de las contrapartidas que conllevaría su no captura. Un ejemplo sería un memorando de una organización que se ocupe de temas políticos. La organización podría decidir que sólo los memorandos que se considerasen importantes pasaran a convertirse en registros (esto es, que los memorandos sin interés, como los relativos a las cuestiones de organización de una reunión, no formasen parte de tales registros). La presente especificación pretende ofrecer una respuesta ante cualquiera de esas posibilidades. En otras palabras, esta especificación MoReq describe un sistema ofimático de uso general, no simplemente un sistema de gestión de registros para ciertas clases de aplicaciones o para uso exclusivo de archiveros o administradores.

Perfil del usuario

Esta especificación considera que existen dos tipos de usuarios:

«Usuario» ..... Cualquier persona con acceso autorizado a la aplicación del SGRE. En la práctica, todas las personas que elaboran, reciben, revisan o utilizan los registros y quienes administran el SGRE.

«Administrador» ..... Un usuario que gestiona los registros almacenados en el SGRE y el sistema en sí, junto con sus bases de datos.

En la práctica, la mayoría de las organizaciones dispondrán de más de una persona que desempeñe tales funciones, y muchas de ellas definirán otras funciones nuevas. Para más información, véase la sección 13.4.

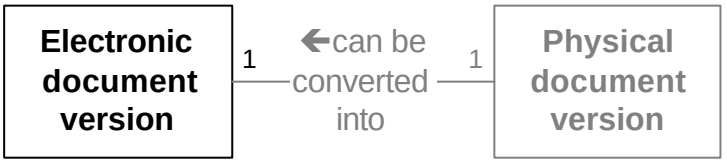
2.3 Modelo de relación entre entidades

En esta sección se expone un modelo de relación entre entidades que puede facilitar la comprensión de la especificación. La sección 13.3 incluye una exposición detallada a tal respecto.

Una característica notable de este diagrama es que no representa estructuras reales almacenadas en el SGRE, sino un enfoque de los metadatos asociados a los registros. Un SGRE utiliza estos metadatos en la gestión de sus registros de igual forma que si la estructura mostrada en el diagrama existiese de veras. Para una explicación más pormenorizada de esta cuestión, véase la sección 2.2 .

Las relaciones entre ficheros, volúmenes, registros y demás entidades se muestran de forma más rigurosa en el siguiente diagrama sobre las relaciones entre entidades, que constituye una representación formal de ciertas estructuras que conforman un SGRE.

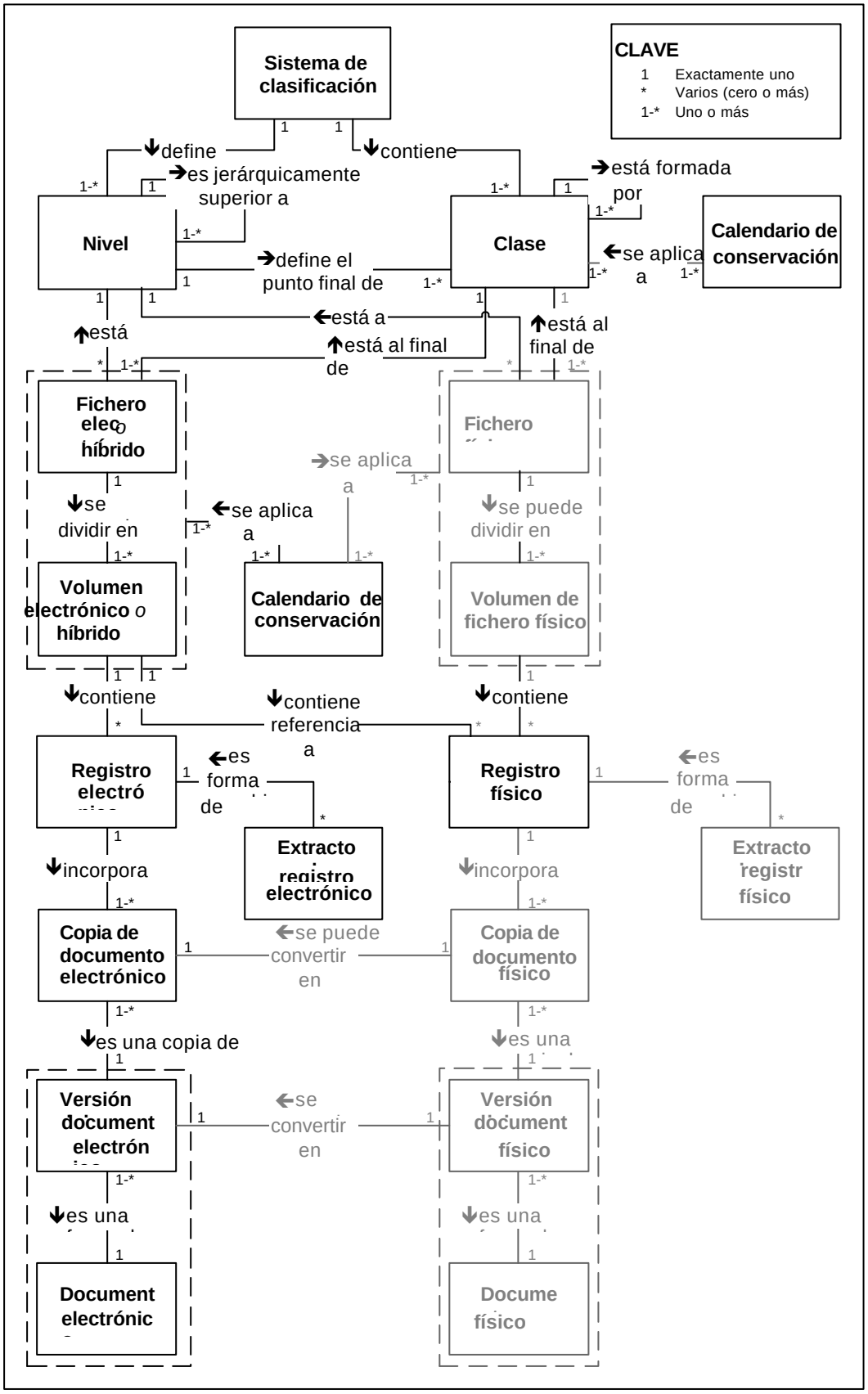
En el diagrama, las entidades (ficheros, registros y demás) se representan mediante rectángulos y las líneas que los unen representan las relaciones entre entidades. Cada relación se describe en el centro de la línea con un texto que se debería leer en la dirección de la flecha. A cada extremo de la línea que representa la relación se encuentra un número que hace referencia a la frecuencia (en sentido estricto, la cardinalidad) y que se explica en la clave. Así por ejemplo, el siguiente fragmento del diagrama:



Versión electrónica del documento ←se puede convertir en Versión física del documento

significa «Una versión física del documento se puede convertir en una versión electrónica del documento» (obsérvese la dirección de la flecha).

Nótese que la entidad «clase» se relaciona consigo misma en virtud de la relación «está formada por». Esta relación recurrente describe, en términos formales, la jerarquía de las carpetas, en las que una clase puede contener a otra. Del mismo modo, un nivel puede estar en una posición jerárquicamente superior a la de otros niveles.


Sistema de clasificación
CLAVE
1 Exactamente uno
* Varios (cero o más)
1-* Uno o más
define
contiene
es jerárquicamente superior a
está formada por
Nivel
Clase
Calendario de conservación
define el punto final de
se aplica a
está a
está al final de
está
está al final de
Fichero electrónico o híbrido
Fichero
se aplica a
se dividir en
se aplica a
se puede dividir en
Volumen electrónico o híbrido
Calendario de conservación
Volumen de fichero físico
contiene
contiene referencia a
contiene
Registro electrónico
es forma de
Registro físico
es forma de
Extracto registro electrónico
Extracto registro físico
incorpora
incorpora
Copia de documento electrónico
se puede convertir en
Copia de documento físico
es una copia de
es una
Versión document electrónica
se convertir en
Versión document física
es una
es una
Document electrónic
Docume física

3 SISTEMA DE CLASIFICACIÓN

El sistema de clasificación constituye el elemento clave de cualquier SGRE, tal y como se describe con detalle en la sección 2.2. Define el modo en que los registros electrónicos se organizarán en ficheros electrónicos, así como las relaciones entre los ficheros.

La sección 3.1. de este capítulo se ocupa de los requisitos necesarios para la creación del sistema de clasificación. A continuación se citan los requisitos de las clases y ficheros (sección 3.2) y de los volúmenes (sección 3.3). En la última sección (3.4) se enumeran los requisitos relativos al mantenimiento del sistema de clasificación.

3.1 Configuración del sistema de clasificación

Ref.	Requisito
3.1.1	El SGRE debe permitir la utilización del sistema de clasificación de la organización y ser compatible con él.
3.1.2	El SGRE debe permitir la utilización de un sistema de clasificación en el que los ficheros se puedan representar dispuestos en una jerarquía con un mínimo de tres niveles. *Los tres niveles se consideran el mínimo esencial; en ciertos entornos serán necesarios más.*
3.1.3	Conviene que el SGRE no restrinja el número de niveles de la jerarquía del sistema de clasificación.
3.1.4	El SGRE debe permitir que en el momento de la configuración se definan mecanismos de denominación.
3.1.5	El SGRE debe permitir la elaboración inicial de un sistema de clasificación en el momento de la configuración, de forma que sea posible proceder a la captura o la importación de registros.
3.1.6	El SGRE debe permitir a los administradores añadir nuevas clases en cualquier posición dentro de una clase, siempre y cuando los ficheros no se almacenen en el punto en cuestión. *Téngase en cuenta que esto puede suceder en cualquier nivel.*
3.1.7	Cuando el SGRE posea una interfaz gráfica, ésta deberá permitir la navegación y la exploración, en un entorno visual, de los ficheros y la estructura del sistema de clasificación, así como la selección, la recuperación y la presentación de los ficheros electrónicos y su contenido por medio de tal mecanismo.

Ref.	Requisito
3.1.8	Conviene que el SGRE permita la definición y el uso simultáneo de varios sistemas de clasificación. *Esto puede ser necesario, por ejemplo, tras la fusión de dos organizaciones; sin embargo no está previsto que esta característica se use habitualmente.*
3.1.9	Conviene que el SGRE permita el uso de un sistema de clasificación distribuido cuyo mantenimiento se pueda realizar a través de una red de depósitos de registros electrónicos.

3.2 Clases y ficheros

En esta sección se enumeran los requisitos aplicables a las clases y los ficheros.

Ref.	Requisito
3.2.1	El SGRE debe soportar los metadatos de ficheros y clases en el sistema de clasificación. Una vez se ha capturado un registro, el sistema debe reservar a los administradores la capacidad de añadir o modificar sus metadatos. *En el capítulo 12 se describen los requisitos de los metadatos.*
3.2.2	El SGRE debe permitir la aplicación de al menos dos mecanismos de denominación de ficheros electrónicos y clases en el sistema de clasificación: • Un mecanismo que asigne un código de referencia con una estructura numérica o alfanumérica, es decir, un identificador único en todo el sistema de clasificación (véase el capítulo 7) a cada fichero electrónico. • Un mecanismo que asigne un texto como título a cada fichero electrónico. Debe ser posible aplicar ambos identificadores de forma conjunta o independiente en la misma aplicación.
3.2.3	El SGRE debe permitir a los administradores añadir (abrir) ficheros en el nivel más bajo de cualquier clase del sistema de clasificación. *Téngase en cuenta que no tiene por qué existir una coincidencia en las cotas de los niveles inferiores de todas las clases.*
3.2.4	El SGRE debe grabar la fecha de apertura de una nueva clase o fichero e incluirla entre los metadatos del fichero.

Ref.	Requisito
3.2.5	Siempre que se abra una nueva clase o fichero, el SGRE deberá, de forma automática, incluir entre en sus metadatos los atributos relacionados con su posición en el sistema de clasificación (por ejemplo, el nombre y código de clasificación). *Así, si un fichero denominado «Correspondencia» está en una trayectoria jerárquica:* *Desarrollo del plan regional: Consulta pública: Correspondencia* *y el administrador añade un nuevo fichero denominado «Objeciones formales» en el mismo nivel que el fichero de «Correspondencia», el primer fichero deberá heredar de forma automática el prefijo «Desarrollo del plan regional: Consulta pública».*
3.2.6	Conviene que el SGRE admita una clase facultativa y un mecanismo de denominación de ficheros que se basen en términos incluidos en un vocabulario controlado y en relaciones extraídas de un tesauro que satisfagan la norma ISO 2788 o la ISO 5964. Asimismo, es conveniente que permita la vinculación del tesauro al sistema de clasificación.
3.2.7	Conviene que el SGRE permita la existencia de un mecanismo de denominación de ficheros y una clase facultativa que incluya nombres (por ejemplo, de personas) y fechas (por ejemplo, de nacimiento) en la designación de ficheros. Esta característica abarca también la validación de los nombres de acuerdo con una lista. *Este requisito resulta pertinente en entornos dedicados al procesamiento de transacciones.*
3.2.8	Además del resto de los requisitos detallados en la presente sección, conviene que el SGRE admita la asignación de términos incluidos en un vocabulario controlado que satisfagan la norma ISO 2788 o la ISO 5964 como clase descriptiva o como términos referentes a los temas en los metadatos de los ficheros.
3.2.9	El SGRE no debe imponer límite práctico alguno al número de clases o ficheros que se pueden definir.
3.2.10	El SGRE debe permitir la creación y el mantenimiento automático de una lista o repertorio de ficheros.

3.3 Volúmenes

Esta sección se ocupa de los requisitos aplicables a la utilización de volúmenes, usados en general para subdividir ficheros que de otro modo podrían adquirir un tamaño desmedido y resultarían difíciles de manejar.

Ref.	Requisito
3.3.1	El SGRE debe permitir que los administradores añadan (es decir, que abran) volúmenes electrónicos a cualquier fichero electrónico que no se haya cerrado.
3.3.2	El SGRE debe grabar la fecha de apertura de cada nuevo volumen e incluirla entre los metadatos de éste.
3.3.3	Siempre que se abra un nuevo volumen, el SGRE deberá incluir de forma automática entre sus metadatos los atributos comunes a los metadatos del fichero raíz, tales como su nombre y su código de clasificación.
3.3.4	El SGRE debe permitir la aplicación del concepto de volúmenes de ficheros abiertos y cerrados, conforme a las siguientes normas: • En un fichero sólo se puede abrir el volumen de creación más reciente. • El resto de los volúmenes de tal fichero han de estar cerrados (aunque pueden existir excepciones temporales, establecidas por el requisito 3.3.6). *Téngase en cuenta que se puede acceder a los registros de un volumen con independencia de si dicho volumen está abierto o cerrado.*
3.3.5	El SGRE debe impedir que el usuario añada registros electrónicos a un volumen cerrado (excepto en los casos que exige el requisito 3.3.6).
3.3.6	El SGRE debe permitir que el administrador reabra un volumen previamente cerrado de forma temporal y que, tras añadirle registros, lo cierre de nuevo. *Se ha previsto la utilización de esta característica con vistas a la rectificación de errores de los usuarios, por ejemplo, cuando un volumen se cierra por equivocación.*

3.4 Mantenimiento del sistema de clasificación

Ref.	Requisito
3.4.1	El SGRE debe permitir la reubicación de un fichero electrónico y sus volúmenes, o bien de una clase completa de la jerarquía, en un lugar distinto del sistema de clasificación. Asimismo, debe garantizar que todos los registros electrónicos ya colocados sigan vinculados a los ficheros y volúmenes reubicados. *La utilización de este instrumento se ha previsto sólo para casos excepcionales, como fusiones de organizaciones, otras reestructuraciones y corrección de errores de copia. Este requisito ha de entenderse conjuntamente con el 3.4.3, el 3.4.4 y el 3.4.5.*
3.4.2	El SGRE debe permitir que un registro electrónico se pueda volver a clasificar en otro volumen de fichero electrónico. *La utilización de este instrumento está prevista en casos excepcionales, como cuando es preciso corregir errores de copia. Este requisito ha de entenderse conjuntamente con el 3.4.3, el 3.4.4 y el 3.4.5.*

Ref.	Requisito
3.4.3	El SGRE debe reservar a los administradores la capacidad de trasladar las clases, los ficheros, los volúmenes y los registros del sistema de clasificación.
3.4.4	El SGRE debe dejar constancia clara del estado de cualquier clase, volumen o registro con anterioridad a su reclasificación, de modo que pueda conocerse fácilmente todo su historial. *Como mínimo, este dato se debe almacenar en la pista de auditoría. También puede resultar conveniente guardar este dato en algún otro lugar (por ejemplo, en los metadatos de los objetos que se trasladan).*
3.4.5	Conviene que el SGRE permita al administrador introducir las razones conducentes a la reclasificación de cualquier clase, fichero, volumen o registro.
3.4.6	El SGRE debe evitar en todo momento que se elimine un fichero electrónico o cualquier parte de su contenido, salvo en caso de: • destrucción conforme al calendario de conservación (véase el capítulo 5); • eliminación llevada a cabo por un administrador como parte de un procedimiento auditado (véase 9.3).
3.4.7	El SGRE debe permitir el cierre de un fichero electrónico conforme a un procedimiento específico reservado a los administradores.
3.4.8	Conviene que el SGRE pueda cerrar un volumen de un fichero electrónico de forma automática cuando se cumplan unos criterios determinados definidos en el momento de la configuración y que, cuando menos, incluyan: • los volúmenes delimitados por una fecha de corte anual, como el término del año natural, fiscal o cualquier otro ciclo anual definido; • el transcurso del tiempo desde una acción determinada, por ejemplo, desde la fecha más reciente en que se añadió un registro electrónico a ese volumen; • el número de registros electrónicos que contiene un volumen. *En determinadas circunstancias puede resultar conveniente aplicar otros criterios (por ejemplo, cuando el tamaño del volumen llega al límite de la capacidad de almacenamiento de un disco extraíble).*
3.4.9	El SGRE debe grabar la fecha de cierre de un volumen e incluirla entre los metadatos de dicho volumen.
3.4.10	El SGRE debe impedir que un volumen abierto de forma temporal (como sucede en cumplimiento del requisito 3.3.6) siga abierto después de que el administrador se desconecte del sistema.
3.4.11	Conviene que el SGRE permita a los usuarios crear referencias cruzadas (véanse también los tipos de vínculos) entre los ficheros relacionados entre sí.

Ref.	Requisito
3.4.12	El SGRE debe mantener en todo momento la integridad interna de las relaciones y del resto de los elementos, con independencia de: • las actividades de mantenimiento • otras acciones del usuario • el fallo de los componentes del sistema. *Dicho de otro modo, no se debe permitir que surja una situación en la que, debido a la acción de un usuario o a un fallo del software, se produzca una incoherencia en el SGRE o en su base de datos.*
3.4.13	Conviene que el SGRE permita crear entradas múltiples para un registro electrónico en varios ficheros electrónicos, sin duplicación física del registro electrónico. *En otras palabras, conviene que en la captura de más de un registro basado en el mismo documento se utilicen marcadores.*
3.4.14	Conviene que el SGRE aporte herramientas destinadas a la presentación al administrador de estadísticas sobre las características de la actividad en el sistema de clasificación, incluido el número de ficheros, registros o volúmenes electrónicos creados, cerrados o eliminados en un período determinado.

4 CONTROLES Y SEGURIDAD

En este capítulo se agrupan los requisitos de una amplia gama de controles relacionados con la seguridad de los registros.

Las organizaciones han de ser capaces de controlar a quién se permite el acceso a los registros y en qué circunstancias, pues éstos pueden contener información reservada de carácter personal, comercial u operativo. También puede ser conveniente restringir el acceso a los usuarios externos. Por ejemplo, en ciertos países donde la legislación sobre la libertad de información da acceso a ciertos registros públicos, los clientes pueden desear consultar los registros. En la sección 4.1 se enumeran los requisitos relativos a estos controles.

Asimismo, puede resultar conveniente almacenar en la pista de auditoría los accesos a los registros y cualquier otra actividad asociada a ellos, así como los documentos o la información relacionados, con objeto de garantizar su admisibilidad jurídica y facilitar la recuperación de los datos. En la sección 4.2 se detallan los requisitos del control de tal información.

La seguridad de los registros abarca también la capacidad de protegerlos ante cualquier fallo del sistema mediante la creación de copias de seguridad y la posibilidad de restaurar los registros a partir de éstas. En la sección 4.3 se enumeran tales requisitos.

Por diversas causas, puede resultar necesario trasladar los registros a varios sistemas y emplazamientos. En la sección 4.4 se presentan los requisitos del control de tales transferencias.

En la sección 4.5 se detallan los requisitos del control de la autenticidad de los registros.

Por último, en la sección 4.6 se presentan los requisitos de seguridad de los documentos con marcas de protección (que suelen utilizar ciertos departamentos gubernamentales y sus contratistas).

4.1 Acceso

Normalmente, las organizaciones necesitan controlar el acceso a sus registros. En general, deben limitar o permitir el acceso a determinados registros y ficheros en función del usuario o el grupo de usuarios. También pueden tomar en consideración el grado de autorización de los usuarios, cuando se trata de temas de seguridad nacional.

Sólo ciertos perfiles han de poder determinar los derechos de acceso. En la tabla de la sección 13.4 se deduce que de ello se encarga el administrador. No obstante, conviene recordar que esta función se limita a la aplicación, desde el punto de vista del sistema, de las decisiones que adoptan los directivos de jerarquía superior, que

suelen estar basadas en leyes y normativas en materia de información, seguridad de los datos, archivos e industria. Estos asuntos se abordan en la sección 11.5.

Ref.	Requisito
4.1.1	El SGRE debe permitir que el administrador restrinja el acceso a los registros, ficheros y metadatos a determinados usuarios o grupos de usuarios.
4.1.2	El SGRE debe permitir que el administrador asocie al perfil del usuario ciertos atributos que determinarán las características, los campos de metadatos, los registros y los ficheros a los que el usuario tendrá acceso. Los atributos del perfil servirán para: • vetar el acceso al SGRE cuando no se aplique un mecanismo de autenticación aceptado atribuido al perfil del usuario; • vetar el acceso del usuario a ciertos ficheros o registros; • restringir el acceso del usuario a ciertas clases del sistema de clasificación; • restringir el acceso del usuario según el grado de autorización de su perfil; • restringir el acceso del usuario a ciertas funciones, como la lectura, la actualización y la eliminación de determinados campos de metadatos; • vetar el acceso después de una fecha concreta; • asignar el usuario a uno o varios grupos de usuarios. *Un ejemplo de mecanismo de autenticación aceptado es la contraseña.*
4.1.3	El SGRE debe proporcionar las mismas funciones de control para los perfiles y para los usuarios. *Esta característica permite que los administradores gestionen y mantengan un conjunto limitado de perfiles de derechos de acceso, en lugar de ocuparse de un gran número de usuarios individuales. Entre estos perfiles podrían encontrarse el de gerente, el de encargado de la tramitación de reclamaciones, el de analista de seguridad o el de administrador de bases de datos.*
4.1.4	El SGRE debe ser capaz de establecer grupos de usuarios asociados a un conjunto de ficheros o registros. *Como ejemplos de estos grupos podemos citar el personal, el equipo de ventas, etc.*
4.1.5	El SGRE debe permitir la pertenencia de un usuario a más de un grupo.
4.1.6	El SGRE debe permitir que sólo los administradores establezcan perfiles de usuarios y asignen los usuarios a grupos. *Véase también la sección 13.4.*

Ref.	Requisito
4.1.7	Conviene que el SGRE permita a un usuario decidir qué otros usuarios o grupos pueden acceder a los registros de los que él es responsable. Sin embargo, la asignación de esta función correspondería al administrador, según las directrices de la organización.
4.1.8	El SGRE debe reservar a los administradores la capacidad de modificar los atributos de seguridad de los grupos o los usuarios (como los derechos de acceso, el nivel de seguridad y la asignación y gestión de contraseñas).
4.1.9	Si un usuario busca un registro, volumen o fichero o solicita acceder a él sin tener derecho a consultarlo, el SGRE debe darle una de las siguientes respuestas (que se seleccionarán cuando se configure el sistema): • Visualización del título y los metadatos. • Reconocimiento de la existencia del fichero o registro (esto es, visualización del número del fichero o del registro), pero sin revelar su título ni ningún otro metadato. • Ocultación de toda información sobre el registro y de cualquier otra indicación que pueda sugerir su existencia. *Estas opciones se presentan en orden creciente en cuanto al grado de seguridad que ofrecen. Téngase en cuenta que la tercera opción (la más rigurosa) supone la exclusión de tales registros de las listas de resultados de búsqueda del SGRE. Este grado de seguridad suele resultar apropiado cuando se trata de registros que tratan de asuntos como la seguridad nacional.*
4.1.10	Si un usuario lleva a cabo una búsqueda de texto íntegro, el SGRE jamás deberá incluir en los resultados registros a los que el usuario no tenga derecho a acceder. *Aunque puede parecer que la elección del primer tipo de requisito 4.1.9 contradice este requisito, este aparente conflicto es deliberado, pues si el requisito no existiese los usuarios podrían realizar búsquedas en el texto para investigar el contenido de documentos a los que no tendrían derecho a acceder. Por lo tanto, este requisito debe prevalecer sobre el 4.1.9.*
4.1.11	Cuando el SGRE permita que los usuarios intenten acceder a ficheros, volúmenes o registros sin la autorización debida, debe quedar constancia de tales intentos en la pista de auditoría. *Esta característica podría adaptarse de tal forma que sólo afectase a las categorías de administradores establecidas en función de la seguridad (tal como se han definido en el requisito 4.6).*
4.1.12	Si el SGRE mantiene un repertorio de ficheros (véase 3.2.10), deberá ser capaz de limitar el acceso de los usuarios a determinadas partes de éste que se especificarán en el momento de la configuración.

4.2 Pista de auditoría

La pista de auditoría es un registro de las acciones realizadas que conciernen al SGRE. Entre ellas se encuentran las realizadas por los usuarios o administradores y las iniciadas de forma automática por el SGRE como resultado de los parámetros del sistema. En la sección 13.1 del Glosario se puede consultar una definición formal de la pista de auditoría. Aunque no es indispensable, la pista de auditoría de los registros se puede considerar parte de sus metadatos, pues está formada por datos que describen ciertos aspectos del historial de los registros.

El SGRE debe poder ocuparse de la gestión y el control de los registros electrónicos conforme a las normas precisas para el cumplimiento de los requisitos de admisibilidad y seguridad jurídica, además de demostrar ese cumplimiento. En este sentido, la pista de auditoría es un elemento clave en el cumplimiento de tales exigencias, puesto que registra de forma exhaustiva todas las acciones que atañen a cualquier registro.

Cuando se controlan todas las acciones, el volumen de la pista de auditoría puede adquirir grandes proporciones. Por consiguiente, en ciertos sistemas la gerencia puede determinar que no es preciso registrar determinadas acciones, y en la mayoría de los casos la pista de auditoría en línea se traslada periódicamente a un lugar de almacenamiento fuera de línea y se puede borrar en cuanto se han tomado las medidas pertinentes en relación con los registros en cuestión. Todos estos temas pertenecen al ámbito de la política de gestión o bien a los requisitos jurídicos o normativos, por lo que esta especificación incluye los requisitos del sistema que permiten realizar tales acciones, pero no especifica en qué medida se recurre a ellos.

Ref.	**Requisito**
4.2.1	El SGRE debe mantener una pista de auditoría inalterable, capaz de capturar y almacenar de forma automática datos sobre: • todas las acciones relacionadas con los registros electrónicos, los ficheros electrónicos y el sistema de clasificación; • el usuario que inicia o realiza la acción; • la fecha y la hora de la acción. *La palabra «inalterable» significa que el usuario no puede borrar ni modificar en modo alguno la pista de auditoría. Sin embargo, de ser necesario, cabe la posibilidad de reorganizar o copiar esa información en un medio extraíble mediante, por ejemplo, software de bases de datos, siempre y cuando no se modifique su contenido.*
4.2.2	Una vez se ha activado la funcionalidad de la pista de auditoría, el SGRE debe ser capaz de rastrear sin intervención manual alguna todas las acciones y de almacenar en la pista de auditoría datos sobre ellas.

Ref.	Requisito
4.2.3	El SGRE debe mantener la pista de auditoría durante el tiempo necesario, que al menos abarcará el ciclo de vida de los registros o ficheros electrónicos a los que hace referencia.
4.2.4	El SGRE debe permitir consignar en la pista de auditoría todas las modificaciones que afecten a: • grupos de ficheros electrónicos • ficheros electrónicos individuales • volúmenes electrónicos • registros electrónicos • documentos electrónicos • metadatos relativos a cualquiera de los elementos anteriores.
4.2.5	El SGRE debe permitir consignar en la pista de auditoría todas las modificaciones realizadas en los parámetros administrativos. *Ejemplo: Si el administrador modifica los derechos de acceso de un usuario.*
4.2.6	El SGRE debe ser capaz de capturar y almacenar en la pista de auditoría datos sobre las siguientes acciones: • la fecha y la hora de la captura de todos los registros electrónicos; • la reclasificación de un registro electrónico en otro volumen (véase 3.4.2); • la reclasificación de un fichero electrónico dentro del sistema de clasificación (véase 3.4.1); • cualquier modificación del calendario de conservación de un fichero electrónico; • cualquier modificación realizada en los metadatos asociados a las clases, los ficheros o registros electrónicos; • la fecha y la hora de creación, modificación y eliminación de los metadatos; • los cambios realizados en los privilegios de acceso relativos a un fichero o registro electrónico o bien a un usuario; • las acciones de exportación o transferencia de un fichero electrónico; • la fecha y la hora de visualización (véase sección 13.1 del Glosario); • la eliminación o destrucción de ficheros o registros electrónicos.
4.2.7	Conviene que el SGRE permita al administrador configurar el instrumento de la pista de auditoría de forma que pueda seleccionar las acciones que se consignarán de forma automática. Asimismo, el SGRE debe garantizar el almacenamiento de esta selección y las modificaciones que en ella se realicen en la pista de auditoría.

Ref.	Requisito
4.2.8	El SGRE debe permitir el examen, previa solicitud, de la pista de auditoría, de modo que sea posible identificar una acción concreta y acceder a todos los datos relacionados con ella. Este procedimiento ha de poder ser utilizado por personal externo autorizado poco familiarizado con el sistema o que lo desconozca completamente.
4.2.9	El SGRE debe ser capaz de exportar la pista de auditoría de determinados registros y ficheros electrónicos y también de grupos de ficheros, sin que ello repercuta en la almacenada por el sistema. *Esta función puede ser utilizada por auditores externos que deseen examinar o analizar la actividad del sistema.*
4.2.10	El SGRE debe poder capturar y guardar un registro de violaciones, esto es, de los intentos de un usuario de acceder a un registro, volumen o fichero sin autorización, y (cuando sea factible) de los intentos de violación de los mecanismos de control de acceso. *Para ejemplos de circunstancias en las que se pueden permitir intentos de violación del sistema, consúltese 4.1.9.*
4.2.11	Como mínimo, el SGRE debe ser capaz de proporcionar informes sobre las acciones que hacen referencia a clases, ficheros y registros organizados por: • registros, ficheros o clases • usuarios • secuencias cronológicas.
4.2.12	Conviene que el SGRE sea capaz de generar informes sobre las acciones relacionadas con ficheros y registros organizados por grupos de trabajo y (cuando proceda por motivos técnicos) según la dirección de la red.

4.3 Copias de seguridad y recuperación

Tanto la normativa vigente como las propias empresas exigen que los SGRE cuenten con procedimientos exhaustivos de creación periódica de copias de seguridad de los registros y metadatos, de forma que sea posible recuperar rápidamente cualquier registro perdido debido a un fallo del sistema, un accidente, un fallo en la seguridad, etc.

Las tareas de creación y restauración automática de copias periódicas de seguridad pueden corresponder al SGRE o bien ser una función integrada en los servicios y procedimientos de un sistema de gestión electrónica de documentos (EDMS) o de un sistema de gestión de bases de datos que funcione conjuntamente con el de registros electrónicos.

En la práctica, las funciones de copia de seguridad y restauración se pueden repartir entre los administradores del SGRE y el personal del departamento de operaciones de TI.

Ref.	Requisito
4.3.1	El SGRE debe estar dotado de procedimientos automáticos de copia de seguridad y restauración que permitan realizar copias periódicas de seguridad de todas las clases, los ficheros, los registros, los metadatos y los atributos administrativos del depósito del SGRE o de algunos de ellos.
4.3.2	El SGRE debe permitir al administrador programar rutinas de copias de seguridad en las que pueda: • especificar la frecuencia de la copia de seguridad; • escoger las clases, ficheros o registros de los que se hará una copia de seguridad; • seleccionar un medio de almacenamiento, un sistema o un emplazamiento para la copia de seguridad (por ejemplo, un almacenamiento fuera de línea, en otro sistema o en un emplazamiento remoto).
4.3.3	El SGRE debe restringir al administrador la restauración de sus copias de seguridad. La integridad de los datos no se debe ver afectada en modo alguno por esa restauración.
4.3.4	El SGRE debe restringir al administrador la actualización de las copias de seguridad, manteniendo la plena integridad de los datos.
4.3.5	Conviene que el SGRE sea capaz de notificar a los usuarios la posibilidad de que se haya realizado una recuperación incompleta. La notificación tendría lugar la siguiente vez que el usuario se conectara al sistema.
4.3.6	El SGRE debe permitir que los usuarios especifiquen los registros que se considerarán «vitales». *Los registros vitales son los absolutamente necesarios para la continuidad de la actividad de la organización, ya sea en cuanto a su capacidad de hacer frente a situaciones de emergencia o a catástrofes, ya en relación con la protección de sus intereses financieros y jurídicos. Por consiguiente, la identificación y la protección de tales registros es de gran importancia en cualquier organización.*
4.3.7	El SGRE debe permitir la restauración de los registros vitales y los demás en operaciones separadas.

4.4 Control del traslado de registros

A lo largo de su ciclo de vida, los ficheros y sus metadatos se pueden transferir de un medio o lugar de almacenamiento a otro, a medida que su actividad disminuye o se modifica su uso. Este traslado puede ser local, ya sea casi en línea (*near line*) (por ejemplo, a un medio extraíble en un aparato automático, como CD grabables

en un reproductor de CD), fuera de línea (local o remoto) o a otro depósito de registros (como un archivo nacional o público). Es preciso que exista un instrumento de control que permita registrar el cambio de emplazamiento, tanto por razones normativas como para facilitar el acceso a los datos.

Ref.	Requisito
4.4.1	El SGRE debe contar con un instrumento de seguimiento que permita controlar y registrar información sobre el emplazamiento y la transferencia de los ficheros, tanto físicos como electrónicos.
4.4.2	La función de seguimiento debe registrar información sobre las transferencias que incluirá: • un identificador único de los ficheros o registros; • el emplazamiento actual y el número de emplazamientos anteriores que fije el usuario (convendría que el usuario definiese los emplazamientos); • la fecha en que el fichero se retiró o trasladó de su emplazamiento; • la fecha de recepción del fichero en su emplazamiento (cuando se trate de transferencias); • el usuario responsable del traslado (cuando proceda).
4.4.3	El SGRE debe conservar el acceso al contenido del registro electrónico, incluida la capacidad de reproducirlo y de realizar el mantenimiento de su estructura y su formato, a lo largo del tiempo e independientemente de la utilización de nuevas versiones de aplicaciones de software ofimático. *Este último requisito se puede satisfacer, aunque no es obligatorio que así se haga, con el uso de una aplicación que permita visualizar múltiples formatos. En la sección 11.7 se ofrece más información sobre cuestiones relacionadas con la visualización a largo plazo.*

4.5 Autenticidad

Los registros que se deben capturar y el momento en que se realizará la captura son cuestiones que se determinarán en función de la política de la empresa y de los requisitos de mantenimiento de los registros de los procesos empresariales. Una vez capturado el registro, es esencial que no se modifiquen los componentes, la estructura ni los metadatos necesarios para verificar su autenticidad. Los registros capturados se deben conservar de un modo que no admita revisiones, de forma que queden protegidos, durante toda su vida, contra cambios deliberados o accidentales de contenido, contexto, estructura y apariencia, y puedan así conservar su autenticidad.

Ref.	Requisito
4.5.1	El SGRE debe restringir el acceso a las funciones del sistema según el perfil del usuario y aplicando controles estrictos de la administración del sistema. *Esta característica es necesaria para proteger la autenticidad de los registros electrónicos.*
4.5.2	En caso de que sea posible y proceda, conviene que el SGRE muestre una advertencia cada vez que se intenta capturar un registro incompleto o incoherente de algún modo que pueda repercutir, en apariencia, en su futura autenticidad. *Ejemplo: Una orden de compra sin una firma electrónica válida o una factura de un proveedor no reconocido.*
4.5.3	En caso de que sea posible y proceda, conviene que el SGRE muestre una advertencia cada vez que se intenta capturar un registro cuya futura verificación de autenticidad no resulte factible.
4.5.4	El SGRE debe evitar que los usuarios o los administradores modifiquen el contenido de los registros electrónicos, excepto cuando los cambios formen parte del proceso empresarial o documental, tal y como se comenta más adelante en la presente especificación.

4.6 Categorías de seguridad

La sección 4.1 describe los requisitos del control del acceso de los usuarios y grupos de usuarios. En ciertos entornos, y principalmente cuando está en juego la seguridad nacional, es preciso restringir más el acceso mediante un sistema de categorías y habilitaciones de seguridad. Tales habilitaciones prevalecen sobre cualquier derecho de acceso que se pueda conceder en virtud de las características definidas en la sección 4.1. Los requisitos de esta sección sólo son aplicables a los entornos en los que existe tal necesidad.

Dicha necesidad se satisface asignando a las clases, ficheros o registros una o más «categorías de seguridad», expresión que se utilizará en esta especificación para designar «uno o varios términos asociados a un registro y que definen las normas que rigen el acceso a éste». El término no es de uso corriente y se ha acuñado expresamente para la presente especificación.

A continuación, a cada usuario se le pueden asignar una o más habilitaciones de seguridad que evitarán su acceso a todas las clases, ficheros o registros de categorías de seguridad superiores.

Las categorías de seguridad se pueden dividir en subcategorías. Algunas subcategorías son de naturaleza jerárquica, mientras que otras se pueden organizar conforme a criterios diferentes, por lo general específicos a una organización o sector. En esta especificación sólo se describen con detalle los requisitos de una subcategoría jerárquica.

Ref. **Requisito**

4.6.1 El SGRE debe permitir la asignación de categorías de seguridad a los registros.

4.6.2 El SGRE debe permitir que en el momento de la configuración se escoja una de las siguientes opciones:

- la asignación de categorías de seguridad a clases, ficheros o volúmenes;
- la existencia de clases, ficheros o volúmenes electrónicos que no tengan asignada ninguna categoría de seguridad.

Esta es una característica conveniente, pues ciertas organizaciones prefieren asignar categorías de seguridad a los ficheros electrónicos, tal y como harían con ficheros físicos o en papel, mientras que otras optan por proteger solamente los registros que se encuadran en tales ficheros.

4.6.3 Conviene que el subsistema de seguridad del SGRE se pueda utilizar de forma eficaz en conjunción con otros productos de seguridad general.

4.6.4 El SGRE debe permitir, aunque no exigir necesariamente, que las categorías de seguridad se subdividan en una o varias «subcategorías».

Así, una categoría de seguridad se podría desglosar en tres categorías, como se indica en el siguiente ejemplo ficticio:

Subcategoría	***Valores permitidos***
Clase	*Máximo secreto* *Secreto* *Confidencial* *Restringido* *Sin clasificar*
Advertencia	*Reservado personal OTAN* *Reservado personal UEO*
Descriptor	*Comercial* *Personal* *Gestión* *Auditoría y contabilidad*

En este ejemplo imaginario, la subcategoría «clase» es de naturaleza jerárquica (véase 4.6.6), al contrario que el resto de las subcategorías. Los requisitos de las subcategorías jerárquicas son comunes y se detallan más adelante. Sin embargo, los requisitos de las subcategorías de naturaleza jerárquica pueden ser complejos y, a excepción del 4.6.5, no se estudian en el presente documento.

Ref.	Requisito
4.6.5	Conviene que el SGRE permita la aplicación específica de normas de seguridad únicas o complejas. *Tal requisito se puede satisfacer con las interfaces de programas de aplicación adecuadas, lo que resulta necesario cuando hay que gestionar registros aplicando convenciones de marcaje no tratadas en este documento, como la de IDO (International Defence Organisation), o bien cuando se trata de restringir el acceso a las historias clínicas.*
4.6.6	El SGRE debe soportar, al menos en una subcategoría, una jerarquía de un mínimo de cinco niveles, desde un acceso sin restricciones en el nivel inferior a un acceso extremadamente restringido en el nivel superior. *Ejemplo: La subcategoría «clase» del requisito 4.6.4.*
4.6.7	El SGRE debe permitir la asignación a los usuarios de habilitaciones de seguridad acordes a la subcategoría. *Siguiendo con el ejemplo de 4.6.4, se asignaría a los usuarios una de las siguientes habilitaciones:* *Máximo secreto* *Secreto* *Confidencial* *Restringido* *Sin clasificar*
4.6.8	El SGRE debe vetar el acceso de los usuarios a los registros electrónicos (y a las clases y ficheros electrónicos, en función de la selección realizada en el requisito 4.6.2) pertenecientes a una categoría de seguridad más restringida que la de su propia habilitación. *Obsérvese que el nivel correcto de habilitación de seguridad puede ser insuficiente para obtener acceso, y que éste se puede restringir aún más en aplicación de las características descritas en la sección 4.1 y limitarse a ciertos usuarios, perfiles o grupos.*
4.6.9	El SGRE debe soportar la aplicación automática del valor por defecto del nivel más bajo de seguridad a la subcategoría de una clase, fichero o registro electrónico no asignado a ninguna otra categoría de seguridad. *Volviendo al ejemplo del requisito 4.6.4, el valor por defecto sería «Sin clasificar».*
4.6.10	Convendría que el SGRE fuera capaz de evitar la asignación de un fichero electrónico a una clasificación de categoría de seguridad inferior a la de cualquier registro electrónico de dicho fichero (en función de la opción escogida en relación con el requisito 4.6.2).

Ref.	Requisito
4.6.11	Conviene que el administrador pueda averiguar, con una simple consulta, cuál es la categoría de seguridad más alta de un registro cualquiera perteneciente a cualquier clase o fichero. *En ciertos entornos, ésta será una característica esencial que mejorará la facilidad de uso del sistema.*
4.6.12	Conviene que el SGRE admita la revisión programada y rutinaria de las categorías de seguridad.

5 CONSERVACIÓN Y ELIMINACIÓN

Un aspecto fundamental de la gestión de registros viene dado por el uso de calendarios de conservación que rigen la eliminación de los registros de los sistemas en funcionamiento. Los calendarios de conservación determinan el tiempo que el SGRE debe conservar los registros y cómo se deben eliminar. En la sección 5.1 se establecen los requisitos relativos a los calendarios de conservación

En las secciones posteriores se detallan los procesos que pueden tener lugar en la fecha especificada en los calendarios de conservación; en la sección 5.2 se enumeran los requisitos de los procesos de revisión y en la 5.3 se presentan los requisitos de transferencia, exportación y destrucción

Terminología

Tal y como se explicaba en la sección 2.2 bajo el epígrafe «Ficheros y volúmenes electrónicos», unas veces los registros se gestionan en ficheros y otras en volúmenes de ficheros. Esta posibilidad se plantea en todas las etapas de los procesos descritos en este capítulo. Por consiguiente, en aras de una mayor simplicidad, en este capítulo la palabra «fichero» designará «un fichero o un volumen, según proceda».

5.1 Calendarios de conservación

Ref.	Requisito
5.1.1	El SGRE debe incluir una función que especifique los calendarios de conservación, que automatice las acciones de informe y destrucción de datos y que cuente con instrumentos integrados para exportar registros y metadatos.
5.1.2	El SGRE debe ser capaz de reservar al administrador el proceso de creación y modificación de los calendarios de conservación.
5.1.3	El SGRE debe permitir que el administrador defina y guarde un conjunto normalizado de calendarios de conservación personalizados.
5.1.4	El SGRE debe ser capaz de asociar un calendario de conservación a cualquier registro, fichero o clase de un sistema de clasificación. *El calendario de conservación se puede seleccionar entre el conjunto normalizado o bien introducirse de forma manual cuando se abra el fichero.*

Ref.	Requisito
5.1.5	Conviene que el SGRE sea capaz de asociar más de un calendario de conservación a cualquier fichero o clase de un sistema de clasificación. *Ejemplos:* • *Un fichero puede tener asociado un calendario normalizado de la organización al que pertenece y un calendario especial relacionado con el litigio al que hace referencia el fichero.* • *Una clase puede tener asociado un calendario de conservación en virtud de una norma legislativa y contener una subclase que tenga asignado un segundo calendario con normas distintas en materia de conservación de historias clínicas.*
5.1.6	Todo registro de un fichero o clase debe, por defecto, estar sujeto al calendario o a los calendarios de conservación asociados a dicho fichero o clase.
5.1.7	Todo calendario de conservación debe incluir una decisión sobre su disposición (5.1.10), el período de conservación (5.1.11), el motivo y el origen de la decisión.
5.1.8	En relación con cada fichero, el SGRE debe: • rastrear de forma automática los períodos de conservación asignados al fichero o a la clase a la que pertenece; • iniciar el proceso de eliminación una vez se haya llegado al término del período de conservación.
5.1.9	Cuando un fichero o una clase tengan asociado más de un calendario de conservación, el SGRE deberá rastrear de forma automática todos los períodos de conservación especificados en tales calendarios, así como iniciar el proceso de eliminación una vez se haya superado la última de todas las fechas de conservación.
5.1.10	El SGRE debe permitir la adopción de, cuando menos, las siguientes decisiones en relación con cada calendario de conservación: • La conservación de forma indefinida. • La presentación para su revisión en una fecha futura, que se definirá como se indica en 5.1.11. • La eliminación en una fecha futura, que se definirá como se indica en 5.1.11. • La transferencia en una fecha futura, que se definirá como se indica en 5.1.11.

Ref.	Requisito
5.1.11	Cada calendario de conservación debe permitir que se fijen unos períodos de conservación (tal y como se han definido en 5.1.10) en relación con una fecha futura, que se determinará al menos en función de: • El transcurso de un tiempo determinado tras la apertura del fichero. • El transcurso de un tiempo determinado tras el cierre del fichero. • El transcurso de un tiempo determinado desde la última adición de un registro al fichero. • El transcurso de un tiempo determinado desde la recuperación de un registro del fichero. • El transcurso de un tiempo determinado tras una acción concreta (que se describirá en el calendario y que el administrador comunicará al SGRE, en vez de ser detectada de forma automática por el sistema; por ejemplo, «después de la firma del contrato»). • Un tiempo especificado como «indefinido» que indicará la conservación a largo plazo de los registros. *Si bien los puntos anteriores cubren casi todo el espectro de posibilidades, ciertos tipos de registros podrían presentar tipos de requisitos de conservación que no se recogen en el presente documento.*
5.1.12	El SGRE debe permitir la existencia de períodos de conservación que vayan de un mes a cien años, en cumplimiento del requisito 5.1.11. *Tales períodos máximos y mínimos se proponen como lapsos de tiempo arbitrarios que intentan evitar cualquier limitación práctica. Aunque parece improbable que un SGRE se prolongue durante cien años, un requisito de esta clase permitirá que los registros se exporten a futuros sistemas sin necesidad de revisar sus calendarios de conservación.*
5.1.13	El SGRE debe tomar nota e informar al administrador de forma automática de todas las acciones relacionadas con la eliminación.
5.1.14	El SGRE debe permitir que el calendario de conservación asignado a un fichero prevalezca sobre el asociado a una clase a la pertenezca el fichero.
5.1.15	El SGRE debe permitir que el administrador modifique cualquier calendario de conservación asociado a cualquier fichero en cualquier momento de la vida de éste.
5.1.16	El SGRE debe permitir que el administrador modifique los calendarios asociados a un fichero en cualquier momento de la vida de éste.

Ref.	Requisito
5.1.17	Conviene que el SGRE admita la definición de conjuntos de normas de procedimiento que se puedan aplicar a determinados ficheros y clases como instrumento de alarma antes de que dé comienzo el proceso de eliminación. Por ejemplo: • La revisión del fichero y de su contenido por un gestor determinado o bien por el administrador. • La notificación al administrador de que un fichero presenta un nivel de seguridad determinado.
5.1.18	Convendría que el SGRE permitiese de forma opcional que, cuando un administrador desplace registros o ficheros electrónicos entre clases del sistema de clasificación, el calendario de la clase destino pueda sustituir a los calendarios de conservación antes aplicados a tales registros.

5.2 Revisión

La revisión es el proceso de comprobación de los ficheros que tiene lugar una vez alcanzada la fecha o la acción especificada en el calendario de conservación, con el propósito de decidir si la información debe conservarse, trasladarse a otro sistema o destruirse. El revisor puede examinar los metadatos, el contenido o ambos. En ciertos entornos, los calendarios de conservación se utilizan para dirigir la eliminación de registros sin una revisión previa.

La eliminación de ciertos registros está sujeta a leyes y reglamentos. La revisión se ha de llevar a cabo de conformidad con tales normas y leyes y, cuando proceda, en colaboración con las autoridades de archivo responsables. Un debate más profundo de estas cuestiones superaría el ámbito de la presente especificación.

Ref.	Requisito
5.2.1	Conviene que el SGRE sea capaz de notificar periódicamente al administrador todos los calendarios de conservación que se aplicarán en un periodo determinado, y de proporcionar informes cuantitativos sobre los volúmenes y tipos de registros.
5.2.2	Conviene que el administrador sea capaz de especificar la frecuencia con que se realizará el informe sobre el calendario de retención y la información que contendrá, así como las excepciones notables, como las demoras en las eliminaciones.

Ref.	Requisito
5.2.3	El SGRE debe facilitar el proceso de revisión por medio de la presentación de los ficheros electrónicos que serán objeto de examen, con sus metadatos y la información relativa a su calendario de conservación (la razón), de tal modo que el revisor pueda explorar a conciencia (navegando y estudiando) el contenido del fichero y sus metadatos. *En la práctica, esto supone la existencia de funciones que permitan la navegación hacia adelante, hacia atrás, etc., tanto dentro de los ficheros como entre ellos, y desde y hacia los metadatos de los ficheros y registros.*
5.2.4	Conviene que el SGRE avise al administrador cuando en un fichero aparezca un vínculo con otro fichero que esté previsto destruir. Además, el sistema deberá paralizar el proceso de destrucción y permitir la adopción de la medida siguiente: • La confirmación del administrador de la continuación o la cancelación del proceso. • La generación de un informe en el que se detallen los ficheros o registros afectados, así como todas las referencias o vínculos de los que sean destino.
5.2.5	El SGRE debe permitir que, durante la revisión, el revisor tome al menos una de las siguientes decisiones en relación con cada fichero: • marcar el fichero para su eliminación; • marcar el fichero para su transferencia (véase 5.3.7); • modificar el calendario de conservación o asignar uno distinto, de forma que el fichero se conserve y se revise de nuevo en una fecha posterior que se definirá conforme a 5.1.11.
5.2.6	El SGRE debe permitir que el revisor introduzca en los metadatos del fichero comentarios sobre las razones de las decisiones derivadas de la revisión.
5.2.7	El SGRE debe comunicar al administrador qué ficheros está previsto eliminar antes de llevar a cabo una acción en este sentido. Una vez que el administrador haya confirmado el procedimiento, el sistema deberá ser capaz de iniciar las acciones de eliminación especificadas en 5.1.10.

Ref.	Requisito
5.2.8	Conviene que el SGRE admita herramientas de informe y análisis que el administrador pueda utilizar en la gestión de la conservación y de los calendarios de conservación. Entre las funciones de dichas herramientas estará la capacidad de: • presentar un listado de todos los calendarios de conservación; • presentar un listado de todos los ficheros electrónicos a los que se haya asignado un calendario de conservación determinado; • presentar un listado de los calendarios de conservación asociados a todos los ficheros que queden por debajo de un punto determinado en la jerarquía del sistema de clasificación; • identificar, comparar y revisar los calendarios de conservación (incluido su contenido) de todo el sistema de clasificación; • determinar las contradicciones formales existentes en los calendarios de conservación de todo el sistema de clasificación.
5.2.9	El SGRE debe almacenar en la pista de auditoría todas las decisiones adoptadas por el revisor en el desempeño de sus tareas.
5.2.10	Conviene que el SGRE admita o aporte la capacidad necesaria para interactuar con un instrumento de flujo de tareas que permita el proceso de programación, revisión y exportación o transferencia, rastreando: • el progreso o estado de la revisión, que podría estar pendiente o en curso, e información sobre el revisor y la fecha; • los registros pendientes de eliminación como resultado de una decisión derivada de la revisión; • el progreso del proceso de transferencia.
5.2.11	Conviene que el SGRE sea capaz de acumular estadísticas sobre las decisiones de revisión adoptadas en un período determinado y de presentar informes tabulares y gráficos sobre la actividad.

5.3 Transferencia, exportación y destrucción

Las organizaciones pueden verse obligadas a trasladar los registros desde sus SGRE a otros emplazamientos o sistemas. En el presente documento, tal proceso se denomina «transferencia». Téngase en cuenta que el término transferencia se utiliza incluso cuando únicamente se envíe una copia a otro sistema o emplazamiento. Entre las razones de la transferencia están:

- La conservación con carácter permanente de los documentos por motivos jurídicos, administrativos o de investigación.

- La utilización de servicios externos en la gestión a corto o medio plazo de los registros.

A menudo, esta acción da lugar a la transferencia de los registros al entorno de un SGRE distinto. Nótese que, tras la transferencia, en algunos casos se borrarán los registros que en principio se guardaban en el SGRE, mientras que en otros casos se optará por conservarlos.

En otras circunstancias, la organización tendrá que exportar los registros, esto es, trasladar una copia a otro emplazamiento o sistema y conservar los registros. Y también puede darse el caso de que sea preciso destruir los registros.

Sea como sea, el requisito consiste en la ejecución de la transferencia, exportación o destrucción de una manera controlada. Al mismo tiempo que se adoptan disposiciones sobre los registros, se deberán tener siempre en cuenta los metadatos y las pistas de auditoría asociados a ellos.

Obsérvese que en este contexto «destrucción» no es sinónimo de «borrado». El borrado de registros en otras circunstancias se trata en la sección 9.3.

Ref.	**Requisito**
5.3.1	El SGRE debe incluir un proceso bien gestionado de transferencia de registros a otro sistema o a una organización externa.
5.3.2	Siempre que el SGRE transfiera una clase, un fichero o un volumen, la transferencia deberá incluir: • en relación con las clases: todos los ficheros de la clase; • en relación con los ficheros: todos los volúmenes que, en la jerarquía, queden por debajo del fichero; • todos los registros de tales ficheros y volúmenes; • todos los metadatos asociados a tales ficheros, registros y volúmenes.
5.3.3	El SGRE debe ser capaz de transferir o exportar un fichero o una clase en una sola secuencia de operaciones, de modo que: • no se degrade el contenido ni la estructura de sus registros electrónicos; • todos los componentes de un registro electrónico (cuando posea más de uno) se exporten como si se tratase de una sola unidad; por ejemplo, un mensaje de correo electrónico se exportará con sus ficheros adjuntos; • se conserven todos los vínculos entre el registro y sus metadatos; • se conserven todos los vínculos entre los registros, volúmenes y ficheros electrónicos.
5.3.4	En la transferencia o exportación de registros electrónicos, el sistema debe ser capaz de incluir una copia de los datos de la pista de auditoría asociada a los registros, volúmenes y ficheros objeto de la transferencia.

Ref.	Requisito
5.3.5	Conviene que el SGRE incluya una herramienta o un instrumento de conversión que permita reproducir los registros marcados para la transferencia o exportación en uno o varios formatos de transferencia aprobados. *Ejemplos: El formato PDF o equivalente y el lenguaje de marcado extensible (XML).*
5.3.6	El SGRE debe presentar un informe en el que se detalle cualquier fallo que se haya producido durante la transferencia, la exportación o el borrado. El informe deberá indicar cuáles de los registros que estaba previsto transferir han generado errores durante la operación, así como especificar qué ficheros o registros no se han transferido, exportado o borrado satisfactoriamente.
5.3.7	El SGRE debe conservar todos los ficheros electrónicos que se hayan transferido, al menos hasta que se reciba la confirmación de que el proceso de transferencia ha concluido satisfactoriamente. *Esta característica se propone como procedimiento de salvaguardia para garantizar que los registros no se borren antes de que el receptor comunique que la transferencia ha concluido satisfactoriamente.*
5.3.8	Conviene que el SGRE sea capaz de exportar toda una clase del sistema de clasificación en una sola secuencia de operaciones, sin que se alteren: • el emplazamiento relativo de cada fichero en el sistema de clasificación, de modo que sea posible reconstruir la estructura del fichero; • todos los metadatos de los niveles más altos de la jerarquía, que se trasladarán junto con la clase.
5.3.9	Cuando se transfieran, exporten o destruyan ficheros híbridos, convendría que antes de proceder a la transferencia, la exportación o la destrucción de las versiones electrónicas el SGRE pidiese al administrador confirmación de que la versión en papel de esos ficheros se ha transferido, exportado o destruido.
5.3.10	Con el propósito de facilitar la gestión de archivos, conviene que el SGRE permita añadir elementos de metadatos definidos por el usuario a ficheros electrónicos seleccionados para ser transferidos.
5.3.11	Conviene que el SGRE permita clasificar los ficheros electrónicos seleccionados para ser transferidos en listas organizadas de acuerdo con los elementos de los metadatos seleccionados por el usuario.
5.3.12	Conviene que el SGRE sea capaz de generar formularios definidos por el usuario en los que se describan los ficheros electrónicos que se vayan a exportar o transferir.

Ref.	Requisito
5.3.13	Conviene que el SGRE permita la destrucción total de clases y de ficheros concretos almacenados en soportes regrabables, de forma que queden eliminados por completo y no se puedan restaurar con instrumentos especializados de recuperación de datos. *En ciertos entornos puede resultar necesario realizar reiteradas operaciones de reescritura de datos, de conformidad con las normas establecidas.* *Cuando se exija una garantía de la destrucción, puede resultar conveniente considerar la posibilidad de conservar copias de seguridad en un soporte adecuado a tal fin. No obstante, esta cuestión escapa al alcance de la presente especificación.*
5.3.14	Si los registros se almacenan en soportes no regrabables, el SGRE debe incluir instrumentos que faciliten el acceso a ellos de modo que no se puedan restaurar con un uso normal del SGRE o de las utilidades normalizadas del sistema operativo. *Por lo general, ello supone la destrucción del índice de datos (que se conserva en los soportes regrabables), en el que registra el emplazamiento de los datos en los soportes no regrabables.* *Cuando se exija una garantía de la destrucción, puede resultar conveniente considerar la posibilidad de conservar copias en un soporte adecuado a tal fin. No obstante, esta cuestión escapa al alcance de la presente especificación.*
5.3.15	El SGRE debe ser capaz de conservar los metadatos de los ficheros y registros transferidos o destruidos. *En ciertos entornos, puede resultar conveniente conservar información detallada sobre los registros destruidos. El sistema también puede permitir la simple identificación de los registros destruidos o transferidos, lo que está muy relacionado con 5.3.16.*
5.3.16	El SGRE debe permitir que el administrador seleccione, para conservarlo, un subconjunto de metadatos de los ficheros que se destruyan, se transfieran o se desplacen fuera de línea. *Esta es una característica aconsejable, pues permite a la organización saber de qué registros ha dispuesto en el pasado y en qué fechas se han destruido o se les ha dado salida, sin tener que conservar el conjunto completo de los metadatos del fichero.*
5.3.17	El SGRE debe permitir la exportación o transferencia de los registros en repetidas ocasiones.

6 CAPTURA DE REGISTROS

Terminología

El término «capturar» se utiliza para designar el proceso de grabación de un registro, la decisión sobre la clase en la que se incluirá, la adición de metadatos complementarios y su almacenamiento en el SGRE.

En el contexto de un SGRE, la grabación y el resto de los procesos que la acompañan pueden ser independientes o indistinguibles unos de otros.

En el Glosario (sección 13.1) se pueden consultar las definiciones formales.

Resumen

Este capítulo trata de los requisitos de la introducción de registros en un SGRE. Su primera sección (6.1) aborda el proceso de captura; la siguiente (6.2) cubre la importación de grandes volúmenes de registros de otros sistemas; la sección (6.3) presenta ciertas consideraciones relacionadas con determinados tipos de documentos, y por último, la sección 6.4 se dedica al correo electrónico, vista su importancia creciente.

6.1 Captura

En esta sección se presentan los requisitos del proceso de captura.

Los documentos electrónicos generados o recibidos en el curso de los procesos empresariales proceden de fuentes internas y externas. Los documentos electrónicos pueden presentar distintos formatos y su autoría puede ser muy diversa. Además, se pueden recibir como ficheros de documentos únicos o compuestos por varios documentos. Por otro lado, pueden llegar a través de distintos canales de comunicación, como redes de área local, redes de área extensa, correo electrónico, fax y correo postal (que se escaneará) y presentar frecuencias y volúmenes de llegada variables. Para respetar toda esa diversidad de requisitos, es preciso un sistema flexible de entrada que capture los documentos con un buen control de la gestión.

Ref.	Requisito
6.1.1	El proceso de captura de registros del SGRE debe contar con los controles y la funcionalidad adecuada para: • grabar y gestionar todos los registros electrónicos, con independencia del método de codificación empleado y de otras características tecnológicas; • garantizar que los registros se asocian a un sistema de clasificación y a uno o más ficheros; • integrarse con el software de aplicaciones que genera los registros; • validar y controlar la entrada de metadatos al SGRE.
6.1.2	El sistema debe ser capaz de incorporar al entorno de gestión de registros electrónicos: • el contenido del registro electrónico, incluida la información que determina su forma y visualización y la que define la estructura y el comportamiento del registro electrónico, sin menoscabo de su integridad estructural (por ejemplo, se deberán conservar todos los elementos de un mensaje de correo electrónico con sus ficheros adjuntos, o todos los componentes de una página web, con sus vínculos respectivos); • información sobre el documento electrónico (por ejemplo, el nombre del fichero); • la fecha de creación y otros metadatos del documento relativos a los elementos del registro; • información sobre el contexto en que se originó, creó y declaró el registro electrónico (por ejemplo, el proceso empresarial, su origen y su autor); • información sobre el programa de aplicaciones que generó el registro, incluida su versión. *En ocasiones, la información sobre la reproducción se desprende del tipo de extensión del fichero informático (por ejemplo, «doc» o «pdf»). La mayor parte de las veces puede bastar con ello, pero no cuando es necesaria una conservación o largo plazo o una precisión superior (como la precisión del espacio cromático).*
6.1.3	El SGRE debe permitir la adquisición, en la captura, de todos los elementos de los metadatos especificados en el momento de la configuración, así como su conservación junto con los registros electrónicos en una relación muy estrecha que se mantendrá en todo momento.
6.1.4	El SGRE debe garantizar que sólo administradores y usuarios autorizados puedan modificar el contenido de determinados elementos de los metadatos del registro electrónico.

Ref.	Requisito
6.1.5	Conviene que el SGRE sea capaz de asignar los mismos registros electrónicos a distintos ficheros electrónicos de un documento electrónico, sin que haya una duplicación física de los registros en cuestión. *Así, un usuario podría añadir una factura al fichero de un proveedor mientras otro la asigna a un fichero de productos. En otro ejemplo, un usuario podría decidir añadir un documento referente a dos asuntos a los dos ficheros pertinentes.* *Por lo general, esto se consigue con el uso de marcadores.*
6.1.6	El SGRE debe soportar la asistencia automática en la grabación de documentos electrónicos, extrayendo automáticamente los metadatos de los siguientes tipos de documentos, como mínimo: • Documentos de oficina (ejemplo: cartas escritas con un procesador de textos con un formato normalizado). • Correo electrónico sin ficheros adjuntos, tanto recibido como enviado. • Correo electrónico con ficheros adjuntos, tanto recibido como enviado. • Mensajes por fax recibidos y enviados.
6.1.7	El SGRE debe registrar como metadatos la fecha y la hora de la grabación. *Si la fecha y la hora forman parte del identificador único no será necesario almacenarlas por separado, siempre y cuando puedan extraerse de forma explícita de ese número.* *La exactitud de la hora dependerá de la aplicación.*
6.1.8	El SGRE debe garantizar la existencia de una entrada visualizable para cada registro grabado, de la que formarán parte los siguientes metadatos especificados en el momento de configurar del sistema. *Algunos de los metadatos exigidos pueden estar ya presentes o ser extraídos del registro automáticamente. El SGRE debe exigir la introducción del resto de los metadatos.*
6.1.9	El SGRE debe permitir la introducción de más metadatos descriptivos o de otros tipo en: • el momento de la grabación; y/o • una etapa posterior del proceso.
6.1.10	Cuando exista más de una versión de un documento, el SGRE deberá permitir que los usuarios opten al menos por una de las siguientes posibilidades: • La grabación de todas las versiones del documento en un solo registro. • La grabación de una sola versión del documento como registro. • La grabación de cada versión del documento como registro.

Ref.	Requisito
6.1.11	El SGRE debe facilitar de forma automática la adopción de decisiones sobre la clasificación de los registros electrónicos en ficheros electrónicos, de acuerdo con alguna de las posibilidades siguientes o con todas ellas: • dando acceso a un usuario o perfil de usuario a un solo subconjunto de un sistema de clasificación; • almacenando los ficheros más utilizados últimamente por cada usuario o perfil de usuarios; • sugiriendo los ficheros más utilizados últimamente por ese usuario; • sugiriendo ficheros que contienen registros electrónicos relacionados; • sugiriendo ficheros a partir de deducciones inferidas de elementos de los metadatos del registro, como palabras clave utilizadas en el título del documento; • sugiriendo ficheros a partir de deducciones inferidas del contenido del registro.
6.1.12	Conviene que, para completar el proceso de captura, el SGRE permita que los usuarios hagan llegar a otros usuarios registros electrónicos.
6.1.13	En relación con los registros electrónicos con más de un componente, el SGRE debe: • manejar el registro como si se tratase de una entidad única e indivisible, conservando las relaciones existentes entre sus componentes; • respetar la integridad estructural del registro; • permitir, más adelante, su recuperación, su visualización y su gestión integradas; • gestionar la eliminación de todos los componentes del registro electrónico como si se tratase de una sola unidad, es decir, en una sola operación. *Un ejemplo de tales registros lo constituirían las páginas web con gráficos incrustados.*

Ref.	Requisito
6.1.14	El SGRE debe permitir la asistencia automática en la grabación de los documentos electrónicos, extrayendo automáticamente tantos metadatos como sea posible de todas las clases de documentos que pueda. *La razón fundamental de este requisito es reducir al máximo la cantidad de datos que introducen los usuarios y aumentar así la precisión de los metadatos. Los elementos de los metadatos en cuestión y los tipos de documentos que admite este tratamiento dependerán del entorno. Por ejemplo, en una oficina, donde se trata con numerosos documentos de texto no estructurados o parcialmente estructurados, sería razonable incluir:* • *las cartas, los memorandos y otros documentos elaborados con procesadores de textos, aplicando plantillas normalizadas por la organización, que permitan la identificación automática de los elementos de los metadatos;* • *el correo electrónico, con o sin ficheros adjuntos, tanto recibido como enviado;* • *los mensajes que se envíen por fax.*
6.1.15	El SGRE debe prevenir a los usuarios que intenten grabar documentos ya grabados en el mismo fichero.

6.2 Importación de grandes volúmenes de registros

Pueden llegar al sistema grandes volúmenes de registros por muy distintos modos (por ejemplo, desde otro SGRE), como ficheros electrónicos formados por varios registros del mismo tipo (como facturas diarias) o en una transferencia en masa desde un EDMS. El SGRE debe ser capaz de aceptar estas importaciones e incluir elementos que le permitan gestionar el proceso de captura.

Ref.	Requisito
6.2.1	El SGRE debe ser capaz de capturar documentos sobre transacciones generados por otros sistemas. Esto deberá incluir: • la posibilidad de importar transacciones de ficheros de lotes predefinidos; • la edición de reglas que permitan personalizar la grabación automática de los registros; • el mantenimiento de la validación de la integridad de los datos.
6.2.2	El SGRE debe contar con instrumentos dedicados a la gestión de las colas de entrada.

Ref.	Requisito
6.2.3	Conviene que el SGRE sea capaz de crear múltiples colas de entrada para los distintos tipos de documentos. *Por ejemplo, en distintos entornos podría haber colas para el correo electrónico, la correspondencia escaneada, los documentos procedentes de un departamento, de un grupo de departamentos o individuales, las transacciones desde una aplicación informática o los documentos procedentes de un sistema de gestión de documentos.*

6.3 Tipos de documentos

Resumen

Las organizaciones tendrán que capturar una amplia gama de tipos de documentos con distintos formatos y estructuras. Los requisitos técnicos de su captura variarán en función de la complejidad de los documentos. En ciertos entornos no resulta posible identificar todas las clases de documentos por anticipado, pues algunos de ellos se reciben desde fuentes externas.

Documentos que se modifican por sí solos

En ocasiones es preciso capturar documentos capaces (o aparentemente capaces) de modificarse por sí mismos. Esta posibilidad puede dar lugar a requisitos complejos que en este documento sólo se tratarán someramente.

Ciertos documentos parecen modificarse por sí solos, esto es, su contenido da la impresión de cambiar sin necesidad de que el usuario intervenga. Un ejemplo bastante corriente lo ofrecen los documentos elaborados con procesadores de textos o con hojas de cálculo que contienen un «campo» o «código» que muestra la fecha de forma automática. La reproducción del documento (véase el Glosario en la sección 13.1) varía según la fecha. En casos extremos, el «campo» o el «código» pueden variar tanto que llegan a modificar por completo la apariencia del documento. Un ejemplo sería un código que mostrase la trayectoria completa del directorio de unos documentos: en ciertos casos, las modificaciones de esa trayectoria podrían causar grandes cambios en la paginación, debido la existencia de un nombre largo en un SGRE con una jerarquía de gran tamaño. No obstante, en realidad el documento no cambia, sólo lo hace su reproducción, según el software que se use para visualizarlo. Aunque los documentos que parecen cambiar por sí solos no incumplen el requisito de que el contenido del registro debe ser inmutable, parece que lo hagan, por lo que conviene evitarlos.

Otros documentos pueden contener códigos que sí modifican de veras el documento, como sería el caso de una hoja de cálculo con una «macro» sofisticada que cambiase el documento (por medio del software de aplicación utilizado para visualizarlo) y luego lo grabase de forma automática. En tales casos se corre el

riesgo de que el documento cambie durante el proceso de captura, en función de los detalles del proceso y los controles del SGRE. Obviamente, esta posibilidad resulta inaceptable.

En la mayoría de los casos es aconsejable almacenar estos documentos en un formato en que el código de automodificación quede desactivado, o bien visualizarlos únicamente con programas que no activen la modificación. Si el código de automodificación constituye una parte esencial del registro, habrá que tomar medidas adecuadas a cada caso.

Cuando se trata de documentos que se pueden imprimir, el formato PDF de Adobe y el ENVOY de Tumbleweed Software son ejemplos de formatos que desactivan el código de automodificación. En este caso, es fundamental cerciorarse de que la conversión al formato deseado no se efectúa de alguna forma que lleve a los documentos a modificarse de un modo no deseado. Por ejemplo, si se trata de una carta cuya fecha se modifica automáticamente, la conversión tendría que realizarse en la fecha que aparece en la carta.

Cuando resulte indispensable almacenar algún documento que se modifique automáticamente o que parezca hacerlo, conviene consignar la información sobre tales características en los metadatos de los registros.

Ref.	**Requisito**
6.3.1	El SGRE debe ser capaz de capturar como registros documentos pertenecientes a una gama de estructuras y tipos de formato de documento electrónico diferentes. *Conviene especificar esta gama antes de evaluar un sistema conforme a la presente especificación.*
6.3.2	El SGRE debe permitir la captura de los documentos de oficina de uso más común, tanto simples como complejos. Los formatos de documentos admitidos deben abarcar : • documentos sencillos: faxes, documentos de oficina, presentaciones, texto, imágenes, mensajes de correo electrónico (véase la sección 6.4), voz; • documentos complejos: correo electrónico con ficheros adjuntos, documentos de autoedición, páginas web, gráficos. *La lista de tipos de documentos que debe admitir el SGRE variará según la organización.*
6.3.3	Los formatos de documentos admitidos en el requisito 6.3.2 deben ser ampliables a medida que se introducen nuevos formatos.

Ref.	Requisito
6.3.4	Conviene que el SGRE pueda capturar los siguientes tipos de documentos: • Calendarios electrónicos • Información procedente de otras aplicaciones informáticas (por ejemplo, de contabilidad, nóminas y diseño asistido por ordenador) • Documentos en papel escaneados • Ficheros de voz • Videoclips • Mapas y esquemas digitales • Datos estructurados (por ejemplo, transacciones de IED) • Bases de datos • Documentos multimedios. *La lista de tipos de documento que convendría que admitiese el SGRE variará según la organización.*
6.3.5	El SGRE no debe imponer ningún límite práctico al número de registros que se puedan capturar en un fichero ni al número de registros que se puedan almacenar en el propio SGRE.
6.3.6	Conviene que el SGRE permita la captura de documentos compuestos de una de las siguientes maneras: • como un solo registro compuesto; • como una serie de registros simples vinculados, uno por cada componente del documento compuesto.

6.4 Gestión del correo electrónico

El correo electrónico se utiliza para enviar tanto mensajes simples como documentos (adjuntos), dentro de una misma organización o entre varias organizaciones. Las características del correo electrónico pueden dificultar su grabación y seguimiento. Las organizaciones han de ser capaces de realizar controles de gestión que les permitan:

- capturar todos los mensajes de correo electrónico recibidos y enviados y sus ficheros adjuntos; y/o
- dotar a sus usuarios de la capacidad de capturar ciertos mensajes de correo electrónico y sus ficheros adjuntos.

Esta última posibilidad exige que los usuarios evalúen la pertinencia y la importancia de los elementos, así como los riesgos que supone su no captura.

Ref.	Requisito
6.4.1	El SGRE debe permitir la elección de uno de los siguientes modos de funcionamiento en el momento de la configuración: • que los usuarios puedan capturar mensajes de correo electrónico (esto es, después de decidir si desean grabarlos); o bien • que el SGRE cuente con un proceso automático de captura de todos los mensajes de correo electrónico recibidos y enviados.
6.4.2	Conviene que el SGRE permita a los usuarios individuales tratar y capturar los mensajes de correo electrónico que reciban desde dentro del sistema de correo electrónico. Convendría que el usuario pudiera procesar cada mensaje en el buzón de entrada, desde el interior de su sistema de correo, tal y como se explica a continuación, ayudado por: • la visualización de cada mensaje de correo y de un indicador de sus ficheros adjuntos (si los hay); • la visualización del contenido de los ficheros adjuntos con un visor de documentos que admita múltiples formatos; • la grabación del mensaje de correo y de sus ficheros adjuntos como un nuevo registro en el SGR; • la vinculación del mensaje de correo y sus ficheros adjuntos a un registro ya existente en el SGRE.
6.4.3	Conviene que el SGRE garantice la captura de una versión de la dirección asociada al mensaje de correo electrónico que resulte inteligible para las personas; por ejemplo, es preferible «Jan Schmidt» a «jsa97@xyz.int».

7 REFERENCIAS

Las distintas entidades que componen el SGRE (clases, ficheros, volúmenes, registros) precisan identificadores únicos cada vez que se considere la entidad en cuestión. Esta característica se debe extender a todo el SGRE o bien al nivel jerárquico correspondiente. Dado que los requisitos de tales referencias coinciden, en este capítulo hemos agrupado los de las clases, ficheros, volúmenes y registros.

Ref.	Requisito
7.1.1	Siempre que aparezca en el SGRE un nuevo elemento de una de las siguientes categorías, el sistema deberá asociarlo a un identificador único (como se define más adelante): • Clase • Fichero • Volumen • Registro • Extracto de registro.
7.1.2	Todos los identificadores únicos del SGRE deben: • ser únicos en todo el SGRE; o bien • ser únicos en el nivel inmediatamente superior de la rama adecuada de la jerarquía en la que aparecen. *Como ejemplo de esta segunda opción, la trayectoria* *Contratos: Nombre de la empresa: Correspondencia* *es única, pero su segmento final se puede repetir en otras trayectorias, como en:* *Desarrollo del plan regional: Consulta pública: Correspondencia*
7.1.3	El SGRE debe ser capaz de almacenar los identificadores únicos como elementos de los metadatos de las entidades a las que se refieren.
7.1.4	Conviene que el SGRE permita especificar el formato del identificador único en el momento de la configuración. *El identificador puede ser numérico o alfanumérico o bien puede incluir una sucesión de identificadores de los volúmenes y los ficheros electrónicos que quedan por encima del registro en el sistema de clasificación.*

Ref.	Requisito
7.1.5	El SGRE debe: • generar el identificador único de forma automática y evitar que los usuarios lo introduzcan manualmente y que lo modifiquen (por ejemplo, un número secuencial); o bien • permitir que los usuarios introduzcan el identificador único, pero comprobando, antes de aceptarlo, que de veras es único (por ejemplo, un número de cuenta). *Una opción sería generar el identificador único de forma automática y luego ocultarlo al usuario, permitiendo que éste introdujera una cadena no única (por ejemplo, un apellido) como «identificador». El usuario utilizaría esta cadena como identificador, pero el SGRE lo consideraría un metadato definido por el usuario con posibilidad de búsqueda.*
7.1.6	Al crear una nueva clase o fichero electrónico en un sistema de clasificación que utilice una referencia de código numérico estructurada basada en una numeración secuencial, convendría que el SGRE generase de forma automática la siguiente secuencia de números disponibles en esa posición dentro del sistema de clasificación. *Por ejemplo, si una clase del sistema de clasificación ya contiene los ficheros:* *900 - 23 - 01 Fabricación: Tramitación del pedido: Validación del pedido* *900 - 23 - 02 Fabricación: Tramitación del pedido: Facturación* *900 -23 - 03 Fabricación: Tramitación del pedido: Tratamiento de notas de crédito* *De este modo, si el administrador añadiera un nuevo fichero a esta clase, convendría que el SGRE le asignara de forma automática la referencia 900 - 23 - 04.* *De igual forma, si el administrador añadiera una nueva clase a la de «Fabricación», convendría que el SGRE le asignara automáticamente la referencia 900 - 24.*
7.1.7	Si un SGRE genera de forma automática identificadores únicos, conviene que en el momento de la configuración permita al administrador especificar por qué número empezarán (por ejemplo, 0, 00, 100) y las unidades en que se incrementarán (por ejemplo 1, 10) en todos los casos.

8 BÚSQUEDA, RECUPERACIÓN Y REPRODUCCIÓN

La capacidad de que el usuario recupere ficheros y registros es parte integrante del SGRE. Esta opción abarca la búsqueda y reproducción de ficheros cuando se desconocen detalles concretos. La reproducción consiste en la presentación en pantalla («visualización en pantalla») o en su impresión, o bien en una presentación en vídeo o en audio (véase el Glosario, en la sección 13.1).

El acceso a los ficheros y registros y su posterior visualización exigen una gama amplia y flexible de funciones de búsqueda, recuperación y reproducción que respondan a las necesidades de los distintos tipos de usuarios. Aunque esta característica puede no considerarse una función clásica de la gestión de registros, en el presente documento se describe la funcionalidad necesaria, dado el escaso valor que tendría un SGRE desprovisto de buenos instrumentos de recuperación.

En la sección 8.1 se enumeran los requisitos de la búsqueda y la recuperación. Los relacionados con la reproducción se dividen en tres secciones: en la sección 8.2 se enumeran los requisitos de la visualización en pantalla; la sección 8.3 trata de la impresión, y la 8.4 se ocupa de la reproducción de los registros que no se pueden imprimir.

Seguridad

Todas las características y funcionalidades descritas en el presente capítulo deben estar sujetas a los controles de acceso descritos en la presente especificación, incluidos los controles de seguridad. En otras palabras, el SGRE nunca debe presentar a un usuario información que éste no tenga derecho a recibir. Para simplificar las cosas se parte de esta premisa, que no se repetirá en la exposición detallada de los requisitos.

8.1 Búsqueda y recuperación

El proceso de búsqueda consiste en la identificación de registros o ficheros por medio de unos parámetros definidos por el usuario con objeto de confirmar, localizar y recuperar los registros, los ficheros o sus metadatos, así como de acceder a ellos.

Las herramientas de búsqueda y navegación del SGRE dedicadas a la localización de metadatos, registros, volúmenes o ficheros precisan una serie de técnicas de búsqueda que respondan tanto a las necesidades de los usuarios «investigadores», más sofisticados, como a las de los ocasionales, con menores conocimientos de informática.

Ref.	Requisito
8.1.1	El SGRE debe incluir una gama flexible de funciones aplicables a los metadatos asociados a todos los niveles de la agregación de registros (fichero, clase) y al contenido de los registros a través de parámetros definidos por el usuario, a partir de los cuales se localizarán y recuperarán los registros y/o sus metadatos y se accederá a ellos, de forma individual o en grupo.
8.1.2	Convendría que los instrumentos de búsqueda del SGRE estuviesen integrados y que se presentasen de la misma forma a los usuarios en todos los niveles del sistema de clasificación. *Dicho de otro modo, convendría que todos los usuarios se encontrasen ante la misma interfaz, las mismas características y las mismas opciones, independientemente de si realizan búsquedas en clases, ficheros o registros.*
8.1.3	En el caso de los ficheros, conviene que el SGRE presente una funcionalidad compacta en las búsquedas de ficheros electrónicos, híbridos (véase 10.1) y físicos.
8.1.4	El SGRE debe permitir la búsqueda en todos los registros, volúmenes y metadatos de ficheros.
8.1.5	El SGRE debe permitir las búsquedas de contenido de texto en los registros.
8.1.6	El SGRE debe permitir que el usuario efectúe una solicitud de búsqueda única con combinaciones de metadatos y/o contenidos de registros.
8.1.7	El SGRE debe permitir a los administradores configurar y cambiar los campos de búsqueda, incluyendo: • la especificación como campo de búsqueda de cualquier elemento de los metadatos del fichero, el registro o el volumen y, de forma opcional, del contenido íntegro del registro; • la modificación de la configuración del campo de búsqueda.
8.1.8	El SGRE debe incluir herramientas de búsqueda que cubran las siguientes técnicas: • la búsqueda de texto libre de combinaciones de elementos de los metadatos de los registros y los ficheros y el contenido de los registros; • las búsquedas booleanas de elementos de los metadatos.
8.1.9	Conviene que el SGRE permita la búsqueda de texto libre y metadatos de una forma integrada y coherente.
8.1.10	Conviene que el SGRE permita la búsqueda conceptual mediante el uso de un tesauro incorporado como índice en línea. *Esto permitirá la recuperación de documentos, de su contenido o metadatos utilizando un término más amplio, más restringido o relacionado. Por ejemplo, una búsqueda de «servicios oftalmológicos» podría obtener como resultados «servicios sanitarios», «pruebas oculares» u «oftalmología».*

Ref.	Requisito
8.1.11	El SGRE debe permitir la búsqueda de metadatos utilizando «comodines» que permitan la expansión hacia atrás, hacia delante e interna. *Por ejemplo, el término de búsqueda «proy*» podría obtener como resultados «proyecto» y el término C*n obtendría «Comisión».*
8.1.12	Conviene que el SGRE admita la búsqueda por proximidad, que permite precisar la distancia entre dos palabras en el registro para poder aceptar el resultado.
8.1.13	Cuando se utilice una interfaz de usuario gráfica, el SGRE deberá disponer de un mecanismo que permita navegar por un entorno gráfico o de visualización de otro tipo, tanto a nivel de clase como a nivel de fichero. *Esta característica se podría utilizar con las técnicas de búsqueda antes descritas con objeto de proporcionar una representación de primer nivel de los metadatos de un grupo de registros o ficheros que cumplan los criterios de búsqueda especificados.*
8.1.14	El SGRE debe permitir la búsqueda dentro de un fichero electrónico (independientemente del nivel de la jerarquía del sistema de clasificación en que se encuentre) o entre ficheros.
8.1.15	El SGRE debe ser capaz de buscar y recuperar un fichero electrónico completo o un volumen de un fichero con todo su contenido y sus metadatos contextuales y representar esas entradas exhaustiva y exclusivamente en el contexto de ese fichero como grupo discreto y en un único proceso de recuperación. *Esta característica resulta necesaria, por ejemplo, cuando un usuario desea imprimir un fichero completo para llevarlo a una reunión o para facilitar un trabajo provisionalmente con documentos en papel por alguna otra razón.*
8.1.16	El SGRE debe ser capaz de buscar, recuperar y reproducir un fichero electrónico a partir de cualquiera de los principios de designación utilizados, entre los que se incluyen: • El nombre del fichero • El identificador del fichero (código de clasificación).
8.1.17	El SGRE debe mostrar el número total de resultados de una búsqueda en la pantalla del usuario y permitir que éste visualice dichos resultados o bien refine sus criterios de búsqueda y realice otra solicitud de búsqueda.
8.1.18	El SGRE debe permitir que los registros, ficheros, etc. enumerados en una lista de resultados sean seleccionados y abiertos (tras superar los controles de acceso) con un simple clic o bien pulsando una tecla.

Ref.	Requisito
8.1.19	Conviene que el SGRE permita realizar búsquedas de metadatos de cualquier objeto (registros, volúmenes, ficheros o clases) recurriendo a las técnicas expuestas en esta sección, se trate o no de documentos en formato electrónico y con independencia de que el objeto esté almacenado en línea, casi en línea o fuera de línea.
8.1.20	Conviene que el SGRE permita a los usuarios grabar y reutilizar sus consultas.
8.1.21	Conviene que el SGRE permita a los usuarios refinar (restringir) sus búsquedas. *Por ejemplo, convendría que un usuario pudiera iniciar una búsqueda a partir de la lista de resultados de otra anterior.*
8.1.22	Conviene que el SGRE permita especificar intervalos de tiempo en las solicitudes de búsqueda, como «la semana pasada», «este mes». *Esto contrasta con la especificación de intervalos basados en días naturales o números de días.*
8.1.23	El SGRE debe permitir a los usuarios recuperar ficheros y registros directamente mediante un identificador único. *Este requisito no será aplicable si el usuario no tiene acceso al identificador único (véase nota a 7.1.5).*
8.1.24	Conviene que el SGRE permita que los usuarios y administradores configuren los formatos de presentación de los resultados de búsquedas, incluyendo características y funciones como: • la elección del orden en que se muestran los resultados de la búsqueda; • la determinación del número de resultados que se muestran cada vez en pantalla en la visualización de la búsqueda; • la determinación del número máximo de resultados de una búsqueda; • la grabación de los resultados de la búsqueda; • la selección de los campos de metadatos que se muestran en la lista de resultados de la búsqueda.
8.1.25	Conviene que el SGRE ofrezca una clasificación de los resultados de la búsqueda según su pertinencia.
8.1.26	Conviene que el SGRE pueda relacionar un «extracto» de un registro electrónico (véase sección 9.3) con el registro original, de forma que la recuperación del primero permita la del segundo, al tiempo que se mantiene el control de acceso y los metadatos respectivos de los dos elementos.

Ref.	Requisito
8.1.27	Cuando se visualiza un registro o una agrupación de registros (por ejemplo, un fichero o una clase) o se trabaja con ellos, conviene, tanto si se trata de los resultados de una búsqueda como si no, que el usuario pueda utilizar las características del SGRE para encontrar, fácilmente y sin abandonar ni cerrar el registro, información sobre el nivel inmediatamente superior de agrupación. *Por ejemplo, al leer el registro el usuario debería ser capaz de averiguar en qué volumen y fichero se encuentra. Por otro lado, del examen de los metadatos del fichero debe desprenderse información sobre la clase en que se localizan.*
8.1.28	Ninguna función de búsqueda o recuperación del SGRE debe revelar jamás al usuario información alguna (contenido o metadatos del registro) que se le oculte en aplicación de los controles de acceso y seguridad (secciones 4.1 y 4.6 respectivamente).
8.1.29	Conviene que el SGRE sea capaz de controlar el acceso a los registros en función de criterios relacionados con restricciones sobre la propiedad intelectual y de generar datos de facturación para tales accesos. *Esta sucinta descripción comprende una amplia gama de funciones que superan el alcance de la presente especificación. Tal requisito se puede satisfacer dotando al sistema de la capacidad de establecer vínculos con un sistema de aplicaciones distinto.*

8.2 Reproducción: Visualización de registros

Un SGRE puede contener registros de muy diversos formatos y estructuras. El usuario debe disponer de instrumentos genéricos de visualización que permitan mostrar en pantalla, reproducir e imprimir una serie de formatos.

Ref.	Requisito
8.2.1	El SGRE debe reproducir los registros que se hayan recuperado con una solicitud de búsqueda. *Cuando el SGRE almacene los registros en un formato propietario, su reproducción se podrá efectuar con una aplicación externa al sistema.*
8.2.2	Conviene que el SGRE pueda reproducir los registros recuperados como resultado de la búsqueda sin necesidad de cargar la aplicación de software asociada. *Por lo general, esto se consigue con la integración de un paquete de software de visualización en el SGRE. La función suele ser conveniente, pues acelera la reproducción.*

Ref.	Requisito
8.2.3	Conviene que el SGRE sea capaz de visualizar todos los tipos de registros electrónicos que determine la organización, de tal modo que conserve la información de los registros (por ejemplo, todas las características de la presentación visual y la estructura producidas por el paquete de aplicaciones generador) y que reproduzca todos los componentes de un registro electrónico. *La organización tendrá que especificar cuáles son los paquetes de aplicaciones y los formatos necesarios.*

8.3 Reproducción: Impresión

Esta sección se ocupa de los registros que se pueden imprimir, así como de la pista de auditoría existente en el marco del SGRE.

El SGRE debe disponer de instrumentos de impresión que permitan a todos los usuarios obtener copias impresas de los registros y sus metadatos, así como otros tipos de información. En todos estos casos se entiende que la «impresión» se desarrolla al nivel de la aplicación, con todos los controles y características de los que se dispone habitualmente, como informes de varias páginas, encabezados o la utilización de una impresora con una configuración adecuada. Por lo general, no se considera que el vaciado de capturas de pantallas a la impresora baste para cumplir este requisito.

Ref.	Requisito
8.3.1	El SGRE debe proporcionar al usuario maneras flexibles de imprimir los registros y sus correspondientes metadatos, incluida la capacidad de imprimir uno o varios registros junto con los metadatos que determine el usuario.
8.3.2	El SGRE debe permitir la impresión de los metadatos de un fichero.
8.3.3	El SGRE debe permitir la impresión en una sola operación de todos los registros de un fichero en el orden que especifique el usuario.
8.3.4	El SGRE debe permitir que el usuario imprima una lista resumen de ciertos registros seleccionados (como el contenido de un fichero) en la que se enumere un subconjunto de elementos de los metadatos de cada registro (como el título, el autor o la fecha de creación) especificados por el usuario.
8.3.5	Conviene que el SGRE permita al administrador resolver si todas las listas impresas o todos los registros tendrán que llevar anejos ciertos elementos de los metadatos, como el título, el número de registro, la fecha y la categoría de seguridad.
8.3.6	El SGRE debe permitir que los usuarios impriman las listas de resultados de sus búsquedas.
8.3.7	El SGRE debe permitir que el administrador imprima uno o todos los parámetros administrativos.

Ref.	Requisito
8.3.8	El SGRE debe permitir a los administradores imprimir calendarios de conservación.
8.3.9	Conviene que el SGRE permita a los administradores imprimir el tesauro.
8.3.10	El SGRE debe permitir a los administradores imprimir el sistema de clasificación.
8.3.11	Cuando se recurra a él, el SGRE debe permitir a los administradores imprimir el repertorio de ficheros (véase 3.2.10).
8.3.12	El SGRE debe permitir a los administradores imprimir pistas de auditoría (véase 4.2).
8.3.13	El SGRE debe ser capaz de imprimir todos los tipos de registros electrónicos que especifique la organización. La impresión debe: • conservar la estructura producida por el paquete de aplicaciones generador; • incluir todos los componentes del registro electrónico (que se puedan imprimir). *La organización tendrá que especificar cuáles son los formatos y paquetes de aplicaciones necesarios.*

8.4 Reproducción: Otros

Esta sección sólo se refiere a los registros para los que no vale la pena recurrir a la impresión.

Ref.	Requisito
8.4.1	El SGRE debe disponer de instrumentos que permitan volcar a soportes apropiados los registros que no se puedan imprimir. *Ejemplos: los sitios web, o los ficheros de audio o vídeo.*

9 FUNCIONES ADMINISTRATIVAS

Cierto grado de transformación organizativa resulta normal, por lo que los instrumentos de apoyo y mantenimiento de los SGRE han de dar cabida a esta posibilidad. Además, estos sistemas deben dotar al administrador de medios que le permitan modificar el número de usuarios, aumentar las exigencias en cuanto a capacidad de almacenamiento, proceder a la recuperación tras un fallo del sistema y efectuar un seguimiento de los errores de éste.

Algunos de estos instrumentos puede aportarlos el EDMS asociado o bien el sistema de gestión de bases de datos.

En el presente capítulo se enumeran los requisitos relativos a la administración general (sección 9.1), a los informes del sistema (sección 9.2) y a la redacción de registros (sección 9.3).

9.1 Administración general

Esta sección trata de los requisitos relativos a la gestión de los parámetros del sistema, las copias de seguridad y la restauración, la gestión del sistema y la administración de usuarios.

Ref.	Requisito
9.1.1	El SGRE debe permitir que los administradores, de forma controlada y sin ningún esfuerzo innecesario, recuperen, visualicen y reconfiguren parámetros del sistema y opciones escogidas en el momento de la configuración, como los elementos que se indexarán, así como la asignación de usuarios y funciones a otros perfiles de usuarios.
9.1.2	El SGRE debe incluir instrumentos de copia de seguridad y características que permitan restaurar el sistema a partir de tales copias y de la pista de auditoría, sin menoscabo de la integridad del sistema. *En otras palabras, el SGRE debe ser capaz de recrear los registros y metadatos tal y como eran en un momento determinado, mediante una restauración de las copias de seguridad combinada con el uso de pistas de auditoría.*
9.1.3	El SGRE debe incluir instrumentos de recuperación y restauración en previsión de posibles fallos del sistema o de errores en la actualización. Asimismo, deberá notificar a los administradores el resultado de la operación. *En otras palabras, el SGRE debe permitir que los administradores «deshagan» una serie de transacciones hasta llegar a un estado en que la integridad de la base de datos quede garantizada. Ello sólo será necesario si se produce algún error.*

Ref.	Requisito
9.1.4	El SGRE debe supervisar el espacio de almacenamiento disponible y avisar a los administradores cuando convenga intervenir, ya sea por escasez de espacio, ya porque proceda alguna otra medida de tipo administrativo.
9.1.5	Conviene que el SGRE supervise las tasas de error de los soportes de almacenamiento e informe al administrador de los soportes o dispositivos que presentan tasas superiores a las fijadas en el momento de la configuración. *En especial, este requisito se refiere a los soportes ópticos.*
9.1.6	El SGRE debe permitir que los administradores realicen cambios masivos en el sistema de clasificación, sin menoscabo de la correcta y completa manipulación de todos los metadatos y de la pista de auditoría, de forma que sea posible realizar los siguientes tipos de modificaciones en la organización del sistema: • la división de una unidad de organización en dos; • la combinación de dos unidades de organización en una sola; • el traslado o la redenominación de una unidad de organización; • la división de una estructura íntegra en dos estructuras. Cuando se realiza algún cambio de este tipo, los ficheros cerrados han de mantenerse en ese estado y conservar las referencias al sistema de clasificación previo al cambio. Por su parte, en el caso de los ficheros abiertos se puede optar por una de estas dos posibilidades: • cerrarlos, de forma que conserven las referencias al sistema de clasificación previo al cambio y se constituyan referencias cruzadas a un nuevo fichero del sistema de clasificación modificado; o bien • remitirlos al sistema de clasificación modificado, pero manteniendo todas las referencias al sistema de clasificación previo al cambio. *Los cambios de las unidades estructurales descritos pueden conllevar modificaciones de los sistemas de clasificación de las unidades y sus poblaciones de usuarios.* *La expresión «cambios masivos» designa todas las modificaciones realizadas en las clases, los ficheros y los registros afectados que se pueden llevar a cabo en un número de operaciones pequeñas, en lugar de caso por caso.*
9.1.7	El SGRE debe permitir el movimiento de usuarios entre las distintas unidades de organización .
9.1.8	El SGRE debe permitir que se definan perfiles de usuarios y que a cada perfil se le asocien varios usuarios. *Véase también 4.1.3.*

9.2 Informes

Esta sección se limita a ofrecer requisitos generales, pues no procede intentar reproducir en este documento los requisitos de un subsistema complejo de elaboración de informes. En cualquier caso, los requisitos relativos a la cantidad y la exhaustividad de los informes vendrán determinados por el tamaño, la complejidad y los niveles de cambio del sistema de clasificación, así como por el número y la naturaleza de los registros y por la base de usuarios.

Ref. **Requisito**

9.2.1 El SGRE debe incluir instrumentos flexibles de elaboración de informes a los que pueda recurrir el administrador. Como mínimo, deben incluir la capacidad de informar sobre:

- el número de ficheros, volúmenes y registros;
- las estadísticas de las transacciones con ficheros, volúmenes y registros;
- las actividades de cada usuario.

9.2.2 El SGRE debe permitir que los administradores realicen consultas y generen informes basados en la pista de auditoría. Como mínimo, tales informes han de poder basarse en:

- determinadas clases
- determinados ficheros
- determinados volúmenes
- determinados registros
- determinados usuarios
- determinados intervalos de tiempo.

9.2.3 Conviene que el SGRE permita a los administradores realizar consultas y elaborar informes sobre la pista de auditoría basados en:

- determinadas categorías de seguridad
- determinados grupos de usuarios
- otros metadatos.

9.2.4 El SGRE debe permitir la elaboración de un informe en el que se enumeren todos los ficheros y volúmenes, estructurados de modo que reflejen el sistema de clasificación parcial o totalmente.

9.2.5 Conviene que el SGRE incluya instrumentos que permitan clasificar y seleccionar datos de los informes.

9.2.6 Conviene que el SGRE incluya instrumentos que permitan compendiar y resumir los datos de los informes.

9.2.7 El SGRE debe permitir que los administradores soliciten la elaboración de informes periódicos o puntuales.

Ref.	Requisito
9.2.8	Conviene que el SGRE permita al administrador restringir el acceso de los usuarios a determinados informes.

9.3 Modificación, borrado y redacción de registros

Como principio básico, por lo general los ficheros y registros no se deben poder modificar ni borrar hasta el final de su ciclo de vida en el SGRE. No obstante, pueden surgir circunstancias excepcionales en las que resulte necesario hacerlo (por ejemplo, a causa de un error de un usuario). En esta sección se definen los requisitos pertinentes.

Los administradores se pueden ver obligados a «borrar» registros para corregir errores del usuario (por ejemplo, la inclusión de registros en un fichero equivocado) o bien para cumplir ciertas disposiciones legales en materia de protección de datos. Por borrado se puede entender:

- la destrucción (véase 5.3.13 y 5.3.15);
- la conservación, con una nota en los metadatos del registro que indique que éste se considera retirado del control de la gestión de registros.

La capacidad de borrar ha de ser objeto de un control estricto encaminado a proteger la integridad general de los registros. En particular, habrá que almacenar la información relacionada con el borrado en la pista de auditoría y conservar vestigios de los registros borrados en la carpeta o las carpetas afectadas.

En ocasiones, los administradores deben publicar o facilitar registros con información que aún es de carácter reservado, debido a normas de protección de datos, a consideraciones de seguridad, a algún riesgo comercial, etc. Por lo tanto, han de poder suprimir la información confidencial sin que ello afecte al registro en cuestión. Tal proceso se denomina, en el presente documento, redacción, y el SGRE almacena tanto el registro original como la copia redactada, que aquí llamaremos «extracto» del registro. Téngase en cuenta que la necesidad de realizar extractos varía de un país a otro, según la tradición.

Nótese que las cuestiones relativas al borrado y la modificación también se tratan en el capítulo 5.

Ref.	Requisito
9.3.1	El SGRE debe estar dotado, por defecto o de forma opcional, de un mecanismo que impida que un administrador o usuario borre o traslade un registro tras su captura. Ello supone que cualquier requisito que permita a un administrador considerar un registro «borrado» (como con 9.3.7) o «reubicado» (como en 3.4.1), en realidad significa que el registro se ha marcado de la manera adecuada y que, en el caso de la reubicación, se ha colocado una copia o un marcador en su nuevo emplazamiento. *Este requisito no afecta a la transferencia y la destrucción de registros conforme a un calendario de conservación, œomo se describe en la sección 5.3.*
9.3.2	Conviene que en el momento de la configuración y como alternativa al requisito 9.3.1, el SGRE permita que el «borrado» de un registro equivalga a la destrucción de éste.
9.3.3	El administrador debe ser capaz de modificar la categoría de seguridad de cada registro. *Ésta es una capacidad habitualmente necesaria para reducir el grado de protección de los registros a medida que disminuye su confidencialidad.*
9.3.4	El administrador debe poder modificar las categorías de seguridad de todos los registros de un fichero o una clase en una sola operación. El SGRE debe avisar de la reducción de la categoría de seguridad de un fichero y esperar confirmación antes de concluir la operación. *Ésta es una característica habitualmente necesaria para reducir el grado de protección de un registro a medida que disminuye su confidencialidad.*
9.3.5	Siempre que se satisfagan los requisitos 12.4.10 y 4.6.2, el administrador deberá poder modificar la categoría de seguridad de los ficheros.
9.3.6	El SGRE debe consignar con todo detalle cualquier modificación de la categoría de seguridad de los metadatos del registro, volumen o fichero afectado.

Ref.	Requisito
9.3.7	El administrador debe contar con la posibilidad de borrar clases, ficheros, volúmenes y registros (en función de la opción escogida en 9.3.1). No obstante, siempre que adopte esa medida el SGRE deberá: • registrar la acción con todo detalle en la pista de auditoría; • crear un informe de excepción destinado al administrador; • borrar con un fichero o volumen su contenido íntegro; • cerciorarse de que no se borra ningún documento cuando ello pueda dar lugar a cambios en otro registro, como sucede cuando un documento forma parte de dos registros (véase 6.1.5) y se va a borrar uno de ellos; • señalar al administrador cualquier vínculo que remita otro fichero o registro a un fichero o volumen que esté a punto de borrase, y solicitar su confirmación antes de proceder; • mantener en todo momento la integridad de todos los metadatos (en especial, teniendo en cuenta 12.4.20 y 12.7.24). *La funcionalidad de esta característica sólo está prevista en casos excepcionales.*
9.3.8	El administrador debe ser capaz de modificar cualquier elemento de metadato introducido por el usuario. Cualquier cambio de este tipo deberá constar en la pista de auditoría. *El objeto de esta función es permitir que los administradores corrijan errores de los usuarios, por ejemplo en la introducción de datos, al tiempo que se mantiene el acceso de los usuarios y grupos de usuarios.*
9.3.9	El SGRE debe permitir que el administrador realice una copia de un registro con fines de redacción. *En la presente especificación, tal copia se denominará «extracto» del registro.*

Ref.	Requisito
9.3.10	Conviene que el SGRE posea una función que permita trasladar u ocultar la información confidencial del extracto. Cuando menos, tendría que: • eliminar páginas concretas de un registro de imagen con varias páginas; • superponer rectángulos opacos que cubran los nombres o palabras confidenciales; • contar con cualquier otra característica necesaria en relación con los formatos de audio y vídeo, cuando existan. Si el SGRE no aporta de forma directa tales instrumentos, deberá permitir que otros paquetes de software los proporcionen. *Es esencial que cuando se haga uso de éstas u otras características de redacción la información eliminada u oculta no conste jamás en el extracto, ya se trate de una visualización en pantalla, ya de un documento impreso o reproducible de alguna otra manera, sin que influya el recurso a manipulaciones como la rotación, el zoom y similares.*
9.3.11	Cuando se cree un extracto, el SGRE deberá consignar tal operación entre los metadatos del registro e incluir como mínimo la fecha, la hora, el motivo de la creación y el autor.
9.3.12	Conviene que el SGRE solicite al creador de un extracto que asigne éste a un fichero.
9.3.13	Conviene que el SGRE almacene una referencia cruzada (como en 11.1.18) a un extracto del mismo fichero y volumen del registro original, aunque ese volumen del fichero esté cerrado.
9.3.14	El SGRE debe consignar en la pista de auditoría cualquier modificación realizada en respuesta a los requisitos de esta sección.

10 OTRAS FUNCIONALIDADES

Este capítulo trata de ciertos requisitos que pueden resultar pertinentes en relación con funcionalidades estrechamente relacionadas con la gestión de registros electrónicos. Aborda los requisitos de la gestión de registros físicos dentro del SGRE, la gestión de documentos, los flujos de tareas, las firmas electrónicas y otros mecanismos de autenticación.

Nótese que esta especificación no aborda la necesidad de mantener registros físicos. Tal necesidad puede existir o no, en función de los entornos normativos y legislativos; pero cuando exista será preciso extremar el cuidado en la conservación de la integridad y la usabilidad del conjunto de ficheros físicos y electrónicos. De estas cuestiones se deberían ocupar las políticas organizativas correspondientes.

En cada caso, se ofrece una visión de los requisitos a alto nivel, y, dado que éstos no definen las funciones básicas de un SGRE, se tratan deliberadamente de un modo más bien indicativo.

En cada sección de este capítulo se tratan los requisitos de un ámbito concreto:

- En la sección 10.1, la gestión de registros no electrónicos.
- En la sección 10.2, la conservación y eliminación de ficheros híbridos.
- En la sección 10.3, la gestión de documentos.
- En la sección 10.4, el flujo de tareas.
- En la sección 10.5, las firmas electrónicas.
- En la sección 10.6, la encriptación.
- En la sección 10.7, las filigranas electrónicas, etc.
- En la sección 10.8, la interfuncionalidad y la apertura.

10.1 Gestión de registros no electrónicos

El depósito de registros de una organización puede incluir, aparte de registros electrónicos, registros en papel y en otros soportes, como vídeos o casetes. Tales registros se denominan «ficheros físicos». Conviene que el SGRE pueda incluir los ficheros físicos en el mismo sistema de clasificación que los electrónicos y que permita la administración de «ficheros híbridos» formados por registros físicos y electrónicos.

Ref.	Requisito
10.1.1	El SGRE debe ser capaz de definir ficheros y volúmenes físicos en el sistema de clasificación y permitir que la presencia de registros físicos en tales volúmenes se refleje y se gestione del mismo modo que los registros electrónicos.
10.1.2	El SGRE debe definir en el sistema de clasificación ficheros que (lógicamente) contengan registros tanto físicos como electrónicos, y debe permitir la administración integrada de ambos tipos de registros. *En esta especificación tales elementos se denominan «ficheros híbridos». En la práctica, los ficheros híbridos estarán formados por un fichero electrónico y otro físico.*
10.1.3	El SGRE debe permitir que un fichero físico asociado, en tanto que híbrido, a un fichero electrónico, utilice el mismo título y código de referencia numérica que éste, pero con una indicación añadida de que se trata de un fichero físico híbrido.
10.1.4	El SGRE debe permitir la configuración de un conjunto distinto de elementos de metadatos según se trate de ficheros físicos o electrónicos. Los ficheros físicos incluirán entre sus metadatos información sobre la ubicación física del fichero físico (véase 12.5.7).
10.1.5	Conviene que el SGRE permita el rastreo de los ficheros físicos mediante instrumentos que consignen su salida, su entrada y su recordatorio y reflejen la ubicación del fichero en ese momento.
10.1.6	El SGRE debe garantizar que la recuperación de un fichero híbrido conlleve la de los metadatos de los registros electrónicos y en papel a él asociados.
10.1.7	Siempre que se haya asignado a los ficheros una categoría de seguridad (véase 4.6), conviene que el SGRE garantice que se asigne a los ficheros físicos híbridos la misma categoría que los ficheros electrónicos a los que están asociados.
10.1.8	El SGRE debe incluir características que controlen y consignen el acceso a los ficheros físicos, lo que incluirá controles basados en la categoría de seguridad, comparables con las funciones propias de los ficheros electrónicos (como se definen en el capítulo 4).
10.1.9	Conviene que el SGRE permita la impresión y el reconocimiento de códigos de barras o que admita otros sistemas de rastreo, con vistas a la automatización de la entrada de datos en el rastreo de los movimientos de los ficheros físicos.

10.2 Conservación y eliminación de los ficheros híbridos

Ref.	Requisito
10.2.1	El SGRE debe permitir la asignación de calendarios de conservación a todos los ficheros físicos del sistema de clasificación. Dichos calendarios deben funcionar de un modo coherente con el de los calendarios de los ficheros electrónicos y avisar al administrador cuando se alcance la fecha de eliminación, si bien tomando en consideración las diferencias en los procesos de destrucción o archivo de los ficheros electrónicos y en papel.
10.2.2	El SGRE debe permitir la aplicación del mismo calendario de conservación a los ficheros físicos y electrónicos que componen un fichero híbrido.
10.2.3	El SGRE debe ser capaz de aplicar cualquier decisión sobre revisiones de ficheros electrónicos híbridos que atañan a los ficheros físicos híbridos a ellos asociados.
10.2.4	El SGRE debe avisar al administrador de la existencia y la ubicación de cualquier fichero físico híbrido asociado a un fichero electrónico híbrido que vaya a ser exportado o transferido.
10.2.5	El SGRE debe ser capaz de registrar en la pista de auditoría todas las modificaciones realizadas en las referencias de los metadatos a ficheros y registros físicos o híbridos.
10.2.6	Conviene que el SGRE permita la aplicación de una decisión de revisión de un grupo de ficheros a cualquier fichero físico de tal grupo, mediante la notificación al administrador de las acciones necesarias en relación con tales ficheros físicos.
10.2.7	Conviene que el SGRE sea capaz de exportar y transferir metadatos de los registros y ficheros físicos.
10.2.8	Conviene que el SGRE posea instrumentos capaces de registrar la entrada y la salida de los ficheros físicos del sistema y, en particular, que permitan consignar la ubicación concreta de su destino o la identidad del usuario de destino. Asimismo, convendría que el sistema fuera capaz de mostrar esa información cuando otro usuario solicite el fichero físico. *Previo cumplimiento de las normas de seguridad establecidas en la sección 4.6.*
10.2.9	Conviene que el SGRE incluya una función de recordatorio de los ficheros físicos introducidos en el sistema que permita a los usuarios introducir una fecha de recordatorio o de reserva de un fichero físico y que genere un mensaje al respecto que se hará llegar al usuario en posesión de tal fichero o al administrador, según la configuración. *Previo cumplimiento de las normas de seguridad establecidas en la sección 4.6.*

10.3 Gestión de documentos

Las organizaciones recurren a menudo a los sistemas de gestión electrónica de documentos, o EDMS, para gestionar y controlar documentos electrónicos. Muchas de las funciones e instrumentos de los EDMS coinciden con las de los SGRE. Por lo general, los EDMS abarcan la indexación de documentos, la gestión de su almacenamiento, el control de versiones, la integración con aplicaciones de escritorio y las herramientas de recuperación que permiten el acceso a los documentos. Ciertos SGRE poseen todas las capacidades de un EDMS, mientras que otros no están dotados más que de una parte de ellas. Y a la inversa, también algunos EDMS han incorporado ciertas funciones básicas de gestión de registros.

Con objeto de aclarar ciertos conceptos, en la siguiente tabla se indican las diferencias más frecuentes.

Un EDMS…	**Un SGRE…**
• Permite que se modifiquen los documentos y/o que existan varias versiones de éstos.	• Impide que se modifiquen los registros.
• Puede permitir que los documentos sean borrados por sus propietarios.	• Impide que los registros sean borrados, excepto en ciertas circunstancias sujetas a un control muy estricto.
• Puede incluir calendarios de conservación.	• Debe incluir controles de conservación muy rigurosos.
• Puede contar con una estructura de almacenamiento de documentos de cuyo control se podrían encargar los usuarios.	• Debe contar con una estructura de gestión de registros muy rigurosa (el sistema de clasificación) de cuyo mantenimiento se encarga el administrador.
• Tiene por objetivo esencial facilitar el uso cotidiano de documentos en la actividad en curso.	• Puede facilitar el trabajo cotidiano, pero también tiene por objetivo ofrecer un depósito seguro a los registros más importantes relacionados con la actividad de la organización.

En esta sección se establecen los requisitos que se han de tener más en cuenta durante la creación de una solución integrada SGRE/EDMS. Los requisitos sólo son pertinentes cuando los instrumentos del EDMS forman parte de la solución.

Ref.	Requisito
10.3.1	Siempre que un EDMS forme parte de un SGRE o esté estrechamente integrado en éste, el EDMS debe poder capturar automáticamente documentos electrónicos generados en el curso de la actividad y remitirlos al proceso de grabación del SGRE.
10.3.2	Un SGRE que disponga de instrumentos de gestión de documentos debe ser capaz de: • capturar un registro electrónico en un solo proceso; • registrar un documento electrónico y completar su captura con posterioridad.
10.3.3	Conviene que los usuarios sean capaces de grabar documentos tanto desde dentro del EDMS como desde la aplicación en él integrada. *Este requisito adquiere especial importancia cuando el EDMS/SGRE se utiliza en un entorno general de oficina. En muchos casos se puede considerar obligatorio.*
10.3.4	El usuario del EDMS o de la aplicación en él integrada debe poder transferir los documentos con facilidad desde y hasta el SGRE, con objeto de convertir los documentos en registros desde el mismo EDMS.
10.3.5	Un SGRE con funciones de gestión de documentos debe ser capaz de procurarse los elementos de los metadatos directamente desde la aplicación generadora de documentos y permitir que el usuario añada a éstos otros elementos de metadatos. *Por ejemplo, la hora de creación y el usuario responsable de la generación de un documento, y, cuando existan, metadatos identificables a partir de campos estructurados de esos documentos, como la fecha y el tema.*
10.3.6	El SGRE debe ser capaz de añadir interfaces a las nuevas aplicaciones del EDMS que la organización decida utilizar.
10.3.7	Conviene que un SGRE con funciones de gestión de documentos pueda gestionar documentos electrónicos (no establecidos como registros) en el contexto del mismo sistema de clasificación y acceder a mecanismos de control como registros electrónicos.
10.3.8	Siempre que un EDMS forme parte de un SGRE o esté estrechamente integrado en él, conviene que la integración alcance también a las funciones de mantenimiento del sistema de clasificación.
10.3.9	Conviene que los SGRE con funciones de gestión de documentos sean capaces de administrar versiones de un documento electrónico como si se tratase de entidades separadas pero relacionadas, al tiempo que se mantienen los vínculos entre ellas.

Ref.	Requisito
10.3.10	Conviene que el EDMS sea capaz de restringir la visualización de los usuarios a: • la última versión de un documento; • todas las versiones de un documento o una selección de ellas; • las versiones que se hayan capturado o establecido como registros. En el momento de la configuración se seleccionará una de estas opciones.
10.3.11	Conviene que un SGRE con funciones de gestión de documentos sea capaz de interactuar con paquetes asociados a su actividad, como los sistemas de tratamiento de imágenes, de escáner o de flujos de tareas, sin perjuicio del pleno control de los registros electrónicos existentes.
10.3.12	El SGRE debe ser capaz de copiar el contenido de un registro electrónico para crear un documento electrónico nuevo y separado, al tiempo que se garantiza la conservación del registro original. *Así, un usuario podría copiar un registro con el propósito de enviar una copia a un destinatario que no fuera usuario del SGRE. Esta copia podría considerarse o no un nuevo registro, en función de las circunstancias.*

10.4 Flujos de tareas

La *Workflow Management Coalition (WfMC)*, asociación internacional dedicada al desarrollo de normas sobre los flujos de tareas y la interfuncionalidad de los distintos sistemas de flujos de tareas, define el flujo de tareas como la automatización de una parte o de la totalidad de un proceso empresarial en que ciertos documentos, información o tareas pasan de un participante a otro con vistas a la realización de acciones conforme a un conjunto de normas de procedimiento. En esta definición se entiende por «participante» un usuario, un grupo de trabajo (esto es, un equipo) o una aplicación de software.

Los requisitos enumerados en esta sección solamente resultan pertinentes cuando el SGRE presenta alguna característica relacionada con el flujo de tareas. Éstas van desde las funciones de rutina básicas a los instrumentos de flujo de tareas más sofisticados, que se pueden conseguir integrando en el SGRE un producto de flujo de tareas creado por terceros.

Las tecnologías de flujo de tareas transfieren objetos electrónicos entre los participantes, sometiendo todo el proceso al control automático de un programa. En el contexto de los SGRE, el flujo de tareas se utiliza para mover registros electrónicos entre usuarios y departamentos. Por lo general se recurre a él en:

- la gestión de procesos o tareas vitales, como los procedimientos de grabación y estructuración de ficheros o registros;

- la verificación y aprobación de los registros antes de proceder a su grabación;
- la derivación de registros o ficheros, de forma controlada, de usuario a usuario, con vistas a la realización de determinadas acciones, tales como la comprobación de un documento o la aprobación de una nueva versión;
- la comunicación a los usuarios de la disponibilidad de registros;
- la distribución de registros;
- la publicación de registros en la Red.

La capacidad de los sistemas de flujos de tareas va desde la simple derivación (como la verificación y aprobación de un documento antes de grabarlo) al manejo de un volumen elevado de transacciones, en las que pueden presentarse circunstancias excepcionales, y a la presentación de informes sobre el rendimiento individual y del sistema.

Ref.	**Requisito**
10.4.1	La función de flujo de tareas del SGRE debe ofrecer flujos de tareas formados por una serie de pasos, cada uno de los cuales sería, por ejemplo, el traslado de un registro o fichero de un participante a otro con vistas a la realización de la acción correspondiente.
10.4.2	Conviene que el SGRE no limite en la práctica el número de pasos que componen cada flujo de tareas.
10.4.3	El flujo de tareas del SGRE debe incluir una función que avise a un usuario participante cuando se envía uno de sus ficheros o registros a su «bandeja de entrada electrónica» para que le preste atención, además de indicar al usuario la acción que debe llevar a cabo.
10.4.4	El flujo de tareas del SGRE debe admitir el uso del correo electrónico para que un usuario pueda notificar a otros la existencia de registros que reclaman su atención. *Esta característica conlleva la integración del sistema de correo electrónico existente, más que la implantación de un sistema independiente o con formato propietario.*
10.4.5	La función de flujo de tareas del SGRE debe permitir al administrador la definición y el mantenimiento de flujos de tareas previamente programados.
10.4.6	La función de flujos de tareas del SGRE deberá impedir que los flujos de tareas previamente programados sean modificados por los usuarios, aparte del administrador y quienes cuenten con su autorización.

Ref.	Requisito
10.4.7	Conviene que el administrador sea capaz de decidir qué usuarios podrán reasignar tareas o acciones de un flujo de tareas y remitirlas a otros usuarios o grupos de usuarios. *Un usuario podría desear enviar un fichero o registro a otro usuario, bien debido al contenido del registro, bien por la ausencia del usuario en principio asignado.*
10.4.8	La función de flujo de tareas del SGRE debe consignar en la pista de auditoría todas las modificaciones realizadas de los flujos de tareas previamente programados.
10.4.9	La función de flujo de tareas del SGRE debe consignar el progreso de un registro o fichero a lo largo del flujo, de forma que los usuarios puedan averiguar el estado de cada registro o fichero en cualquier etapa del proceso.
10.4.10	El SGRE no debe limitar en la práctica el número de flujos de tareas que se pueden definir.
10.4.11	Conviene que la función de flujo de tareas del SGRE gestione los ficheros y registros en colas que el administrador pueda examinar y controlar.
10.4.12	Conviene que la función de flujo de tareas del SGRE pueda permitir a los participantes visualizar las colas de trabajo a ellos dirigidas y seleccionar los elementos con los que van a trabajar.
10.4.13	Conviene que la función de flujo de tareas del SGRE permita la existencia de flujos condicionales en función de las decisiones del usuario o de los datos del sistema. *En otras palabras, conviene que permita la existencia de flujos que trasladen el fichero o registro a un participante dependiendo de una condición establecida por uno de los participantes. Por ejemplo, un flujo podría llevar un registro a un participante dedicado al control del crédito o a una sección de consolidación de pedidos, en función de la información que haya introducido un supervisor de ventas, o bien el flujo podría variar conforme al valor de un pedido, calculado por el propio sistema.*
10.4.14	Conviene que la función de flujo de tareas del SGRE incluya una función recordatorio de ficheros y registros.
10.4.15	Conviene que la función de flujo de tareas del SGRE permita a los usuarios interrumpir un flujo (es decir, suspenderlo) de manera temporal, mientras atienden a otras cuestiones.
10.4.16	La función de flujo de tareas del SGRE debe reconocer como «participantes» tanto a los individuos como a los grupos de trabajo.

Ref.	Requisito
10.4.17	Siempre que el participante sea un grupo de trabajo, conviene que la función de flujo de tareas del SGRE incluya un instrumento que distribuya los nuevos elementos entre los miembros del grupo, ya sea por turnos, ya al término de la tarea que el miembro en cuestión esté realizando, con objeto de equilibrar la carga de trabajo de los miembros del equipo.
10.4.18	Conviene que la función de flujo de tareas del SGRE sea capaz de establecer prioridades entre los elementos de las colas.
10.4.19	Conviene que la función de flujo de tareas del SGRE incluya el tratamiento en «rendezvous». *Para ello es necesario que el flujo de tareas se detenga a esperar la llegada de un documento o registro electrónico asociado. Una vez se haya recibido el elemento esperado, el flujo volverá a ponerse en movimiento de forma automática.*
10.4.20	Conviene que la función de flujo de tareas del SGRE sea capaz de asociar fechas límite a pasos o procesos individuales de cada flujo y de informar de los elementos atrasados conforme a tales límites.
10.4.21	Conviene que la función de flujo de tareas del SGRE permita que la recepción de un documento electrónico ponga en funcionamiento de forma automática un flujo de tareas.
10.4.22	La función del flujo de tareas del SGRE debe incluir instrumentos de informe exhaustivos que permitan a los gestores controlar el volumen, los resultados y las excepciones del proceso.

10.5 Firmas electrónicas

Las firmas electrónicas, también denominadas firmas digitales, son secuencias de caracteres que, tras la aplicación de unos complejos procedimientos algorítmicos y «claves» (una larga cadena de dígitos análogos a una contraseña), se pueden emplear para verificar la integridad de un registro o la autenticidad de la identidad del remitente de un registro. El MD5 es un ejemplo de algoritmo de firma electrónica de uso común.

El uso habitual del correo electrónico e Internet entre las organizaciones ha aumentado el número de documentos que se mueven a escala interna, y sobre todo externa, en entornos que, en términos relativos, están sujetos a un control escaso. En este contexto, la adopción de las firmas electrónicas como medio de autenticación y confirmación de la integridad de los envíos se está convirtiendo en un fenómeno generalizado.

Los requisitos enumerados en esta sección sólo se aplicarán cuando exista la necesidad de gestionar registros dotados de una firma electrónica. En el momento de elaborar el presente documento, este concepto tiene una gran influencia de las

nuevas tecnologías, aún sujetas a cambios e incertidumbre. Los usuarios de esta especificación deberían verificar con los expertos pertinentes los requisitos y las consecuencias del almacenamiento a largo plazo.

Ref.	Requisito
10.5.1	El SGRE debe ser capaz de conservar la información relativa a las firmas electrónicas, la encriptación y los datos de los correspondientes organismos de verificación.
10.5.2	Conviene que el SGRE presente una estructura que facilite la introducción de distintas tecnologías de firma electrónica. *Vistas las transformaciones que se suceden en este ámbito, ésta característica resulta especialmente valiosa.*
10.5.3	Conviene que el SGRE sea capaz de verificar la validez de una firma electrónica.
10.5.4	El SGRE debe poder conservar y mantener como metadatos ciertos detalles relacionados con el proceso de verificación de una firma electrónica, tales como: • la prueba de la verificación de la validez de la firma; • la autoridad de certificación que ha validado la firma; • la fecha y la hora en que se realizó la verificación.
10.5.5	Conviene que el SGRE sea capaz de verificar la validez de una firma electrónica en el momento de la captura del registro.
10.5.6	Conviene que el SGRE posea funciones que permitan mantener la integridad de los registros dotados de firmas electrónicas (y demostrar ese mantenimiento), aun cuando un administrador haya modificado algunos de sus metadatos, pero no el contenido del registro, con posterioridad a la aplicación de la firma electrónica al registro en cuestión. *No existe ninguna obligación en relación con el procedimiento que habría que seguir.*
10.5.7	Conviene que el SGRE pueda almacenar, junto con el registro electrónico: • la firma o las firmas electrónicas asociadas a tal registro; • el certificado o los certificados digitales que validen la firma; • cualquier refrendo de verificación añadido por la autoridad de certificación, de tal forma que pueda recuperarse con el registro, y sin menoscabo de la integridad de una clave privada.

10.6 Encriptación

La encriptación es un proceso en virtud del cual se realiza una transformación compleja de un objeto electrónico de modo que éste no puede ser reproducido por

aplicación alguna de manera legible ni comprensible a menos que se lleve a cabo la correspondiente operación inversa. Este proceso se puede realizar para garantizar la seguridad de los objetos electrónicos mediante transformaciones que exigen el uso de códigos electrónicos de seguridad.

Los requisitos detallados en la presente sección sólo son pertinentes cuando existe la necesidad de gestionar registros encriptados.

Ref.	Requisito
10.6.1	Cuando una aplicación de software que interactúe con el SGRE envíe o reciba un registro electrónico en forma encriptada, el SGRE deberá ser capaz de restringir el acceso a dicho registro a los usuarios que consten como portadores de la correspondiente clave de desencriptación, sin perjuicio de cualquier otro tipo de control de acceso asignado a dicho registro
10.6.2	Cuando una aplicación de software que interactúe con el SGRE envíe o reciba un registro electrónico en forma encriptada, conviene que el SGRE conserve como metadatos de ese registro: • el hecho de que se ha realizado una transmisión encriptada • el tipo de algoritmo • el nivel de encriptación aplicado.
10.6.3	Conviene que el SGRE sea capaz de garantizar la captura de registros encriptados directamente desde la aplicación de software que posea tal capacidad, y que limite el acceso a los usuarios que consten como portadores de la clave de desencriptación correspondiente.
10.6.4	Conviene que el SGRE permita eliminar la encriptación cuando se capture o importe el registro. *Tal característica puede resultar necesaria en ciertos archivos de registros de gran tamaño para los que existen requisitos de acceso a largo plazo (debido a que la encriptación y otras características pueden ir en detrimento de la capacidad del sistema de leer registros a largo plazo). En este caso, la organización confiaría en una pista de auditoría o un elemento similar que demostrase que la encriptación o la característica aplicada han estado presentes, pero se han eliminado. En otros casos, esta característica puede resultar inconveniente desde el punto de vista jurídico.* *Para más información sobre la transferencia y la importación, véase 5.3.*
10.6.5	Conviene que el SGRE presente una estructura que permita introducir fácilmente distintas tecnologías de encriptación.

10.7 Filigranas electrónicas y elementos similares

Las filigranas electrónicas se pueden utilizar para marcar una imagen electrónica de forma que quede constancia de su procedencia o de su propiedad. Sobre la

imagen de bits se superpone un patrón complejo, visible o invisible, que sólo se puede eliminar recurriendo a un algoritmo y a una clave de seguridad. En el caso del sonido digital o de las animaciones, se utiliza una tecnología similar. Las filigranas electrónicas se suelen utilizar para proteger la propiedad intelectual.

Los requisitos de esta sección sólo resultan pertinentes cuando existe la necesidad de gestionar registros que porten una filigrana electrónica o cualquier otro tipo de control tecnológico equiparable.

Ref.	Requisito
10.7.1	El SGRE debe ser capaz de almacenar registros dotados de una filigrana electrónica y de conservar con ellos información referente a la filigrana en cuestión.
10.7.2	Conviene que el SGRE sea capaz de recuperar la información almacenada en las filigranas electrónicas.
10.7.3	Conviene que el SGRE presente una estructura que permita introducir fácilmente distintas tecnologías de marcas con filigranas.

10.8 Interfuncionalidad y apertura

Los requisitos detallados en la presente sección son especialmente pertinentes en los entornos en que es preciso establecer una comunicación entre distintos SGRE, como sucede, por ejemplo, en las grandes sociedades o entre distintas entidades estatales.

Ref.	Requisito
10.8.1	Conviene que el SGRE sea capaz de interactuar con otros SGRE.
10.8.2	Conviene que el SGRE sea capaz de actualizar otros sistemas de la empresa.
10.8.3	Conviene que el SGRE sea capaz de interactuar con otras aplicaciones. *La naturaleza de la interfuncionalidad dependerá de la aplicación.*
10.8.4	Conviene que el SGRE sea capaz de procesar transacciones en tiempo real generadas por otros sistemas externos de aplicaciones.

11 REQUISITOS NO FUNCIONALES

Algunos de los atributos propios de un sistema eficaz no se pueden describir en términos de funcionalidad. En la práctica, los requisitos *no funcionales* son primordiales para el éxito de estos sistemas. Si bien los requisitos no funcionales suelen ser difíciles de definir y cuantificar con objetividad, es importante identificarlos para que puedan estudiarse, al menos a alto nivel. Así, algunos de esos requisitos son comunes a numerosas clases de sistemas de TI.

Además, los usuarios de esta especificación tendrán que estudiar sus necesidades en relación con las normas técnicas y funcionales en vigor y con los servicios de asistencia proporcionados por el proveedor del SGRE, incluida la documentación, la formación y la consultoría.

Por otra parte, las organizaciones añadirán sus propios requisitos en tales ámbitos, en función de su tamaño y estructura, sus características físicas y el entorno técnico en el que desarrollen su actividad en ese momento. Esta sección intenta ofrecer una lista de cuestiones que los usuarios deberán tener en cuenta a la hora de establecer sus requisitos, que luego añadirán a los requisitos genéricos descritos en las secciones anteriores.

En algunos de los requisitos que sirven de ejemplo se emplean corchetes agudos (< >) para indicar que el usuario de la especificación debe introducir un valor cuantificado o cualquier otro dato variable según la especificación. Así,

<xx minutos/horas>

significa que el usuario de la especificación tendría que introducir un valor temporal, probablemente medido en minutos u horas, adecuado al requisito específico. De igual modo,

<4 segundos>

indica que el usuario de la especificación debe definir un intervalo de tiempo, y se propone un punto de partida de 4 segundos.

En las diferentes secciones de este capítulo se presentan los requisitos correspondientes a los siguientes ámbitos:

- La facilidad de uso (sección 11.1)
- El rendimiento y la escalabilidad (sección 11.2)
- La disponibilidad del sistema (sección 11.3)
- Las normas técnicas (sección 11.4)
- Los requisitos de carácter normativo y legislativo (sección 11.5)

- La gestión de datos con recurso a contratación externa y a terceros (sección 11.6)
- La conservación a largo plazo y la obsolescencia de la tecnología (sección 11.7).

11.1 Facilidad de uso

La facilidad de uso es una cuestión de especial importancia, pues un SGRE puede fracasar porque sus usuarios no encuentren sencillo su uso.

Los usuarios de la presente especificación deben tomar en consideración la facilidad de uso a la hora de definir un SGRE. Asimismo, han de sopesar el grado de facilidad de uso necesario y cómo ha de especificarse. Ello dependerá de la clase de usuario para el que se haya concebido el SGRE y del grado de formación previsto. A continuación se citan algunos ejemplos de requisitos relativos a la facilidad de uso.

Ref.	**Ejemplo de requisito**
11.1.1	El SGRE debe proporcionar asistencia en línea al usuario en todo momento.
11.1.2	Conviene que la ayuda en línea del SGRE sea sensible al contexto.
11.1.3	Todos los mensajes de error del SGRE deben ser significativos, de forma que los usuarios que probablemente los lean puedan tomar las medidas adecuadas. *Lo más conveniente sería que cada mensaje de error incluyese un texto descriptivo y una indicación de las acciones que el usuario podría efectuar para subsanar dicho error.*
11.1.4	El SGRE debe utilizar un conjunto único, o un pequeño número de conjuntos, de normas de interfaz de usuario. Esas normas deberán ser coherentes con el entorno del sistema operativo en que funcione el SGRE. *Convendría que dichas normas fuesen coherentes con otras aplicaciones ya integradas e instaladas.*
11.1.5	El SGRE debe ser capaz de mostrar varios registros de forma simultánea (salvo requisito contrario derivado de 11.1.4).
11.1.6	Cuando el SGRE recurra a la visualización en pantalla en forma de ventanas, conviene que el usuario pueda configurar cada una de ellas (salvo requisito contrario derivado de 11.1.4).

Ref.	Ejemplo de requisito
11.1.7	La interfaz de usuario del SGRE debe ser adecuada a usuarios con necesidades especiales, esto es, ha de ser compatible con el software especializado que se pueda utilizar y con las orientaciones adecuadas sobre interfaces. *En este contexto, pueden resultar útiles las siguientes directrices, enumeradas en la parte 3 del Anexo 7:* • *Iniciativa SPRITE-S^2 ACCENT: Apoyo y guía en la adquisición de sistemas y servicios de información y de telecomunicaciones.* • *Pautas de Accesibilidad del Contenido en la Web del W3C.* • *Directrices oficiales de Microsoft para desarrolladores y diseñadores de interfaces de usuario.*
11.1.8	El SGRE debe ofrecer al usuario final y al administrador en todo momento funciones de uso fácil e intuitivo de cuya evaluación podría encargarse un grupo de usuarios típicos.
11.1.9	Siempre que el SGRE comprenda la utilización de ventanas, deberá permitir que los usuarios las muevan y que modifiquen su tamaño y su apariencia y que guarden sus modificaciones en un perfil de usuario.
11.1.10	Conviene que el SGRE permita a los usuarios seleccionar el sonido y el volumen de las alarmas sonoras, así como grabar sus modificaciones en un perfil de usuario.
11.1.11	El SGRE debe permitir que, cuando sea conveniente, existan valores por defecto persistentes en la introducción de datos, entre los que convendría que se incluyesen: • Valores definibles por el usuario • Valores idénticos a los del punto anterior • Valores derivados del contexto, como la fecha, la referencia del fichero o el identificador del usuario, según proceda.
11.1.12	Las transacciones más habituales del SGRE se han de diseñar de forma que puedan realizarse con un pequeño número de interacciones (por ejemplo, pulsaciones del ratón).
11.1.13	Conviene que el SGRE se integre estrechamente en el sistema de correo electrónico de la organización, de forma que los usuarios puedan enviar registros y ficheros electrónicos por canales electrónicos sin necesidad de salir del SGRE.
11.1.14	Cuando se satisfaga el requisito 11.1.13, siempre que los usuarios intercambien ficheros y registros conviene que el SGRE envíe, en lugar de copias, referencias a tales elementos. *Pueden existir excepciones, como en el caso de un usuario remoto que no disponga de acceso constante al depósito central.*

Ref.	Ejemplo de requisito
11.1.15	Siempre que el SGRE utilice una interfaz gráfica, deberá permitir que sus usuarios la configuren a su gusto. Conviene que algunos aspectos de la personalización abarquen los elementos siguientes, aunque no tienen por qué limitarse sólo a ellos: • los contenidos de los menús; • la disposición de las pantallas; • la utilización de teclas de funciones; • los colores, las fuentes y el tamaño de las fuentes que se muestran en pantalla; • las alarmas sonoras.
11.1.16	Conviene que el SGRE admita el uso de funciones programadas por el usuario. *Ejemplo: las macros definidas por el usuario (véase la sección 6.3, sobre documentos que se modifican a sí mismos).*
11.1.17	Cuando los usuarios tengan que introducir metadatos de imágenes de documentos impresos, conviene que el SGRE ofrezca funciones que permitan recurrir al reconocimiento óptico de caracteres en la captura de estos elementos (reconocimiento óptico de caracteres por zonas).
11.1.18	Conviene que el SGRE permita a los usuarios definir referencias cruzadas entre registros relacionados que se encuentren en el mismo fichero o en ficheros distintos. Con ello se simplificaría la navegación entre registros.
11.1.19	Conviene que el SGRE incluya una función de ayuda sobre el uso del sistema de clasificación.

11.2 Rendimiento y escalabilidad

Convendría que los usuarios de la presente especificación estudiasen en qué medida el SGRE presenta un tiempo de respuesta breve, acorde a las expectativas del usuario, y es capaz de prestar servicio al intervalo y al tamaño de población de usuarios para el que ha sido concebido. A continuación se exponen ciertas consideraciones y algunos ejemplos de requisitos a tal respecto.

Los tiempos de respuesta dependerán de factores ajenos al SGRE, como:

- la anchura de banda de la red
- la utilización de la red
- la configuración y la utilización de varios recursos del servidor.

En esta especificación no es posible tratar tales factores externos, a los que sólo se hace referencia para señalar que no deben pasarse por alto. Por lo general, para

obtener una estimación fiable del rendimiento es preciso realizar una serie de pruebas en vivo en el propio entorno.

Por consiguiente, conviene interpretar tales requisitos partiendo de una noción común de «tiempo de respuesta», concepto que varía según el entorno, en función del estado de las infraestructuras. Por ejemplo, si el SGRE se está desarrollando para ser integrado en una infraestructura ya existente, puede resultar conveniente especificar los tiempos de respuesta en función del tiempo que transcurre entre la recepción de la pulsación de una tecla en el servidor y el envío de la respuesta; o bien, si la especificación se refiere a un sistema de seguridad que incluya los servidores y la red, puede ser preferible especificar los tiempos de respuesta en función del tiempo transcurrido entre la pulsación de una tecla y la visualización de la respuesta en la estación de trabajo.

Los usuarios de la presente especificación pueden encontrar de utilidad la consulta de la Directiva 90/270/CEE del Consejo, referente a las disposiciones mínimas de seguridad y de salud relativas al trabajo con equipos que incluyen pantallas de visualización, que hace referencia al rendimiento del software.

Ref.	**Ejemplo de requisito**
11.2.1	El SGRE debe ofrecer tiempos de respuesta adecuados para la realización de las funciones habituales en ciertas condiciones normalizadas, como: • con el 75 % de la totalidad de la población prevista de usuarios conectada y activa; • con el 100 % del volumen total previsto de documentos gestionados por el sistema; • con usuarios realizando una combinación de tipos de transacción a distintas velocidades. En estas condiciones, el rendimiento se deberá mantener estable durante un mínimo de diez intentos de transacción.
11.2.2	El SGRE debe ser capaz de realizar una búsqueda sencilla en <3 segundos> y una búsqueda compleja (combinando cuatro términos) en <10 segundos>, con independencia de la capacidad de almacenamiento y el número de ficheros y registros del sistema. *En este contexto, por realización de una búsqueda se entiende la obtención de una lista de resultados, no la recuperación de los registros en sí.*

Ref.	Ejemplo de requisito
11.2.3	El SGRE debe ser capaz de recuperar y mostrar en <4 segundos> la primera página de un registro al que se haya accedido en los últimos <xx> meses, con independencia de la capacidad de almacenamiento y el número de ficheros o registros del sistema. *El objetivo de este requisito es permitir una recuperación rápida de los registros de uso más frecuente, partiendo del principio de que la frecuencia de uso y el uso reciente suelen estar muy correlacionados. La organización deberá introducir la escala temporal tras evaluar a partir de qué intervalo disminuye el uso intensivo de los registros.*
11.2.4	El SGRE debe ser capaz de recuperar y mostrar en <20 segundos> la primera página de un registro al que no se haya accedido en los últimos <xx> meses, con independencia de la capacidad de almacenamiento y el número de ficheros o registros del sistema. *El objetivo de este requisito es permitir que, en los casos en que se recurra a una gestión del almacenamiento jerárquica, los registros de uso menos frecuente se almacenen en soportes más lentos que los de consulta más habitual. La organización deberá introducir la escala temporal tras evaluar a partir de qué intervalo disminuye el uso intensivo de los registros.*
11.2.5	El SGRE debe permitir que una sola implementación del sistema disponga de un almacén de registros electrónicos de al menos <xx gigabytes/terabytes> o <xx miles/millones> de registros y que preste servicio al menos a <xx cientos/miles> de usuarios de forma simultánea. *La organización deberá introducir sus estimaciones sobre la población de usuarios y el volumen de registros.*
11.2.6	Debe resultar posible la expansión controlada del SGRE hasta al menos <xx cientos/miles> de usuarios, sin menoscabo de la continuidad y la eficacia del servicio.
11.2.7	El SGRE debe admitir todo lo indicado anteriormente y permitir el mantenimiento de rutina de: • los datos relativos a los usuarios y grupos de usuarios • los perfiles de acceso • los sistemas de clasificación • las bases de datos • los calendarios de conservación teniendo en cuenta los niveles previstos de transformación estructural y sin imponer gastos excesivos de administración de cuentas/sistemas (véase también el capítulo 9). *Cuando los requisitos del rendimiento sean estrictos, puede resultar necesario cuantificar el grado de transformación estructural previsto.*

Ref.	Ejemplo de requisito
11.2.8	El SGRE debe ser escalable y no presentar ninguna característica que impida su uso en organizaciones de pequeño o gran tamaño, con un número variable de unidades estructurales de distinto tamaño.

11.3 Disponibilidad del sistema

En muchos entornos, la utilización conjunta de un SGRE y un EDMS transformará el uso de los sistemas informáticos. Un cambio fundamental lo constituirá el aumento espectacular de la dependencia de los usuarios con respecto a la red de TI, de modo que si los sistemas de gestión de registros y documentos electrónicos dejan de estar disponibles, a los usuarios les será imposible continuar su trabajo. Por consiguiente, convendría que los usuarios de esta especificación que estén contratando un sistema identifiquen los requisitos de disponibilidad de los usuarios y que los detallen en el momento de la contratación. A continuación se enumeran algunos ejemplos de requisitos relativos al mantenimiento.

Ref.	Ejemplo de requisito
11.3.1	El SGRE debe estar a disposición de los usuarios: • de <xx:00> a <xx:00> • <todos los días de la semana/xxx días al año>.
11.3.2	El período de inactividad previsto del SGRE no debe superar las <xx> horas <cada trimestre>. *La definición de «inactividad» puede variar según la infraestructura y la arquitectura. Así, en ciertos entornos un fallo del hardware del servidor se considerará un fallo del SGRE, mientras que en otros el fallo del hardware principal se clasificará en otra categoría. Conviene acordar una definición adecuada, y como punto de partida proponemos la siguiente: «Se considera que el SGRE está inactivo cuando los usuarios no pueden utilizar ninguna función normal del sistema, siempre que el fallo sea atribuible a cualquier componente del SGRE excepto a la estación de trabajo».*
11.3.3	El tiempo de inactividad no previsible del SGRE no debe superar las <xx horas/minutos > por <trimestre>.
11.3.4	El número de incidentes de períodos de inactividad imprevista del SGRE no debe ser superior a <x> por <trimestre>.
11.3.5	Cuando se produzca un fallo del software o del hardware, debe resultar posible devolver el SGRE a un estado conocido (más reciente que la copia de seguridad del día anterior) en menos de <xx> horas de trabajo con el hardware disponible.

11.4 Normas técnicas

Conviene que el SGRE cumpla las normas de hecho y de derecho. Cuando sea posible, conviene que el SGRE recurra a formatos y especificaciones abiertos, no propietarios.

Los usuarios de esta especificación tendrán que establecer los requisitos de las normas relativas a los siguientes aspectos:

- el entorno de hardware, como las plataformas del servidor y los entornos de las estaciones de trabajo;
- el sistema operativo, ya sea Windows de Microsoft, en sus versiones 98, NT4 o 2000, o bien MacOS o Unix;
- las normas industriales de la interfaz de usuario, ya se trate de Windows, de Microsoft, de X-Windows de Macintosh o de un navegador de intranet;
- la base de datos relacional, que podría ser de tipo ODBC, OLE DB o quizás un producto comercial, como Oracle o Sybase;
- los protocolos de la red y el sistema operativo, como TCP/IP, de clase Ethernet y Novell, Microsoft Windows NT Server;
- la codificación a distintos niveles, como ASCII, Unicode ISO 10646, ISO 8859, Adobe PDF o cualquier otra especificación propietaria equivalente;
- las normas de intercambio, como XML, HTML y SGML;
- los kits de desarrollo y las interfaces de los programas de aplicaciones, como COM, DCOM y CORBA.

Cuando se utilice esta especificación en contratación externa, se tendrán que añadir detalles adicionales sobre el entorno técnico, incluidas todas las interfaces del SGRE, como los sistemas antiguos o de oficina, y cualquier previsión de cambio.

Además, en función de sus circunstancias concretas, los usuarios de la presente especificación tendrán que considerar sus requisitos en los siguientes ámbitos normativos:

Ref.	Ejemplo de requisito
11.4.1	Cuando el SGRE vaya acompañado de un tesauro monolingüe, conviene que éste cumpla la norma ISO 2788, Directrices para el establecimiento y desarrollo de tesauros monolingües.
11.4.2	Cuando el SGRE vaya acompañado de un tesauro, conviene que éste cumpla la norma ISO 5964, Directrices para la creación y desarrollo de tesauros multilingües.

Ref.	Ejemplo de requisito
11.4.3	Cuando el sistema de gestión de registros electrónicos permita el escaneado de documentos en papel, convendría que se respetasen las siguientes normas: • Normas TWAIN o Isis en materia de interfaces de escáner. • El formato de imagen TIFF v6 con compresión de facsímil de Grupo IV en las imágenes de dos niveles. • Los formatos JPEG, PNG, GIF o cualquier otro seleccionado por el usuario, si se admiten imágenes en color o en escala de grises. *Si estas normas no se respetan, habrá que argumentar una razón adecuada.*
11.4.4	El SGRE debe permitir el almacenamiento de los registros utilizando formatos y codificación de ficheros que constituyan normas de derecho o estén bien documentados.
11.4.5	Conviene que el SGRE se atenga a las normas en materia de búsqueda, recuperación e intercambio de información, incluida la ISO 23950, Recuperación de información - Definición de servicio de aplicaciones y especificación de protocolos). *Esta norma también se denomina ANSI Z39.50.*
11.4.6	Cuando el SGRE utilice una base de datos relacional, deberá conformarse a la norma SQL, norma, ISO/IEC 9075, Tecnología de la información - Lenguajes de bases de datos - SQL.
11.4.7	Conviene que el SGRE almacene todas las fechas en un formato compatible con la norma ISO 8601, Elementos de datos y formatos de intercambio - Intercambio de información - Representación de fechas y horas.
11.4.8	Conviene que el SGRE registre todos los nombres de países en un formato que cumpla la norma ISO 3166, Códigos para la representación de los nombres de los países.
11.4.9	Conviene que el SGRE almacene todos los nombres de idiomas en un formato que cumpla la norma ISO 639, Códigos para la representación de los nombres de lenguas.
11.4.10	Cuando el SGRE gestione registros en múltiples idiomas o utilice caracteres no ingleses, deberá ser capaz de manejar la codificación ISO 8859-1.
11.4.11	Cuando el SGRE gestione registros en múltiples idiomas o utilice caracteres no ingleses, deberá poder manejar la codificación ISO 10646 (Unicode).

11.5 Requisitos de carácter normativo y legislativo

El SGRE debe atenerse a requisitos de carácter legislativo y normativo que por lo general varían según la región y la industria de que se trate.

Nótese que en esta especificación no se aborda la necesidad de mantener registros físicos. La existencia de tal necesidad dependerá del entorno legislativo y

normativo. Cuando exista, habrá que procurar conservar la integridad y la posibilidad de utilizar la totalidad de los registros físicos y electrónicos. De tales cuestiones tendrían que ocuparse las políticas de organización pertinentes.

Los siguientes requisitos tendrán que adaptarse según el emplazamiento.

Ref.	Ejemplo de requisito
11.5.1	El SGRE debe atenerse a las normas relativas al efecto 2000 y procesar correctamente todas las fechas. *Ciertos SGRE tienen que procesar fechas que abarcan un intervalo de siglos. El tratamiento correcto de todas ellas puede incluir fechas en distintos siglos. En el Anexo 6 se muestra un ejemplo de declaración en la que se especifica esta cuestión con mayor profundidad.*
11.5.2	El SGRE debe cumplir las normas existentes a escala local en materia de admisibilidad jurídica y de fuerza probatoria de los registros electrónicos.
11.5.3	El SGRE ha de atenerse a cualquier legislación en materia de gestión de registros aplicable a escala local.
11.5.4	El SGRE no debe incluir ninguna característica incompatible con la legislación en materia de protección de datos o de otro tipo.
11.5.5	El SGRE debe cumplir las exigencias normativas de <cualesquiera requisitos normativos o códigos de conducta de carácter local, nacional o europeo aplicables a la industria, la función empresarial o el sector público>. *Este requisito tendrá que adaptarse a cada entorno.*

11.6 Gestión de datos con recurso a servicios externos y a terceros

Numerosas organizaciones se dirigen a proveedores de servicios cuando se trata de almacenar y gestionar los registros que ya no están en activo o que se solicitan muy de tarde en tarde, pero que es preciso conservar durante un tiempo estipulado por la ley, ya porque lo exija una norma jurídica o estatal o los reguladores de la industria, ya por razones derivadas de la conservación a largo plazo.

Además, cada vez se recurre más a los proveedores de servicios de aplicaciones, tanto en la gestión de registros activos como en su archivo. Las organizaciones envían sus documentos o registros (facturas, correspondencia con los clientes, documentación relacionada con la solicitud de hipotecas, etc.) al proveedor de servicios de aplicaciones para que éste los clasifique y almacene. Posteriormente, el personal de la organización puede visualizar los documentos desde Internet o desde una red de área extensa.

La gestión de registros electrónicos por terceros exige que en el contrato con el proveedor del servicio se hayan definido con exactitud los procedimientos y controles en vigor dirigidos al cumplimiento de las normas existentes, al respeto de las buenas prácticas precisas para la admisibilidad jurídica de los registros

electrónicos y a la satisfacción de las exigencias empresariales de los clientes en lo referente al acceso y la disponibilidad.

El contrato habrá de incluir disposiciones destinadas a que:

- la gestión del proveedor del servicio se mantenga a un nivel mínimo equiparable al de la gestión de los registros internos del propio cliente;
- en el futuro, el cliente pueda recuperar los registros del proveedor del servicio y aun así continuar con la gestión de los registros conforme a las normas de la organización y de forma que se cumplan los criterios de admisibilidad jurídica.

Esta subsección se basa en gran parte en el código PD 0008 (véase la sección 4.14, «Utilización de servicios contratados», de la referencia [5] del Anexo 1).

Ref.	Requisito
11.6.1	Se debe establecer con el proveedor del servicio un contrato en el que se detallen los servicios que se vayan a utilizar.
11.6.2	Se deberán documentar los pormenores de los procedimientos de transferencia de registros del cliente al proveedor de servicios y de éste al cliente. *Se podrían utilizar vías de comunicación entre los emplazamientos y transferir ficheros y registros a diario o a intervalos regulares. El cliente deberá aprobar el grado de seguridad del canal de comunicación entre los dos sitios, y tendrán que existir protocolos que verifiquen la correcta recepción de todos los ficheros y la elaboración de informes al respecto.*
11.6.3	El proveedor de servicios debe ser capaz de proporcionar al cliente copias de la pista de auditoría de los procesos de seguimiento y almacenamiento de los registros y ficheros.
11.6.4	El proveedor de servicios deberá demostrar que dispone de mecanismos que permitan la fácil transferencia de los registros, ficheros y metadatos almacenados de vuelta al SGRE del cliente, sin que se produzca pérdida alguna en la estructura o el contenido de los registros. Además, el proveedor del servicio deberá haber implantado mecanismos que permitan al cliente transferir ficheros y registros de forma individual.
11.6.5	El proveedor del servicio deberá ser capaz de permitir un acceso rápido del cliente a los registros de cuya gestión está encargado. El proveedor deberá proporcionar al cliente una visualización del registro o el propio registro original en el tiempo y el precio pactados.
11.6.6	Conviene que el proveedor del servicio sea capaz de permitir al cliente solicitar, visualizar e imprimir registros y ficheros desde sus propias oficinas. *Esto se puede conseguir, por ejemplo, por medio de una conexión en red.*
11.6.7	Conviene que el proveedor del servicio sea capaz de permitir al cliente solicitar en línea la descarga o la transmisión de registros o ficheros entre su SGRE y el dispositivo de almacenamiento del proveedor del servicio.

Ref.	Requisito
11.6.8	Conviene que el cliente sea capaz de solicitar informes sobre los registros que conserve el proveedor del servicio, así como información sobre sus calendarios de conservación, etc. Convendría que el cliente pudiera acceder en línea a este instrumento desde sus propias oficinas.
11.6.9	Conviene que los servicios especificados en los requisitos 11.6.6, 11.6.7 y 11.6.8 : • se presten en el tiempo de respuesta o de tramitación establecido en el contrato; • se desarrollen en entornos seguros.
11.6.10	Conviene que el cliente compruebe que la ubicación del trabajo propuesta es aceptable y cumple los criterios de seguridad adecuados a las necesidades del cliente.
11.6.11	Conviene que el cliente verifique que los procedimientos y procesos de almacenamiento propuestos no suponen para los registros un riesgo mayor que los suyos propios. *El proveedor del servicio tendrá que demostrar que existe una copia de seguridad de todos los registros del cliente y que, en caso de producirse una pérdida de los registros, se podrían recuperar en un intervalo de tiempo pactado en el contrato.*
11.6.12	Cuando la seguridad de los registros sea una cuestión vital, conviene que el cliente compruebe que el proveedor del servicio responde de la integridad de su personal. *Constituye una ventaja que todos los empleados del proveedor de servicios firmen un contrato de confidencialidad como parte de sus condiciones de trabajo.*
11.6.13	Convendría que el envío de registros desde o hasta el cliente o el proveedor de servicios fuese acompañado de un documento de control en el que se consigne la identidad y el número de registros y ficheros.
11.6.14	Conviene que los terceros encargados de los servicios de transporte demuestren cumplir los criterios de calidad y fiabilidad del cliente.

11.7 Conservación a largo plazo y tecnología obsoleta

Esta sección se ocupa de la conservación a largo plazo. El concepto «a largo plazo» no se define con precisión, pero en este documento se refiere a un período de tiempo superior a diez años o similar. En una organización, el período de conservación se debería fijar en función de las exigencias legislativas y de la propia actividad. En ciertos entornos tal período abarcará varios decenios, mientras que en algunos archivos podría llegar a siglos. En cualquier caso, el intervalo de tiempo

será lo bastante prolongado como para que los enfoques habitualmente adoptados en períodos más cortos pierdan su pertinencia.

El mantenimiento a largo plazo de los registros electrónicos entraña una serie de riesgos debidos a tres causas:

- La degradación de los soportes
- La obsolescencia del hardware
- La obsolescencia de los formatos.

Estas cuestiones se discuten más adelante, para luego continuar con la exposición de los requisitos específicos. No obstante, los lectores de este documento han de percatarse de que la presente especificación no propone unos requisitos exhaustivos en relación con todas las facetas de esta cuestión. Por consiguiente, corresponde a cada organización desarrollar y poner en práctica una estrategia de conservación a largo plazo de sus registros electrónicos, tal y como se suele hacer con los registros en papel.

En la exposición que sigue, la conservación de los registros conlleva la de los metadatos y la pista de auditoría que los acompañan.

Degradación de los soportes

Los riesgos debidos a la degradación de los soportes obedecen a la vida limitada de todos los medios de almacenamiento digital. Su ciclo de vida varía según el soporte y las condiciones de almacenamiento (temperatura, humedad e índices de variación). A medida que los soportes alcanzan o superan su esperanza de vida, la posibilidad de que surjan errores en la lectura (esto es, bits con una lectura incorrecta) aumenta de una manera espectacular. La mayor parte del hardware de almacenamiento cuenta con una herramienta de corrección automática de errores que puede hacer frente a cierto nivel de errores de bit y compensarlos de forma eficaz. Sin embargo, en algunos casos los errores de lectura se multiplican tanto que la herramienta de corrección automática ya no puede solventarlos, con lo que los registros se corrompen de manera irreversible. Las consecuencias de la corrupción dependen de numerosos factores, pero pueden convertir en ilegibles únicamente los registros o bien las cintas o discos en su totalidad.

Para prevenir la pérdida de información debido a la degradación de los soportes se pueden tomar las siguientes precauciones:

- Comprobar que todos los soportes se almacenan, utilizan y manejan en un entorno que se encuentra en condiciones idóneas. Como norma general, cuanto más limpio, frío, seco y estable sea un entorno, tanto más larga será la esperanza de vida. No obstante, cuando se trate de soportes especiales, convendrá seguir las indicaciones del fabricante y procurar que la temperatura ambiente no descienda por debajo de un valor determinado, así como limpiar, o no, los soportes a intervalos regulares.

- Sustituir rutinariamente los soportes antes del término de su ciclo de vida previsto (copiando la información en nuevos soportes).

- Mantener varias copias de cada registro y compararlas sistemáticamente conforme a un calendario. A continuación, sustituir cualquier copia de registro o de fragmento de soporte en los que exista algún error irrecuperable. Este enfoque se suele utilizar en los archivos especializados con perspectivas a largo plazo y exige la utilización de sistemas automatizados y hardware de recuperación, cuya descripción escapa al alcance de la presente especificación.

Obsolescencia del hardware

Los periféricos de almacenamiento, como las unidades de cinta o de disco, tienen una vida comercial limitada. Una vez la superan suelen precisar un mayor mantenimiento que, al igual que la reparación, se encarece cada vez más. Al final, su reparación resulta imposible por motivos de tipo práctico. En ocasiones se puede llegar a un acuerdo para compartir los equipos con usuarios de equipos similares o compatibles, pero esta solución no resulta viable de manera indefinida. Llegará un momento en que la información almacenada en dispositivos obsoletos que no se haya trasladado a otros soportes pueda perderse debido a un fallo del dispositivo.

Los ordenadores que gestionan las aplicaciones y el almacenamiento presentan los mismos problemas.

Es evidente que para eludir tales riesgos habrá que adoptar una estrategia basada en la supervisión del estado del hardware y en la migración de la información a soportes nuevos y actuales antes de que la obsolescencia pueda afectarle. En todo caso, conviene escoger los soportes y el hardware tomando en consideración su esperanza de vida. Dicho de otro modo, puede resultar más acertado decantarse por productos más populares o por los «líderes del mercado» que por dispositivos más recientes o punteros.

Obsolescencia del formato

La obsolescencia de los formatos es la cuestión que plantea mayores dificultades en períodos de tiempo superiores a un par de decenios.

El problema radica en la continua evolución de la mayoría de los componentes de software presentes en la «cadena» de transformación entre el soporte y la información visualizada. Tales componentes incluyen:

- Las normas de codificación

- Los formatos de fichero

- El software de aplicaciones

- El software de las bases de datos y de otras herramientas

- El software del sistema operativo.

La evolución de estos elementos es rápida y cada componente se transforma de diferente modo y a un ritmo distinto. En ciertos casos la evolución mantiene la compatibilidad con los formatos anteriores, pero no siempre es así, tal y como viene sucediendo, en especial, en períodos superiores a un par de decenios. No resulta factible evitar la evolución «congelando» la configuración, pues la necesidad de migrar a un hardware actual, ya descrita, entraña con frecuencia la obligación de utilizar nuevos controladores de software, que a su vez exigen un nuevo sistema operativo, etc.

En la actualidad se admiten los siguientes procedimientos:

- La migración, esto es, la conversión a nuevos formatos que puedan utilizar el hardware y el software actuales.

- La emulación, que es el traslado de la información a un nuevo hardware dotado de un componente de software adicional que emule el hardware antiguo y permita la ejecución de la antigua aplicación de software.

- La conservación de la tecnología, es decir, el constante mantenimiento del hardware original. Esta solución no resulta viable a largo plazo.

- La vinculación de los datos al software, enfoque teórico que en el momento de elaborar el presente documento aún estaba en fase de investigación. Para más información véase BS 7978 en la parte 1 del Anexo 7.

Si bien son muchas las investigaciones que en la actualidad se ocupan de identificar procedimientos que reduzcan los riesgos, en el momento de elaborar esta especificación aún no existía un método sencillo y genérico que garantizase el acceso a largo plazo a los registros electrónicos. En términos generales, se coincide en afirmar que la migración y la emulación son, con toda probabilidad, los métodos más fiables; no obstante, en la práctica ambos sistemas exigen ciertas precauciones para la conservación de los metadatos, como se explica a continuación.

Sin embargo, las migraciones a gran escala rara vez transcurren sin ningún tipo de problemas, pues pueden conllevar pérdidas de funcionalidad, detalles, etc.

Por otra parte, no se posee una comprensión plena del proceso de emulación a largo plazo, que también entraña riesgos de pérdida de funcionalidad y otras características.

Estas dificultades se multiplican ante la posibilidad de reiteradas migraciones o emulaciones. Nadie puede prever la naturaleza de las migraciones o emulaciones que pueden resultar necesarias, y tampoco se pueden anticipar las consecuencias de varias migraciones o de varias «capas» de emulaciones.

La estrategia más acertada consiste en conservar la información sólo en formatos abiertos que gocen de la aceptación general, esto es, sobre los cuales exista una documentación exhaustiva en especificaciones públicas. Como sucedía con el

hardware, esto lleva a preferir los «productos líderes del mercado» a los punteros o los pendientes de prueba. También conviene evitar los formatos propios cuyas especificaciones no sean públicas. Además, de todo esto se deduce que la organización deberá recurrir a expertos para seleccionar los formatos.

Debido a la volatilidad del mercado multimedios y de los formatos propios que utiliza, éste ámbito suscita una especial inquietud.

En vista de que este problema exige una respuesta específica en cada organización, no serviría de nada continuar comentándolo en este documento desde un punto de vista general. No obstante, conviene señalar que todos los enfoques suponen un gasto, en hardware, en software, en la preparación y conversión de datos y en su gestión, pese a lo cual ningún método garantiza el acceso sin la aplicación de una estrategia de conservación a largo plazo antes de que la accesibilidad pase a convertirse en un problema. Dicho de otro modo, la conservación a largo plazo exige que, como medida preventiva, se realicen inversiones que pueden llegar a adquirir un tamaño respetable, del mismo modo que sucede con la conservación de los archivos en papel, con la diferencia de que en ciertos casos el gasto será mayor. Por lo tanto, siempre que sea precisa una conservación a largo plazo, los directivos principales de la empresa tendrán que comprometerse con los esfuerzos y los gastos en curso, necesarios para salvaguardar el acceso. En la parte 4 del Anexo 7 se presentan otras fuentes de información.

Metadatos de conservación

Una cuestión esencial es que, cuando sea necesario un almacenamiento a largo plazo, los metadatos de conservación se almacenen con los registros. Estos metadatos proporcionan más información que la descrita en la presente especificación, como datos sobre el entorno técnico y sobre el software empleado en la creación de un registro o el necesario para representarlo, así como sobre todos sus componentes. Si el período de conservación es indefinido, el número de elementos de los metadatos tendrá que ser considerable. En el momento de elaborar el presente informe existían en Europa, Norteamérica y Australia varios proyectos de investigación dedicados al desarrollo de marcos de metadatos, cuyos resultados se están publicando en Internet. La complejidad de los metadatos de conservación ha llevado al desarrollo del modelo de referencia OAIS (véase la parte 4 del Anexo 7), que se puede utilizar en la organización de los metadatos con vistas a su posterior conservación.

Requisitos específicos

Siempre que se contemple la posibilidad del almacenamiento a largo plazo, los requisitos expuestos en la presente sección se han de entender como exigencias técnicas mínimas. Sin embargo, como ya se ha indicado, en esta cuestión el compromiso de la dirección de la organización es igualmente importante.

Ref.	Requisito
11.7.1	El medio de almacenamiento del SGRE debe ser utilizado y conservado en entornos compatibles con la esperanza de vida prevista o deseada y correspondiente a los valores indicados en la especificación del fabricante del soporte. *En ciertos casos se puede citar una norma como la BS 4783 (véase la parte 1 del Anexo 7).*
11.7.2	Como procedimiento preventivo frente a la degradación de los soportes, conviene que el SGRE cuente con funciones que permitan comparar automáticamente, a intervalos regulares, copias de información, así como sustituir cualquier copia defectuosa.
11.7.3	El SGRE debe permitir la conversión en masa de los registros, con sus metadatos y pista de auditoría, a otros soportes o sistemas en línea que admitan las normas correspondientes al formato o los formatos en uso.
11.7.4	El proveedor del SGRE debe haber instalado un programa verificable de actualización de la tecnología básica del sistema que permita acceder a la información existente sin que existan cambios en el contenido.
11.7.5	Conviene que el SGRE sólo utilice normas que gocen de aceptación general y con especificaciones abiertas y de dominio público en materia de codificación, almacenamiento y estructuras de bases de datos.
11.7.6	Cuando el SGRE utilice sistemas propietarios de codificación, almacenamiento o bases de datos, éstos tendrán que estar bien documentados y el administrador deberá poder acceder a tal documentación. *Nótese que puede no bastar con que el proveedor conserve una copia de la documentación, pues en el marco temporal que se maneja no existe certeza alguna de la estabilidad del proveedor. Por lo tanto, puede resultar conveniente que el usuario o una tercera parte neutral conserven una copia de esta documentación.*
11.7.7	Conviene que el SGRE sea capaz de gestionar la conservación de una serie de elementos de los metadatos de los registros y de los componentes de éstos. *Véase 12.7.13.*

12 REQUISITOS DE LOS METADATOS

En el presente documento, el concepto de metadatos abarca los datos empleados en la indexación, además de otros, como la información referente a la restricción del acceso. En la sección 13.1 se ofrece una definición formal del concepto.

La disposición de este capítulo difiere de la adoptada en los anteriores. A tal respecto, véase la sección 12.2.

12.1 Principios

No resulta factible definir todos los requisitos de los metadatos en relación con todos los SGRE que pueden existir en la práctica. Cada tipo de organización y de aplicación presenta unas necesidades y tradiciones propias que pueden variar enormemente, Así, ciertas organizaciones precisarán una indexación basada en las denominaciones de las cuentas y las fechas de transacción, mientras que otras recurrirán a una numeración estrictamente jerárquica; algunas entidades deberán definir volúmenes en función de los ejercicios presupuestarios, mientras que en otras será más importante centrarse en los controles de acceso, ya sea por razones de seguridad, ya por motivos relacionados con la propiedad intelectual, etc.

Por consiguiente, este capítulo se limita a sugerir unos requisitos mínimos de carácter genérico que luego se podrán personalizar. Entre ellos se incluye una lista de ciertos elementos concretos de los metadatos que el SGRE ha de poder capturar y procesar.

Casi cualquier posible SGRE puede configurarse con los campos suficientes para admitir los elementos de los metadatos enumerados a continuación. Sin embargo no basta con ello, pues también es fundamental que:

- el SGRE utilice elementos de metadatos que admitan y den soporte a la funcionalidad definida en el resto de la presente especificación (véase 12.1.2);
- el SGRE incluya características que permitan aplicar normas de validación, transmisión y determinación de valores por defecto en el momento de la captura de los elementos de los metadatos.

Ref.	Requisito
12.1.1	La aplicación del SGRE no debe imponer limitación práctica alguna sobre el número de elementos de metadatos permitidos en cada caso (por ejemplo, fichero, volumen, registro). *La definición de «limitación práctica» varía según la aplicación. Así, una organización de pequeño tamaño con un sistema de clasificación restringido puede no precisar tantos elementos de metadatos como una organización grande con un sistema de clasificación más amplio.*

Ref.	Requisito
12.1.2	Cuando el contenido de un elemento de un metadato pueda tener alguna influencia en el comportamiento de las funciones del SGRE, éste debe hacer uso del contenido de ese elemento para determinar la funcionalidad. *Así, si el SGRE almacena las categorías de seguridad de los registros y también las habilitaciones de seguridad de los usuarios, debe consultar estas últimas antes de conceder o denegar a un usuario el acceso a un registro. Sin embargo, este requisito se pasa por alto cuando el SGRE sólo almacena las habilitaciones y categorías como campos textuales que no intervienen en el control del acceso.* *Obsérvese que se trata de un requisito de carácter general que atañe a gran número de elementos de metadatos. Esta especificación no pretende identificar todos los casos en que procede su aplicación.*
12.1.3	En el momento de la configuración, el SGRE debe permitir que se definan varios conjuntos de elementos de metadatos adecuados a las distintas clases de registros electrónicos. *Por ejemplo, los registros consistentes en imágenes escaneadas tendrán que contar con metadatos referentes a los procesos de escaneado e indexación, mientras que las facturas precisarán metadatos referentes a los números de cuentas, y la correspondencia necesitará campos de metadatos con múltiples valores relativos a los destinatarios.*
12.1.4	El SGRE deberá permitir que el administrador decida, en el momento de la configuración, cuáles de los elementos de los metadatos son obligatorios y cuáles son facultativos, así como los que podrán ser objeto de búsqueda.
12.1.5	Cuando menos, el SGRE debe admitir los siguientes formatos de elementos de metadatos: • Alfabético • Alfanumérico • Numérico • De fecha • Lógico (esto es, SÍ/NO, VERDADERO/FALSO).
12.1.6	Conviene que el SGRE admita formatos de elementos de metadatos definidos por el administrador creados a partir de la combinación de los formatos enumerados en 12.1.5. *Por ejemplo, una aplicación podría presentar un número de referencia con el formato nnnnn/aa-n.*
12.1.7	El SGRE debe admitir todos los formatos de fecha definidos en la norma ISO 8601.

Ref.	Requisito
12.1.8	En el momento de la configuración, el SGRE debe permitir que se defina la procedencia de los datos de cada elemento de un metadato. *En los requisitos 12.1.9, 12.1.10, 12.1.11, 12.1.12 se describen las posibles fuentes.*
12.1.9	El SGRE debe permitir la extracción automática de elementos de los metadatos de los registros en el momento de su captura. *En ciertas aplicaciones, éste podría ser un requisito no obligatorio; sin embargo, se considera preceptivo en la presente especificación, debido a la especial importancia que presenta en numerosas ocasiones. Algunos ejemplos podrían ser la extracción automática de las fechas, los nombres de los destinatarios y los números de referencia de los documentos creados en un procesador de textos o que reflejan una transacción estructurada, como sucede con las facturas.*
12.1.10	El SGRE debe permitir que el administrador decida qué elementos de los metadatos se pueden introducir y mantener mediante la entrada de datos desde el teclado y cuáles se escogerán de una lista desplegable
12.1.11	Conviene que el SGRE permita la asignación automática de los valores de los metadatos desde el siguiente nivel de la jerarquía del sistema de clasificación. *Por ejemplo, cuando se trata de un volumen, el valor de ciertos elementos de los metadatos debe proceder de su fichero raíz, mientras que cuando hablamos de un registro puede que el valor de alguno de los metadatos venga determinado por el del volumen en que se almacena.*
12.1.12	Conviene que el SGRE permita obtener los valores de los metadatos a partir de tablas de referencias o de llamadas a otras aplicaciones de software. *Por ejemplo, el SGRE podría dirigir el nombre y el código postal a una aplicación de direcciones, que a su vez, devolvería el nombre de una calle que se utilizaría como metadato.*

Ref.	Requisito
12.1.13	El SGRE debe permitir la validación de los metadatos cuando los usuarios se encargan de su introducción o bien cuando se importan. Dicha validación deberá emplear, como mínimo, los siguientes mecanismos: • El formato del contenido del elemento. • El intervalo de valores. • La validación frente a una lista de valores mantenida por el administrador. • La referencia a un sistema de clasificación válido. *Un ejemplo de una validación de formato sería la comprobación de que todo su contenido es de carácter numérico o tiene formato de fecha (de conformidad con 12.1.5).* *Un ejemplo de validación de un intervalo de formato es la comprobación de que el contenido queda dentro del intervalo comprendido entre el 1 de enero de 1999 y el 31 de diciembre de 2001.* *Un ejemplo de validación frente a una lista de valores es la verificación de la existencia de un destino de exportación en una lista.*
12.1.14	Conviene que el SGRE permita validar los elementos de los metadatos mediante algoritmos de verificación de dígitos. *Por ejemplo, los ficheros se pueden identificar con el número de una tarjeta de crédito de dieciséis dígitos, el último de los cuales será un dígito de control calculado a partir de los otros quince con un algoritmo módulo 10.* *Por lo general se considera aceptable dotar al programa de una interfaz que permitirá a las organizaciones la introducción del algoritmo seleccionado.*
12.1.15	Siempre que sea necesario, el SGRE deberá permitir la validación de los metadatos mediante llamadas a otras aplicaciones (por ejemplo, a un sistema de personal, con objeto de comprobar si ya se ha asignado un número de empleado, o bien a un sistema de base de datos de códigos postales).
12.1.16	Siempre que la introducción de los valores de los elementos de los metadatos se haga de forma manual, el SGRE deberá permitir la existencia de valores persistentes por defecto definidos por el usuario. *Un valor persistente por defecto es el que aparece cada vez que se introduce un elemento en el campo de entrada hasta que lo modifica un usuario. Una vez modificado, el nuevo valor se mantiene, esto es, pasa a ser persistente.*
12.1.17	Conviene que el SGRE admita una configuración tal que cualquier elemento de un metadato se pueda utilizar como campo en una búsqueda no estructurada (por ejemplo, una búsqueda de texto libre).

Ref.	Requisito
12.1.18	Siempre que un elemento de un metadato se almacene en formato de fecha, conviene que el SGRE permita realizar búsquedas que reconozcan el valor de la fecha. *Por ejemplo, conviene que el SGRE permita realizar búsquedas en un intervalo de fechas. No basta con almacenar una fecha como campo textual.*
12.1.19	Siempre que un elemento de un metadato se almacene en formato numérico, conviene que el SGRE permita realizar búsquedas que reconozcan el valor del número.
12.1.20	El SGRE debe restringir la capacidad de realizar modificaciones en los valores de los metadatos, tal y como se define en la matriz de la sección 13.4.
12.1.21	El SGRE debe permitir que se redefinan los conjuntos de metadatos establecidos por el administrador y debe consignar los cambios en la pista de auditoría. *Por ejemplo, tras un cambio en la organización puede resultar necesario añadir un nuevo elemento de dato, como «identificador de departamento», a ciertos tipos de documentos.*
12.1.22	Conviene que el SGRE pueda adquirir metadatos creados por: • el paquete de aplicaciones de creación de documentos, el sistema operativo o el software de red; • el usuario, en el momento de la captura o la declaración; • las normas definidas en el momento de la configuración sobre la generación de metadatos por parte del SGRE cuando se produce una declaración.
12.1.23	El SGRE debe ser capaz de impedir cualquier modificación de los metadatos generada directamente por otros paquetes de aplicaciones, el sistema operativo o el SGRE, como los datos transmitidos por correo electrónico.
12.1.24	El SGRE debe impedir que se modifique el contenido de ciertos campos de metadatos especificados en el momento de la configuración.

12.2 Disposición del resto de este capítulo

En el resto del presente capítulo se procede a la enumeración de elementos genéricos de metadatos funcionales en relación con cada nivel de la jerarquía de ficheros:

- El sistema de clasificación
- Los ficheros
- Los volúmenes de los ficheros

- Los registros.

El formato de las listas de los requisitos de los metadatos difiere del que presentan las tablas de los otros capítulos. Tal y como se hacía hasta ahora, se disponen en columnas con los epígrafes que se indican a continuación:

Ref.

El número de referencia de un requisito.

Elementos de los metadatos

La capacidad del SGRE de incluir cada elemento de un metadato se muestra como un requisito.

Todos los requisitos comenzarán con la frase «El SGRE debe ...» o «Conviene que el SGRE ...». Igual que en el resto de la especificación, el verbo «deber» indica un requisito obligatorio y el verbo «convenir» un requisito facultativo.

En aras de una mayor simplicidad, en las listas no constan los valores transmitidos desde los niveles más altos de la jerarquía. Por ejemplo, aunque ciertos metadatos como el nombre y el número de referencia se trasmitan de forma natural de los ficheros raíz a los volúmenes de los ficheros, tales datos no aparecerán en la presente especificación.

Incidencia

El requisito precisa, para cada elemento, el número de veces que el SGRE debe permitir que aparezca ese elemento. En términos técnicos, esta característica se denomina «cardinalidad». La incidencia se designa del siguiente modo:

1 Indica que el elemento del metadato debe aparecer una vez por cada elemento al que hace referencia, sea fichero, volumen o registro.

Ejemplo: Sólo debe existir un *identificador único de registro electrónico* para cada registro electrónico del SGRE.

1-n Refleja que el elemento del metadato debe aparecer al menos una vez por cada elemento al que hace referencia, pero que se puede presentar en más de una ocasión.

Ejemplo: Cada usuario del SGRE debe tener, cuando menos, un perfil asignado, pero puede contar con más de uno.

0-1 Significa que el elemento del metadato puede no existir, pero que cuando existe se presentará en una sola ocasión. Esta categoría incluye los elementos de metadatos necesarios en algún momento del ciclo de vida del volumen del fichero o del registro, así como los que podrían no resultar jamás necesarios en relación con un elemento determinado.

Ejemplo: La *fecha de cierre de un fichero electrónico* no se presentará hasta el cierre del fichero, pero al menos ha de aparecer una vez en cuanto se haya cerrado el fichero.

Ejemplo: Una *categoría de seguridad con marca protectora de registro* puede no asignarse jamás a un registro electrónico, pero de llevarse a cabo sólo cabría la asignación de una única categoría de seguridad.

0-n Indica que el elemento del metadato puede no aparecer jamás o presentarse en numerosas ocasiones en cada caso.

Ejemplo: Un *comentario de revisión sobre un fichero* electrónico puede no aparecer jamás o bien puede encontrarse una o más veces, dependiendo del historial de revisión del tal fichero.

Req.

Por último, cada elemento de un metadato remite al requisito en que se origina. Así, esta sección se puede utilizar para comprender un requisito que genera la necesidad de un elemento de metadato, con lo que, a su vez, se facilita la comprensión de dicho elemento.

En ocasiones son varios los requisitos que hacen referencia a un elemento de un metadato; en tales casos no se enumeran todos ellos. Por consiguiente, conviene destacar que esta sección no supone una ayuda a la hora de determinar qué requisitos hacen referencia a determinado elemento de un metadato.

Se hace una excepción con los elementos de los «metadatos definidos por los usuarios». Tales requisitos no remiten a ningún otro elemento.

En la versión electrónica de la presente especificación, el número del requisito constituye un hipervínculo con el requisito en sí.

Una entrada «N/A» indica «no aplicable».

12.3 Sistema de clasificación de los elementos de los metadatos

Conviene que el SGRE permita la existencia de los siguientes elementos en cada sistema de clasificación:

Ref.	Elemento del metadato	Incidencia	Req.
12.3.1	Nombre. *Puede ser el nombre de la unidad estructural de la organización (departamento, sección, etc.) responsable del sistema de clasificación.*	0-1	3.1.8
12.3.2	Identificador.	0-1	3.1.8

Ref.	Elemento del metadato	Incidencia	Req.
12.3.3	Descripción.	0-1	3.1.8
12.3.4	Elementos de metadatos definidos por el usuario. *Nota: Al menos deben estar presentes 12.3.1, 12.3.2 y 12.3.3.*	0-n	N/A

12.4 Elementos de los metadatos relativos a las clases y los ficheros

El SGRE debe permitir la existencia de los siguientes elementos en relación con cada clase y fichero:

Ref.	Elemento del metadato	Incidencia	Req.
12.4.1	Identificador.	1	3.2.2 7.1.1
12.4.2	Nombre.	1	3.2.2 7.1.1
12.4.3	Palabras clave descriptivas.	0-n	3.2.8
12.4.4	Descripción.	0-1	3.2.2
12.4.5	Fecha de apertura.	1	3.2.4
12.4.6	Fecha de cierre.	1	3.3.4
12.4.7	Persona o cargo responsable del mantenimiento.	1	4.1.1 4.1.7
12.4.8	Derechos de acceso de los grupos de usuarios. *Información acerca de cuáles de los grupos de usuarios pueden acceder al fichero o clase y del tipo de acceso que se les concede.*	0-n	4.1.1 4.1.7
12.4.9	Derechos de acceso de los usuarios. *Información acerca de los usuarios que pueden acceder al fichero o clase y del tipo de acceso que se les concede.*	0-n	4.1.1 4.1.7
12.4.10	Categoría de seguridad.	0-1	4.6.2

Ref.	Elemento del metadato	Incidencia	Req.
12.4.11	Cuando se admite el requisito 12.4.10 se ha de contar con un historial de categorías de seguridad que recoja, en relación con la categoría anterior: • la categoría • las fechas del cambio • los motivos del cambio • el usuario responsable del cambio	0-n	9.3.6
12.4.12	Norma(s) sobre el cierre de volúmenes.	1-n	3.4.8
12.4.13	Cuando el SGRE se utilice en la gestión de los ficheros en papel, los detalles de los ficheros en papel asociados (o una indicación de la existencia de los ficheros híbridos). *No necesario en relación con las clases.*	0-1	10.1.1
12.4.14	Elementos de metadatos definidos por el usuario.	0-n	N/A
12.4.15	Fecha de borrado.	0-1	9.3.7
12.4.16	Autor del borrado.	0-1	9.3.7
12.4.17	Calendario de conservación.	0-n	5.1.4 5.1.5
12.4.18	Historial de clasificación.	0-n	3.4.4 9.1.6
12.4.19	Motivos de la reclasificación.	0-n	3.4.5

Conviene que el SGRE admita la existencia de los siguientes elementos en relación con cada clase y fichero:

Ref.	Elemento del metadato	Incidencia	Req.
12.4.20	Vínculos con los ficheros asociados. *No es necesario cuando se trata de clases.*	0-n	3.4.11
12.4.21	Información sobre otros accesos. *Por ejemplo, información sobre la exclusión de un fichero con arreglo al Convenio de Derechos Humanos o a restricciones de la propiedad intelectual.*	0-n	8.1.29
12.4.22	Nombre basado en una palabra clave.	0-n	3.2.6
12.4.23	Otro nombre.	0-1	3.2.7

Ref.	Elemento del metadato	Incidencia	Req.
12.4.24	Términos descriptivos.	0-n	3.2.8

12.5 Elementos de los metadatos relativos a los ficheros y los volúmenes ficheros

Algunos elementos de los metadatos pueden referirse tanto a los ficheros como a sus volúmenes. Esto se debe a las diferencias en la utilización de ficheros y volúmenes, tal y como se explica en la sección 2.2, en el epígrafe «Ficheros y volúmenes electrónicos».

Por consiguiente, los usuarios de la presente especificación deben determinar el nivel adecuado de esos elementos de metadatos, de conformidad con sus necesidades. Así, las decisiones de la dirección en materia de clasificación de seguridad, eliminación o revisión se pueden adoptar a nivel del fichero o a nivel de volumen. En ciertos SGRE, todas estas cuestiones se pueden tratar a nivel de fichero, mientras que en otras se hará a nivel de volumen o dependerán de los ficheros.

El SGRE debe admitir la existencia de los siguientes elementos en relación con cada fichero o volumen de fichero:

Ref.	Elemento del metadato	Incidencia	Req.
12.5.1	Calendario de conservación, o de no tenerse en cuenta el requisito 5.1.5, fecha de la revisión de la eliminación o acción e instrucciones de eliminación.	1-n	5.1.4 5.1.5 10.2.1
12.5.2	Fecha de apertura.	1	3.3.2
12.5.3	Fecha de cierre.	0-1	3.4.9
12.5.4	Identificador de la organización a la que se va a exportar el fichero, como los archivos públicos o nacionales, siempre que se contemple tal posibilidad.	0-n	5.3.1 5.3.17
12.5.5	Estado de la transferencia.	0-n	5.3.7
12.5.6	Indicador de elemento físico o híbrido.	1	10.1.1 10.1.2 10.1.3 10.2.4
12.5.7	Emplazamiento físico, cuando se trate de ficheros físicos.	1	4.4.2 10.1.4

Ref.	Elemento del metadato	Incidencia	Req.
12.5.8	Estado en relación con la salida y la entrada, cuando se trate de ficheros físicos.	1	4.4.2 10.1.5 10.2.8
12.5.9	Fecha de salida, cuando se trate de ficheros físicos.	1	4.4.2 10.2.8
12.5.10	Fecha de salida y lugar al que se dirige, cuando se trate de ficheros físicos.	1	4.4.2 10.2.8
12.5.11	Fecha de recordatorio, cuando se trate de ficheros físicos.	1-n	10.2.9
12.5.12	Recordatorio para, cuando se trate de ficheros físicos.	1-n	10.2.9
12.5.13	Texto recordatorio, cuando se trate de ficheros físicos.	1-n	10.2.9
12.5.14	Estado, en relación con la destrucción	1	5.1.4 5.3.17
12.5.15	Fecha de destrucción y usuario responsable.	0-1	9.3.7
12.5.16	Comentario de revisión.	0-n	5.2.6
12.5.17	Fecha de destrucción.	0-1	5.3.15
12.5.18	Elementos de metadatos definidos por los usuarios.	0-n	N/A

Conviene que el SGRE permita la existencia de los siguientes elementos en relación con cada fichero o volumen de fichero:

Ref.	Elemento del metadato	Incidencia	Req.
12.5.19	Cuando se admita el requisito 12.4.10, conviene revisar la fecha de la clasificación de seguridad.	0-1	4.6.12
12.5.20	Códigos de barras y/u otros datos sobre el emplazamiento físico, cuando se trate de ficheros físicos	0-1	10.1.9
12.5.21	La transferencia o el borrado lógico de un fichero.	0-1	9.3.1
12.5.22	Estado de un fichero híbrido en relación con la transferencia, el traslado o el borrado.	0-n	5.3.9

12.6 Elementos de los metadatos relativos al volumen

El SGRE debe permitir la existencia de los siguientes elementos en relación con cada volumen:

Ref.	Elemento del metadato	Incidencia	Req.
12.6.1	Identificador.	1	3.3.1 7.1.1
12.6.2	Indicador de fichero híbrido o físico.	0-1	10.1.1 10.1.2 10.1.3
12.6.3	Elementos de los metadatos definidos por el usuario.	0-n	N/A

12.7 Elementos de los metadatos relativos a los registros

El SGRE debe permitir la existencia de los siguientes elementos en relación con cada registro:

Ref.	Elemento del metadato	Incidencia	Req.
12.7.1	Identificador.	1	7.1.1
12.7.2	Tema.	1	6.1.2 10.3.5
12.7.3	Autor. *Puede ser un individuo o una organización, y siempre que sea posible se capturará de forma automática.*	1	6.1.2 6.4.3 10.3.5
12.7.4	Persona o cargo responsable del mantenimiento del registro en el SGRE.	0-1	4.1.7
12.7.5	Fecha (y hora, cuando proceda) de la compilación del registro. *Por ejemplo:* • *Cuando el registro sea una carta, la fecha que consta en la parte superior de la carta.* • *Cuando el registro sea un sonido o cualquier otra grabación de un periodo, la hora de inicio y la de término.* *Siempre que sea posible, la captura realizará se forma automática.*	1	6.1.2 10.3.5

Ref.	Elemento del metadato	Incidencia	Req.
12.7.6	Destinatario o destinatarios. *Individuo o individuos, o bien organización u organizaciones a las que se dirigía la información del registro. Siempre que sea posible, la captura se realizará de forma automática.*	1-n	6.1.2 6.4.3
12.7.7	Tipo de registro *Por lo general, una carta, una factura, un memorando, etc. Siempre que sea posible, la captura se realizará de forma automática.*	1	6.1.2 10.3.5
12.7.8	Fecha y hora de la grabación. *Su captura se realizará de forma automática.*	1	6.1.7
12.7.9	Derechos de acceso de los grupos de usuarios. *Información sobre los grupos de usuarios que pueden acceder al registro y el tipo de acceso que se les concede.*	0-n	4.1.1
12.7.10	Derechos de acceso de los usuarios. *Información sobre los usuarios que pueden acceder al registro y el tipo de acceso que se les concede.*	0-n	4.1.1
12.7.11	Categoría de seguridad. *Siempre que sea posible, la captura se realizará de forma automática a partir del documento que constituye el registro.*	0-1	4.6.1
12.7.12	Historial de las categorías de seguridad, esto es, para cada una de las clasificaciones anteriores: • la categoría • las fechas de modificación • el motivo del cambio • el usuario responsable del cambio.	0-n	9.3.6

Ref.	Elemento del metadato	Incidencia	Req.
12.7.13	Metadatos de conservación, siempre que el SGRE se haya concebido con objeto de conservar el registro durante un tiempo superior al del ciclo de vida previsto para las aplicaciones fuentes. Suelen incluir los siguientes elementos, aunque no tienen por qué limitarse a ellos: • Nombres de los ficheros • Dependencia del hardware • Dependencia del sistema operativo • Dependencia del software de aplicaciones (nombres y versiones de las aplicaciones) • Formatos de fichero • Resolución • Versión del algoritmo de compresión y sus parámetros • Sistema de codificación • Información sobre la reproducción. *Pueden ser valores múltiples siempre que se incluyan documentos compuestos.*	1-n	6.1.2 8.2 8.3 8.4 11.7.7
12.7.14	Indicador de registro crítico.	1	4.3.6
12.7.15	Identificador o identificadores del extracto.	0-n	8.1.26
12.7.16	Calendario de conservación.	0-n	5.1.4 5.1.5
12.7.17	Estado de la transferencia.	0-n	5.3.17
12.7.18	Elementos de los metadatos definidos por el usuario.	0-n	N/A

Conviene que el SGRE permita la existencia de los siguientes elementos en relación con cada fichero electrónico:

Ref.	Elemento del metadato	Incidencia	Req.
12.7.19	Fecha en la que se revisará la clasificación de seguridad.	0-1	4.6.12
12.7.20	Firma(s) electrónica(s), certificado(s), refrendo(s).	0-n	10.5.7

Ref.	Elemento del metadato	Incidencia	Req.
12.7.21	Autenticación de las firmas electrónicas, incluidas la autoridades de certificación y la fecha y hora de la verificación.	0-n	10.5.1 10.5.4
12.7.22	Fecha del envío. *Siempre que sea posible, se capturará de forma automática.*	1	6.1.2
12.7.23	Fecha de la recepción. *Siempre que sea posible, se capturará de forma automática.*	1	6.1.2
12.7.24	Vínculos con los registros relacionados.	0-n	11.1.18
12.7.25	Restricciones derivadas de la propiedad intelectual *Por ejemplo, normas sobre la utilización de la información contenida en el registro y los desembolsos en concepto de derechos de autor.*	0-n	8.1.29
12.7.26	Versión del documento.	0-n	6.1.10
12.7.27	Idioma.	0-n	11.4.11
12.7.28	Información sobre la encriptación.	0-1	10.6.2
12.7.29	Información sobre la filigrana electrónica.	0-1	10.7.1

12.8 Elementos de los metadatos relativos a los extractos de registros

El SGRE debe permitir la existencia de los siguientes elementos en relación con cada extracto de registro:

Ref.	Elemento del metadato	Incidencia	Req.
12.8.1	Identificador.	1	7.1.1 9.3.11
12.8.2	Identificador del registro original.	1	8.1.26
12.8.3	Fecha de creación del extracto.	1	9.3.11
12.8.4	Identificador del usuario autor del extracto.	1	9.3.11
12.8.5	Motivos de la creación del extracto.	0-1	9.3.11
12.8.6	Elementos de los metadatos definidos por el usuario.	0-n	N/A

12.9 Elementos de los metadatos relativos al usuario

El SGRE debe permitir la existencia de los siguientes elementos en relación con cada usuario

Ref.	Elemento del metadato	Incidencia	Req.
12.9.1	Identificador del usuario.	1	4.1.1
12.9.2	Perfil del usuario.	1-n	4.1.3
12.9.3	Pertenencia a un grupo de usuarios.	0-n	4.1.5
12.9.4	Derechos de acceso del usuario.	0-n	4.1.1
12.9.5	Fecha de vencimiento de los derechos de acceso.	1	4.1.2
12.9.6	Habilitación de seguridad del usuario, siempre que el entorno la exija.	1	4.6.7
12.9.7	Fecha de vencimiento de la habilitación.	1	4.6.12
12.9.8	Elementos de los metadatos definidos por el usuario.	0-n	N/A

12.10 Elementos de los metadatos relativos al perfil

El SGRE debe permitir la existencia de los siguientes elementos en relación con cada perfil:

Ref.	Elemento del metadato	Incidencia	Req.
12.10.1	Nombre del perfil.	1	4.1.3
12.10.2	Pertenencia a un grupo de perfiles.	0-n	4.1.3
12.10.3	Derechos de acceso del perfil.	0-n	4.1.1
12.10.4	Fecha de vencimiento de los derechos de acceso.	1	4.1.2
12.10.5	Habilitación de seguridad del perfil, siempre que el entorno lo exija.	1	4.1.3
12.10.6	Fecha de vencimiento de la habilitación.	1	4.6.12
12.10.7	Elementos de los metadatos definidos por el usuario.	0-n	N/A

12.11 Puntualizaciones sobre la personalización de los REQUISITOS DE LOS METADATOS

Conviene que los usuarios de la presente especificación analicen los requisitos que en materia de metadatos presenta su aplicación y que los modifiquen atendiendo al resultado del análisis.

Tras identificar los elementos de los metadatos que resultan necesarios, convendría que determinasen, para cada elemento, los siguientes atributos:

- El formato (véase 12.1.5) y la longitud del campo.
- La obligatoriedad (si es preceptivo o facultativo).
- La procedencia de los datos (véase 12.1.9, 12.1.10, 12.1.11 y 12.1.12).
- La naturaleza de la validación (véase 12.1.13, 12.1.14 y 12.1.15).
- Las normas de transmisión (véase 12.1.11).
- Las normas aplicables a los valores por defecto utilizados en la introducción de datos (por ejemplo, la fecha de declaración puede ser, por defecto, la actual, mientras que el tipo de registro podría tener que introducirse de forma manual).

Los requisitos sólo se podrán especificar con detalle tras la aplicación de este procedimiento.

Téngase en cuenta que las normas de validación, captura automática, transmisión y determinación de valores por defecto tienen una influencia primordial a la hora de asegurar la facilidad de uso y una tasa de errores aceptable, siempre que el sistema se utiliza en el funcionamiento normal de oficina (a diferencia de lo que ocurre con un archivo dedicado).

13 MODELO DE REFERENCIA

13.1 Glosario

En el glosario se definen los términos clave empleados en la especificación MoReq, esto es, tanto en los requisitos como en el presente modelo.

Algunas definiciones importantes se han copiado o adaptado de glosarios que aparecen en las publicaciones de referencia citadas en el Anexo 1. Tras cada definición se citan las fuentes empleadas.

Los términos en *cursiva* están definidos en este glosario.

abierto

Dícese del *volumen de fichero electrónico* que aún no se ha cerrado y que, por ello, permite la adición de *registros*.

abrir

Proceso de creación de un nuevo *volumen de fichero electrónico*.

administrador

Perfil responsable de la realización de las operaciones cotidianas propias de la política de gestión de registros en el marco de la organización.

Esta definición constituye una simplificación. Sobre todo en las grandes organizaciones, las tareas que en esta especificación se atribuyen a los administradores se pueden dividir entre varios *perfiles*, con títulos como el de «gestor de registros», «responsable de registros», «archivero», etc.

autenticidad

(sólo en el contexto de la gestión de registros) La cualidad de lo genuino.

Fuente: Adaptado y resumido de la definición de «autenticidad de un registro» del glosario del proyecto UBC-MAS (referencia [8] del Anexo 1).

Nota: En relación con un *registro*, tal cualidad implica que éste es lo que afirma ser, sin ocuparse de la fiabilidad del contenido del registro en tanto que declaración de un hecho.

Nota: Los elementos que confieren autenticidad a un registro son el modo, la forma y/o el estado de la transmisión y/o el modo de conservación y su custodia. Para más información consúltese el glosario del proyecto UBC-MAS (referencia antes indicada).

calendario de conservación

Conjunto de instrucciones asignadas a una *clase* o *fichero* que determinan el período de tiempo que es preciso que la organización conserve los *registros* por motivos relacionados con su actividad, así como el destino final de los *registros* una vez haya finalizado dicho periodo.

Fuente: Adaptado de la definición del «calendario de eliminación» de la especificación funcional de la Public Record Office (véase la referencia [2] del Anexo 1).

captura

Registro, *clasificación*, adición de *metadatos* y almacenamiento de un *registro* en un sistema que gestiona *registros.*

categoría de seguridad

Uno o varios términos asociados a un *registro* que definen las normas que rigen el acceso a éste.

Nota: Las categorías de seguridad se suelen asignar a escala nacional o de organización. Algunos ejemplos de categorías de seguridad utilizadas en los organismos públicos de gran parte de Europa son: «Máximo secreto», «Secreto», «Confidencial», «Acceso restringido», «Desclasificado». A veces, complementan estas categorías términos como «Reservado a la UEO» o «Reservado para el personal en plantilla».

Nota: No es un término de uso corriente.

cerrado

Describe un *volumen de fichero electrónico* que se ha cerrado y no puede admitir la adición de *registros.*

cerrar

Proceso de modificación de los atributos de un *volumen de fichero electrónico* de forma que no admita jamás la adición de *registros*.

clase

(sólo en esta especificación) Parte de una jerarquía representada por una línea que va desde cualquier punto del sistema jerárquico de clasificación a todos los ficheros que quedan por debajo.

Nota: Este término se puede corresponder, en la terminología clásica, con una «clase primaria», un «grupo» o una «serie» (o bien una subclase, un subgrupo, una subserie, etc.) de cualquier nivel del sistema de clasificación.

clasificación

Identificación y estructuración sistemáticas de las actividades empresariales o los *registros* en categorías, de acuerdo con convenciones, métodos y normas de procedimientos organizados de forma lógica y representados en un sistema de clasificación.

Fuente: ISO 15489 (proyecto de norma internacional; véase la referencia [9] del Anexo 1).

destrucción

Proceso de eliminación o borrado de registros de forma que no sea posible reconstrucción alguna.

Fuente: ISO 15489 (proyecto de norma internacional; véase la referencia [9]del Anexo 1).

digital

Véase «*electrónico*».

documento

Información u objeto registrado que se puede tratar como una unidad.

Fuente: ISO 15489 (proyecto de norma internacional; véase la referencia [9] del Anexo 1).

Nota: Un documento puede estar en papel, en microfilm o en un soporte magnético o electrónico de cualquier otro tipo. Puede incluir cualquier combinación de texto, datos, gráficos, sonido, animaciones o cualquier otra clase de información. Un solo documento puede estar formado por uno o varios objetos de datos.

Nota: Los documentos se diferencian de los *registros* en varias cuestiones esenciales. Véase *registro*.

documento electrónico

Un *documento* en su forma electrónica.

Nota: El término «*documento electrónico*» no se refiere únicamente a los documentos de texto que se suelen crear con procesadores de texto, sino que también comprende los mensajes de correo electrónico, las hojas de cálculo, los gráficos e imágenes, los documentos HTML o XML y los documentos compuestos, multimedios o de otros tipos de uso en oficinas.

EDMS

Sistema de gestión electrónica de documentos.

Nota: En la presente especificación no se aborda la funcionalidad necesaria en un EDMS, aunque estos sistemas se utilizan a menudo en estrecha integración con los *SGRE*. Para más información, véase la sección 10.3.

electrónico

En el contexto de la presente especificación, «electrónico» es sinónimo de «digital».

Nota: Si bien las grabaciones analógicas se pueden considerar electrónicas, en el marco de la presente especificación no se admiten como tales, pues no se pueden almacenar en un sistema

informático a menos que se conviertan a su forma digital. De ello se desprende que, de acuerdo con la terminología de la presente especificación, los registros analógicos sólo se pueden almacenar como *registros físicos.*

exportación

Proceso de elaboración de una copia completa de los *ficheros electrónicos* para otro sistema.

Nota: A diferencia de lo que sucede en la *transferencia*, tras la exportación los ficheros siguen en el SGRE.

extracción

(de un *registro*) Copia de un *registro* en el que se han realizado ciertas modificaciones dirigidas a eliminar u ocultar, pero no a añadir ni modificar, el contenido ya existente.

Fuente: Definición de «ejemplar» en la especificación funcional de la Public Record Office (véase la referencia [2] del Anexo 1).

Nota: A menudo, las modificaciones se deben a la existencia de restricciones en la revelación de información. Así, un *registro* no se podrá consultar hasta que se hayan ocultado o eliminado los nombres de ciertos individuos. En este caso, se crea un *extracto* del registro en el que los nombres pasan a ser ilegibles. En ocasiones, este proceso de ocultación se denomina redacción.

fichero

(1) En solitario, este término hará referencia tanto a los ficheros electrónicos como a los ficheros en papel.

(2) Acompañado de modificadores, como sucede, por ejemplo, con *fichero electrónico* o con *fichero en papel*, se aplicará la definición correspondiente.

fichero electrónico

Conjunto de *registros electrónicos* relacionados entre sí.

Fuente: Especificación funcional de «fichero electrónico» de la Public Record Office (referencia [2] del Anexo 1).

Nota: Este término se emplea a menudo en sentido amplio para designar los *volúmenes electrónicos.*

fichero en papel

Un elemento que guarda *documentos físicos*.

Fuente: Especificación funcional de la Public Record Office (véase la referencia [2] del Anexo 1).

Nota: Algunos ejemplos de ficheros en papel podrían ser, entre otros, los sobres, los archivadores o las carpetas de anillas.

fichero híbrido

Un conjunto de *registros electrónicos* y *registros físicos* relacionados almacenados en parte como *ficheros electrónicos* en el marco del SGRE y en parte como *ficheros en papel* conservados fuera del sistema.

Fuente: Definición de «fichero híbrido» en la especificación funcional de la Public Record Office (véase la referencia [2] del Anexo 1).

grabación

Acto por el que se adjudica a un *registro* un identificador único en el momento de su entrada en el sistema.

Fuente: ISO 15489 (proyecto de norma internacional; véase la referencia [9] del Anexo 1).

Nota: Esta operación suele conllevar la grabación en un «registro» de metadatos importantes, como «todos los datos necesarios para la identificación de las personas y actos en cuestión, así como el contexto documental de los registros» (Glosario del proyecto UBC-MAS, referencia [x] del Anexo 1).

habilitación

Véase «habilitación de seguridad».

habilitación de seguridad

Uno o varios términos asociados a un *usuario* que definen las *categorías de seguridad* a las que tiene acceso el *usuario*.

metadatos

(en el contexto de gestión de registros) Información estructurada o semiestructurada que permite la creación, la gestión y la utilización de registros a lo largo del tiempo, tanto dentro de los mismos ámbitos en que se crearon como entre ellos.

Fuente: Definición de trabajo del Archiving Metadata Forum (http://www.archiefschool.nl/amf).

Nota: La distinción entre datos y metadatos puede resultar algo confusa. Así, por lo general parece evidente que los datos esenciales utilizados en la indexación de un registro (título, fecha, etc.) forman parte de los metadatos del registro; en cambio, la pista de auditoría de un registro y el calendario de conservación se pueden considerar tanto datos como metadatos, dependiendo del contexto. Por ejemplo, se pueden definir distintos tipos de metadatos en relación con la indexación, la conservación, la reproducción, etc. Estas características del uso de los metadatos quedan dentro del ámbito de aplicación de la especificación MoReq (en el contexto de la gestión de registros). Información estructurada o semiestructurada que permite la creación, la gestión y la utilización de registros a lo largo del tiempo.

momento de la configuración

Punto del ciclo de vida del SGRE en que éste se instala y se fijan sus parámetros.

PDF

Formato de documento portable (Portable Document Format).

Nota: Este formato es propiedad de Adobe Inc., pero su uso está muy extendido. Su inclusión en el presente glosario no indica ninguna preferencia por este formato.

perfil

Suma de permisos funcionales concedidos a un subconjunto predefinido de usuarios.

Fuente: Especificación funcional de la Public Record Office (véase la referencia [2] del Anexo 1).

pista de auditoría

Información sobre las transacciones u otras actividades que hayan influido o modificado entidades, como los elementos de los metadatos, y que aporta detalles suficientes para permitir la reconstrucción de la actividad anterior.

Nota: Habitualmente, la pista de auditoría está formada por una o más listas, o bien por una base de datos que puede visualizarse en ese formato. Cuando se trata de transacciones informatizadas, un sistema informático genera tales listas; cuando se trata de actividades manuales, la lista se elabora de forma manual. En la presente especificación se trata sobre todo el primer caso.

redacción

Proceso de ocultación de la información confidencial de un *registro*.

Nota: Puede comprender la aplicación de rectángulos opacos que oculten nombres, etc. (el equivalente electrónico a la censura con tinta de documentos en papel) o bien la eliminación de ciertas páginas.

Nota: En ningún caso afecta a la totalidad del *registro electrónico*. La redacción se lleva a cabo sobre una copia del registro electrónico denominada *extracto*.

registro

Documento o documentos elaborados o recibidos por una persona u organización en el curso de su actividad y conservados por esa persona u organización.

Fuente: Adaptado de la especificación funcional de la Public Record Office (referencia [2] del Anexo 1).

Nota: También se pueden aplicar definiciones nacionales locales.

Nota: Un registro puede constar de uno o varios *documentos* (como sucede cuando un documento tiene anexos) y estar en cualquier soporte y formato. Además del contenido del documento o los documentos, debe incluir información contextual y, cuando proceda, estructural (esto es, información que describa los componentes del registro). Una característica esencial de un registro es que no se puede modificar.

registro electrónico

Un *registro* en soporte *electrónico*.

Nota: Puede estar en soporte electrónico porque ha se ha creado mediante un programa informático de aplicación o bien porque se ha digitalizado, esto es, se ha escaneado un documento en papel o microfilm.

repertorio

Lista formada por los títulos de los ficheros existentes desde los niveles más bajos del sistema de clasificación.

reproducción

Manifestación de un *registro electrónico* presentado (es decir, reproducido) de forma que permite que los *usuarios* lo consulten.

Nota: Puede comprender la visualización en pantalla, la impresión y las presentaciones impresas, sonoras o multimedios.

Nota: La naturaleza exacta de la reproducción se puede ver afectada por el entorno de software y hardware. Suele ocurrir que en distintas reproducciones del mismo *registro* se observen variaciones en detalles como el tamaño de las fuentes, los finales de línea, la paginación, la resolución, la profundidad de bits, el espacio cromático, etc. En general, tales diferencias resultan aceptables; sin embargo, a veces es preciso sopesar sus posibles efectos caso por caso. De cualquier modo, tales consideraciones superan el alcance de la presente especificación.

reproducir

Proceso de elaboración de una *reproducción*.

SGRE

Sistema de gestión de registros electrónicos.

Nota: El SGRE difiere del *sistema de gestión electrónica de documentos (EDMS, por sus siglas en inglés)* en varios puntos clave. Para más detalles, véase la sección 10.3.

sistema de clasificación

Véase clasificación.

Fuente: Definición de «Sistema de clasificación» en ISO 15489 (proyecto de norma internacional; véase la referencia [9] del Anexo 1).

Nota: Los sistemas de clasificación se suelen representar como jerarquías.

SQL

Lenguaje de consulta estructurado (por las siglas de la expresión correspondiente en inglés, *Structured Query Language*).

Nota: Define una norma de las bases de datos relacionales que se suelen utilizar en el almacenamiento de los metadatos del SGRE. Dicha norma se define en la ISO 9075 (véase el Anexo 7).

transferir

Trasladar *ficheros electrónicos* completos a otro sistema.

Fuente: Adaptado de la especificación funcional de la Public Record Office (véase la referencia [2] del Anexo 1).

Nota: Con frecuencia se lleva a cabo la transferencia de todos los *ficheros* de una *clase* del *sistema de clasificación*, cuando el objetivo de la operación es el traslado de los ficheros a un archivo para conservarlos permanentemente.

Nota: Véase también *exportar.*

usuario

Cualquier persona que utilice el *SGRE*.

Nota: Ello puede incluir, entre otros, a los administradores, al personal de oficina, al público general y a personal externo, como los auditores.

versión

(de un *documento*). Estado de un documento en algún momento de su desarrollo.

Fuente: Especificación funcional de la Public Record Office (véase la referencia [2] del Anexo 1) .

Nota: Una versión suele ser uno de los borradores de un *documento* o bien el documento definitivo. No obstante, en ocasiones existen varias versiones del documento definitivo, como sucede con los manuales técnicos. Téngase en cuenta que no puede existir más de una versión de un *registro*; véase también *extracto* .

volumen

Subdivisión de un *fichero electrónico* o *en papel*

Fuente: Definición de «parte» en la especificación funcional de la Public Record Office (referencia [2] del Anexo 1).

Nota: Las subdivisiones se establecen para facilitar la gestión del contenido de los ficheros mediante la creación de unidades que no resulten demasiado grandes o difíciles de manejar. Las subdivisiones se realizan en función de criterios más mecánicos (por ejemplo, basadas en el número de registros, en series de números o en lapsos de tiempo) que intelectuales.

13.2 Modelo de relación entre entidades

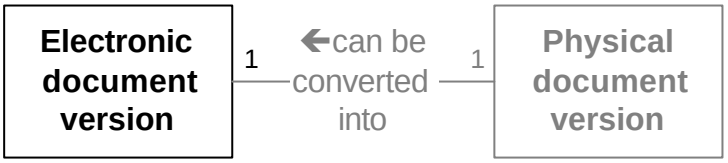
Esta sección es una repetición de la 2.3, con el objetivo de facilitar su consulta.

En ella se expone un modelo de relación entre entidades que puede facilitar la comprensión de la especificación. La sección 13.3 incluye una exposición detallada a tal respecto.

Una característica notable de este diagrama es que no representa estructuras reales almacenadas en el SGRE, sino un enfoque de los metadatos asociados a los registros. Un SGRE utiliza estos metadatos en la gestión de sus registros de igual forma que si la estructura mostrada en el diagrama existiese de veras. Para una explicación más pormenorizada de esta cuestión, véase la sección 2.2 .

Las relaciones entre ficheros, volúmenes, registros y demás entidades se muestran de forma más rigurosa en el siguiente diagrama sobre las relaciones entre entidades, que constituye una representación formal de ciertas estructuras que conforman un SGRE.

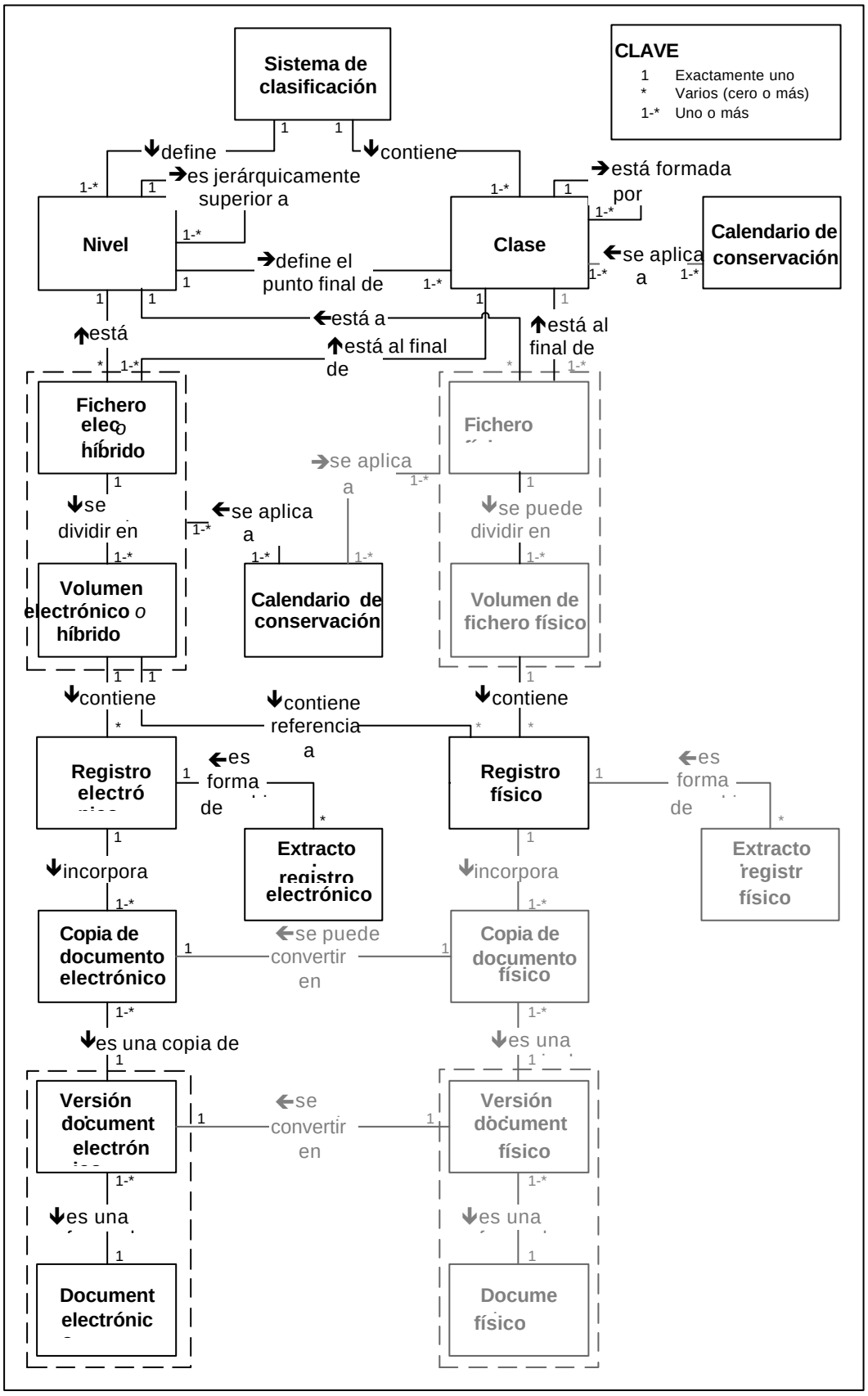
En el diagrama, las entidades (ficheros, registros y demás) se representan mediante rectángulos y las líneas que los unen representan las relaciones entre entidades. Cada relación se describe en el centro de la línea con un texto que se debería leer en la dirección de la flecha. A cada extremo de la línea que representa la relación se encuentra un número que hace referencia a la frecuencia (en sentido estricto, la cardinalidad) y que se explica en la clave. Así por ejemplo, el siguiente fragmento del diagrama:



Versión electrónica del documento ←se puede convertir en Versión física del documento

significa «Una versión física del documento se puede convertir en una versión electrónica del documento» (obsérvese la dirección de la flecha).

Nótese que la entidad «clase» se relaciona consigo misma en virtud de la relación «está formada por». Esta relación recurrente describe, en términos formales, la jerarquía de las carpetas, en las que una clase puede contener a otra. Del mismo modo, un nivel puede estar en una posición jerárquicamente superior a la de otros niveles.


Sistema de clasificación
CLAVE
1 Exactamente uno
* Varios (cero o más)
1-* Uno o más
define
contiene
es jerárquicamente superior a
está formada por
Nivel
Clase
Calendario de conservación
define el punto final de
se aplica a
está a
está al final de
está
está al final de
Fichero electrónico híbrido
Fichero
se aplica a
se dividir en
se aplica a
se puede dividir en
Volumen electrónico o híbrido
Calendario de conservación
Volumen de fichero físico
contiene
contiene referencia a
contiene
Registro electró
es forma de
Registro físico
es forma de
Extracto registro electrónico
Extracto registr físico
incorpora
incorpora
Copia de documento electrónico
se puede convertir en
Copia de documento físico
es una copia de
es una
Versión document electrón
se convertir en
Versión document físico
es una
es una
Document electrónic
Docume físico

13.3 Explicación del diagrama de relaciones entre entidades

El diagrama de relaciones entre entidades de la sección 13.2 ilustra un contexto más amplio de la existencia de bs registros electrónicos. En aras de una mayor claridad, ofrece más detalles sobre la relación entre los registros y documentos electrónicos y en papel que el resto de los capítulos de la presente especificación.

En esta especificación no se incide demasiado en la gestión de los registros físicos y sólo se alude a ellos cuando se hace referencia a la continuidad entre los registros en papel y los electrónicos del SGRE. Por consiguiente, la mayor parte de las entidades y relaciones en papel aparecen en gris, a diferencia de sus equivalentes electrónicos, en negro.

Téngase en cuenta que el diagrama es un modelo simplificado que no pretende representar todas las entidades o relaciones posibles, sino que muestra las más importantes para esta aplicación. Por ejemplo, en él no constan los usuarios, los perfiles, etc.

El resto de la presente exposición se dedica a la descripción de las entidades del diagrama y de las relaciones entre ellas.

Sistema de clasificación

La aplicación de los principios de gestión de registros exige que las organizaciones dispongan de un sistema de clasificación como mínimo. Dicho sistema establece la estructura de archivo, que suele estar formada por una jerarquía, números, nombres y descripciones, para una parte determinada de la organización.

Nivel

El sistema de clasificación se suele representar como una jerarquía o estructura en árbol. La jerarquía abarca una serie de niveles que se corresponden con los «topes máximos» de las clases, grupos, subclases, etc. empleados en la descripción de los sistemas de clasificación de los sistemas físicos. Cada nivel puede presentar niveles inferiores por debajo de él en la jerarquía.

Clase

El sistema de clasificación se puede considerar una jerarquía formada por ciertas clases, del mismo modo que un árbol está formado por ramas. Cada clase se relaciona con la jerarquía en un nivel y puede extenderse a varios niveles e incluir clases de menor tamaño. Ciertas clases pueden empezar en cualquier nivel, pero cada clase comienza sólo en un nivel determinado.

Fichero

Los ficheros se encuentran al final de las clases, en cualquier nivel de la jerarquía, del mismo modo que las hojas se encuentran en los extremos de las ramas de los árboles. Existen ficheros electrónicos, físicos o híbridos. Un fichero físico es el contenedor convencional utilizado en el almacenamiento de documentos o registros físicos, como el papel, la cinta de audio, etc., en lugar de los electrónicos.

Volumen

Los ficheros se pueden dividir en volúmenes, con arreglo a unas reglas concretas. En la práctica, algunos ficheros no se dividen en volúmenes. Las normas pueden variar según el tamaño o el número de los registros o depender de ciertas transacciones o intervalos de tiempo. Esta práctica surgió con los ficheros físicos con el propósito de limitar su tamaño y peso a niveles manejables. Cuando procede, también se aplica a los ficheros electrónicos, con objeto de restringir su tamaño y facilitar su revisión, su transferencia, etc.

En la práctica, los términos «fichero» y «volumen» se utilizan en sentido laxo y a veces intercambiable. Así, suele suceder que un usuario pida un «fichero» cuando, para ser exacto, tendría que solicitar un «volumen». Esto es especialmente obvio cuando un fichero físico está formado por un solo volumen. En este caso, aun cuando desde un punto de vista analítico el fichero está formado por un volumen, no siempre está etiquetado como tal hasta la apertura del segundo volumen. En sentido estricto, todos los usuarios finales manejan volúmenes a los que, para simplificar, se llama ficheros. En torno a los ficheros y volúmenes electrónicos (y también a las correspondientes entidades físicas) se han dibujado recuadros discontinuos. Con ello se refleja la situación real en que la utilización del término volumen electrónico, en lugar de fichero electrónico, podría dar lugar a malentendidos.

Calendario de conservación

Los dos rectángulos de la ilustración representan los calendarios de conservación. Se han dibujado dos para simplificar el diseño del diagrama, aunque en realidad ambos representan una sola entidad.

En el calendario de conservación se fijan las normas que rigen la conservación y la eliminación de los registros. El SGRE puede incluir varios calendarios, uno o más de los cuales se aplicarían a cada clase, fichero o volumen.

Registro

Los registros, la entidad más importante del sistema, constituyen la esencia misma de éste. Son la razón que lleva al desarrollo de toda la infraestructura de gestión de registros, pues constituyen la crónica de las actividades de la organización.

Los registros se forman a partir de los documentos. Cada registro puede comprender uno o varios documentos y cada documento puede aparecer en varios registros. Los registros se organizan en ficheros, con varios registros por fichero.

Extracto de registros

En ocasiones es preciso crear una versión expurgada (esto es, censurada) de un registro (por ejemplo, para eliminar ciertos nombres de personas por razones de confidencialidad). Habida cuenta de que los registros en sí no se pueden modificar, este proceso se denomina «elaboración de un extracto de registro» y consiste en la copia del registro (dejando el original intacto) y la expurgación de esa copia.

Versión de un documento y documento

Los documentos pueden existir en forma física y en forma electrónica.

Los documentos físicos pueden estar en papel, en cinta, en película o en otros soportes. No obstante, en aras de una mayor simplicidad, en el resto de la presente especificación se los denomina, en general, documentos en papel. Los documentos electrónicos son el equivalente digital de los documentos en papel. Suelen asumir la forma de un documento de un procesador de textos o de un mensaje de correo electrónico y pueden constar de varios ficheros informáticos, como un informe realizado con un procesador de textos con tablas de hoja de cálculo integradas, o bien una página de Internet con gráficos incrustados. También pueden ser ficheros de imagen obtenidos a partir del escaneado de documentos en papel.

Pueden existir varias versiones de un documento. Tal y como ocurría con los ficheros y los volúmenes, también existe cierta confusión en esta distinción, debido a que no se suele asignar un número de versión a los documentos que presentan una sola versión. Se han dibujado recuadros discontinuos en torno a los documentos electrónicos y a las versiones de éstos. Con ello se pretende reflejar la situación real en que la utilización del término «versión de documento electrónico» en vez de «documento electrónico» no resulta de ninguna ayuda. Por consiguiente, en esta especificación se utiliza el término «documento electrónico» en sentido amplio, para designar, en numerosas ocasiones, las versiones de documentos electrónicos.

Una copia de un documento físico se puede convertir en una copia de un registro electrónico recurriendo al escáner o a cualquier otro instrumento de digitalización. También se pueden convertir varias copias de documentos físicos en un único registro electrónico, como sucede con la nota de introducción de un informe; y a la inversa: cabe la posibilidad de convertir un solo documento físico en varias copias de registros electrónicos, como ocurre con una factura que se convierte en un registro electrónico incluido en un fichero electrónico relativo al proveedor y en otro fichero sobre el producto.

13.4 Modelo de control de acceso

Esta sección describe un único modelo genérico de perfiles de usuario. Este carácter genérico se consigue con una matriz que sólo reconoce dos perfiles de usuario. Esos perfiles (usuario y administrador) se definen en términos de su acceso a las funciones del SGRE.

El perfil de administrador supone una simplificación. En las grandes organizaciones, especialmente, las tareas que en esta especificación se atribuyen a los administradores se pueden dividir en varios perfiles que se denominarán «administrador», «gestor de registros», «responsable de registros», «archivero», «gestor de datos», «administrador de TI», etc.

Conviene reparar en que en numerosas ocasiones el papel del administrador se limita a llevar a la práctica, desde el punto de vista del sistema, las decisiones adoptadas por los directivos superiores, de conformidad con la legislación y las normas aplicables, como las leyes sobre información, seguridad de datos y archivos o la normativa industrial. A tal respecto, consúltese la sección 11.5. Esta matriz no significa que los administradores hayan de tomar decisiones sobre la gestión, si bien esto puede suceder en ciertos entornos.

A grandes rasgos, los usuarios tienen acceso a los instrumentos que un empleado de oficina o un investigador necesitan cuando utilizan los registros. Ello abarca la adición de documentos y la búsqueda y recuperación de registros; su interés se centra en el contenido de los registros. Por su parte, los administradores se ocupan de la gestión de los registros en sí, por lo que su interés se centra en los registros en tanto que entidades, más que en su contenido. Asimismo, se encargan de la gestión del hardware, el software y el almacenamiento del SGRE, se cercioran de que se realicen las copias de seguridad y verifican el rendimiento del sistema.

En la siguiente tabla,

- SÍ indica que el SGRE debe admitir esa combinación de perfiles y funciones.
- NO significa que el SGRE debe evitar esa combinación de perfiles y funciones.
- FACULTATIVO implica que el SGRE puede admitir o evitar esa combinación de perfiles y funciones. Quien decidirá si sus procedimientos admiten o no tal combinación será la organización que utilice el sistema.

Obsérvese que la matriz se divide en dos secciones. Tales secciones agrupan, por criterios de conveniencia, las funciones normalmente asociadas a los ficheros, a los registros y a la gestión y administración de registros

Conviene considerar esta matriz como un punto de partida, la base formal desde la que se asignarán los derechos. Los usuarios de la presente especificación deberán tener en cuenta requisitos adicionales propios de su entorno. Así, en ciertos medios pueden existir perfiles de «revisor de registros» independientes de los perfiles de administrador. En este caso, habrá que especificar los controles de acceso de tal perfil.

Matriz de acceso

	Perfil de usuario	
Función	**Usuario**	**Administrador**
Creación de nuevos ficheros	FACULTATIVO	SÍ
Mantenimiento de los ficheros y del sistema de clasificación	NO	SÍ
Borrado de ficheros	NO	SÍ
Captura de registros	SÍ	SÍ
Búsqueda y lectura de registros	SÍ[2]	SÍ[2]
Modificación del contenido de los registros	NO	NO[3]
Modificación de los metadatos de los registros	NO	SÍ
Borrado de registros	NO	SÍ
Calendario de conservación y operaciones de eliminación	NO	SÍ
Exportación e importación de ficheros y registros	NO	SÍ
Visualización de la pista de auditoría	FACULTATIVO	SÍ
Modificación de la pista de auditoría	NO	NO
Traslado de la pista de auditoría a medios de almacenamiento fuera de línea	NO	SÍ
Realización de todas las transacciones relacionadas con los usuarios y sus privilegios de acceso	NO	SÍ
Mantenimiento de la base de datos y del almacenamiento	NO	SÍ
Mantenimiento de otros parámetros del sistema	NO	SÍ
Definición y visualización de otros informes del sistema	NO	SÍ

2 Previo cumplimiento de los derechos de acceso de los documentos individuales.

3 Excepto en la redacción (véase la sección 9.3).

ANEXOS

Anexo 1 – Publicaciones de referencia

La presente especificación se ha elaborado tomando como base las siguientes especificaciones y modelos de referencia.

Ref.	Nombre, propietario o fuente	Dirección de Internet o datos de la publicación
[1]	Dublin Core Metadata Element Set (Elementos del conjunto de metadatos de Dublin Core): Descripción de Referencia. Versión 1.1.	http://purl.oclc.org/dc/documents/rec-dces-19990702.htm o http://mirrored.ukoln.ac.uk/dc/
[2]	Functional Requirements for Electronic Records Management Systems (Requisitos funcionales de los SGRE), GB Public Record Office.	http://www.pro.gov.uk/recordsmanagement/eros/invest/default.htm
[3]	Functional Requirements for Evidence in Record Keeping (Requisitos funcionales para las pruebas de la conservación de registros), US University of Pittsburgh.	http://www.lis.pitt.edu/~nhprc/
[4]	Guide for Managing Electronic Records from an Archival Perspective (Guía de la gestión de registros electrónicos desde un punto de vista archivístico), Committee on Electronic Records, International Committee On Archives, ICA Study 8.	http://data1.archives.ca/ica/cer/guide_0.html
[5]	Code of Practice for legal admissibility and evidential weight of information stored electronically (Código práctico para la admisibilidad jurídica y fuerza probatoria de la información almacenada en medios electrónicos), British Standards Institution.	Publicado por la British Standards Institution (www.bsi-global.com) como BSI DISC PD 0008
[6]	Guía de la información electrónica (Foro DLM).	http://europa.eu.int/ISPO/dlm/documents/guidelines.html
[7]	ISAD (G) Norma Internacional para la descripción archivística, segunda edición (Comité de normas descriptivas, Consejo internacional de archivos).	http://www.ica.org/cgi-bin/ica.pl?04_e
[8]	The Preservation of the Integrity of Electronic Records (Conservación de la integridad de los registros electrónicos), UBC-MAS Project, University of British Columbia.	http://www.slais.ubc.ca/users/duranti/
[9]	Records Management, ISO 15489 (Gestión de registros, Norma ISO 15480), International Organization for Standardization.	Pendiente de publicación por la Organización Internacional de Normalización; durante la elaboración del presente informe, la norma se encontraba en la fase de proyecto de norma internacional.

Ref.	Nombre, propietario o fuente	Dirección de Internet o datos de la publicación
[10]	Records/Document/Information Management: Integrated Document Management System for the Government of Canada (Gestión de registros, documentos e información: sistema integrado de gestión de documentos del Gobierno de Canadá) - Request for Proposal - Requirements (RDIM), – Requisitos (RDIM), National Archives of Canada.	En un principio publicado en 1996 en la dirección de Internet http://www.archives.ca/06/4rdims.pdf; En la actualidad puede no estar disponible. Véase también http://www.rdims.gc.ca/
[11]	Standard 5015.2 «Design Criteria Standard For Electronic Records Management Software Applications» (Norma 5015.2 Norma sobre los criterios de diseño en las aplicaciones del software de gestión de registros electrónicos), US Department of Defense).	http://jitc.fhu.disa.mil/recmgt/

Anexo 2 – Desarrollo de la presente especificación

La Comisión Europea encargó el desarrollo de la presente especificación MoReq a Cornwell Affiliates plc, una empresa de consultoría con sede en el Reino Unido. El equipo encargado del proyecto contaba con consultores especializados, que han sido los autores de la especificación, y con un grupo de expertos en gestión de registros procedentes de diversos países. Para más información sobre los autores y los colaboradores, véase la parte 1 del Anexo 4.

El proyecto comenzó con la celebración de una reunión en Londres en la que participó todo el equipo. En ella se fijaron los protocolos de trabajo y demás principios y se identificaron ciertas referencias clave. Ésta fue la única vez que se reunieron todos los componentes del equipo. Durante el resto del proyecto, la gestión se llevó a cabo casi exclusivamente por correo electrónico.

La siguiente fase se dedicó a la investigación teórica y a la búsqueda y obtención de las correspondientes obras de referencia. Los consultores examinaron tales referencias y elaboraron la lista de las publicaciones utilizadas, que consta en el Anexo 1.

El siguiente paso consistió en el análisis de la estructura y el contenido de las referencias seleccionadas. Tras compararlas se elaboró un primer esquema basado en la estructura que se deducía de los índices de las referencias.

A partir de ese momento, los consultores empezaron a redactar el borrador de la especificación utilizando como base ese esquema inicial. Revisaron todas las referencias, casi siempre línea por línea, cerciorándose de que todos los requisitos, implícitos o explícitos, quedaban incluidos en el modelo de requisitos. Esta primera elaboración supuso una leve evolución del esquema inicial que continuó a lo largo de todo el proyecto, a medida que se descubrían criterios más lógicos de agrupación de requisitos.

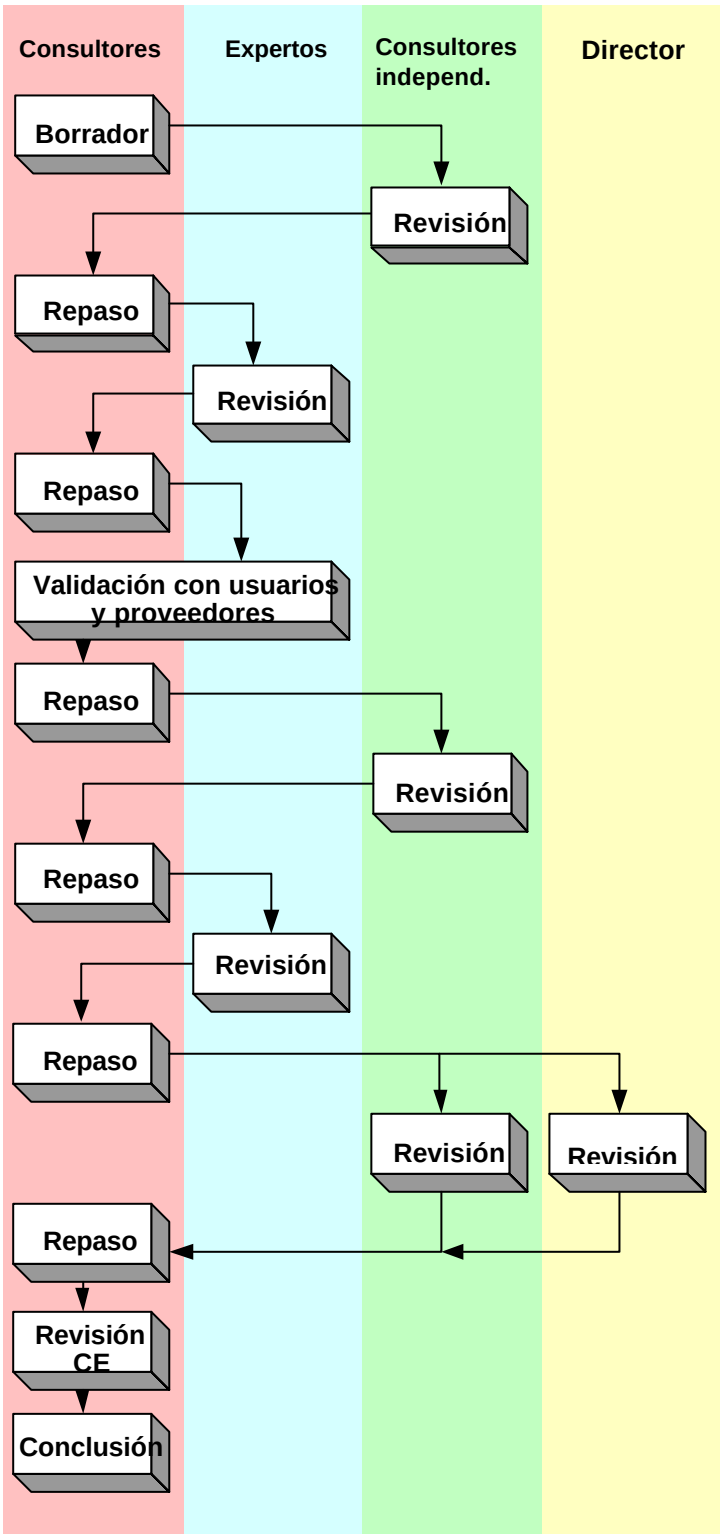
A continuación, el primer borrador se sometió a la primera de varias revisiones, como inicio de un ciclo tradicional de repaso y revisión. Dicho ciclo comprendía cinco tipos de revisiones:

- Intercambios, de forma que cada consultor revisase el trabajo de otro.
- Revisiones realizadas por un experto semiindependiente en gestión de registros completamente ajeno al debate. En especial, este experto se encargó de conciliar los borradores iniciales con las publicaciones de referencia.
- Revisiones realizadas por un grupo de expertos internacionales.
- Revisiones realizadas por el funcionario de la Comisión responsable del proyecto.
- Revisiones para el aseguramiento de la de calidad realizadas por el director del proyecto en Cornwell Affiliates plc.

Durante todo este ciclo se produjo un intercambio constante de ideas, comentarios, etc. entre los expertos y los consultores.

Una vez hubo concluida la práctica totalidad de la especificación, comenzó el proceso formal de validación. Se elaboró un cuestionario que, junto con el borrador de especificación, se remitió a los proveedores de los SGRE y a gestores de registros de las muchas organizaciones que habían ofrecido su colaboración desinteresada (véase la parte 2 del Anexo 4). Todos ellos revisaron el producto para adaptarlo a los productos existentes y potenciar su facilidad de uso en el contexto de su organización.

En el siguiente gráfico de flujo se ilustra de todo el proceso.


Consultores
Expertos
Consultores independ.
Director
Borrador
Revisión
Repaso
Revisión
Repaso
Validación con usuarios y proveedores
Repaso
Revisión
Repaso
Revisión
Repaso
Revisión
Revisión
Repaso
Revisión CE
Conclusión

Anexo 3 - Uso de la versión electrónica de esta especificación

Esta especificación se ha preparado de modo que pueda ser utilizada tanto en papel como en su versión electrónica. Se ha elaborado con Microsoft® Word 97.

La principal ventaja que presenta la utilización de la versión electrónica es su fácil personalización.

Todas las referencias son hipervínculos a los que se puede acceder con un simple clic del ratón. Así, en la frase «véase la sección 13.1 del Glosario», tanto el número como el nombre de la sección son hipervínculos.

Los requisitos se presentan en forma de tabla, colocando un requisito en cada fila, como ilustra la siguiente figura.

Las tablas se dividen en tres columnas:

- **Número.** El número de referencia del requisito que le asigna Microsoft Word de forma automática, pues, al usarse un estilo de «epígrafe», cuando se añaden capítulos, secciones o requisitos la numeración cambia por sí sola.
- **Requisito.** La descripción del requisito, en la que se usa siempre el verbo «deber» para designar un requisito preceptivo y el verbo «convenir» cuando se trata de un requisito facultativo.
- **Columna vacía.** Se puede emplear para calificar propuestas en una licitación o bien para añadir criterios de ponderación adicionales o cualquier otra información. Se puede ampliar, reducir o borrar. Hace uso del estilo «Mand/Des» de Microsoft Word

Téngase en cuenta que cuando se borre algún capítulo, sección o requisito, Microsoft Word sustituirá cualquier referencia a ellos, de existir alguna, con un mensaje de error. Tal mensaje se puede localizar buscando el texto «**¡Error!**» Conviene tener especialmente en cuenta esta cuestión en relación con el capítulo 12 (REQUISITOS DE LOS METADATOS), que incluye numerosas referencias.

Los bordes de las tablas no son visibles por defecto, pero se pueden ver si se selecciona la opción «Mostrar líneas de división».

En el capítulo 12 se emplea una variación de la tabla antes indicada. Se introduce una columna adicional que remite a la exposición de los requisitos. Tales referencias son hipervínculos que llevan a los requisitos.

Anexo 4 - Agradecimientos

1 Equipo encargado del proyecto

Los autores de la especificación son:

- Marc Fresko
- Martin Waldron

con la revisión y las aportaciones de los especialistas enumerados a continuación:

- Francisco Barbedo, Archivo Nacional de Oporto (Portugal).
- Keith Batchelor, consultor independiente (Reino Unido).
- Nils Brübach, Escuela de Archiveros, Marburg (Alemania).
- Miguel Camacho, SADIEL S.A. (España).
- Luciana Duranti, Escuela de Biblioteconomía y Documentación, Universidad de British Columbia (Canadá).
- Mariella Guercio, Universidad de Urbino, Instituto de Biblioteconomía y Archivística (Italia).
- Peter Horsman, Instituto de educación e investigación en materia de archivos de los Países Bajos (Países Bajos).
- Jean-Pierre Teil, Archivo Nacional (Francia).

De la dirección del proyecto se han encargado Keith Cornwell, Director General de Cornwell Affiliates plc, y Paul E. Murphy, funcionario de la DG Empresa, responsable del proyecto en el marco del programa IDA de la Comisión Europea.

Agradecemos a Sue Wallis, Jane Burnand y Neil Grosse, de Cornwell Affiliates plc, su apoyo administrativo.

2 Organizaciones de validación

El equipo encargado del proyecto agradece a las siguientes organizaciones su amable colaboración en el proceso de validación:

Empresa	**Tipo de organización**	**País**
Pfizer	Fabricante farmacéutico	Reino Unido
DERA	Organismo de defensa	Reino Unido
HM Treasury	Gobierno central	Reino Unido
Tower Technology	Proveedor de SGRE	Reino Unido
Technostock	Consultoría	España
Ministerio de Justicia	Gobierno central	Italia

3 Marcas registradas

Todas las marcas registradas citadas en la presente especificación pertenecen a sus respectivos propietarios. Los productos se mencionan únicamente a título ilustrativo y su inclusión no supone recomendación alguna, del mismo modo que la exclusión de otros productos no implica crítica alguna.

Anexo 5 - Correspondencia con otros modelos

1 Correspondencia con el Modelo de Metadatos de Dublin Core

Los elementos de metadatos descritos en el capítulo 12 reflejan el conjunto de elementos de metadatos del modelo de Dublin Core (véase la referencia [1] del Anexo 1). En la siguiente tabla se presenta, a título informativo, una posible correspondencia.

	MoReq	
Nombre del elemento del modelo Dublin Core	**Números de los requisitos**	**Descripción del elemento**
Título	12.7.1	Identificador
Autor	12.7.3	Autor
Claves	12.4.2 12.4.3 12.4.22 12.7.2	Nombre Ref. palabras clave descriptivas. Nombre basado en una palabra clave Tema
Descripción	12.4.4	Descripción
Editor	-	No existe
Otros colaboradores	-	No existe
Fecha	12.7.5 12.7.8 12.7.22 12.7.23	Fecha y hora Fecha y hora de la grabación Fecha de envío Fecha de recepción
Tipo	12.7.7	Tipo de registro
Formato	12.7.13	Metadatos de conservación
Identificador	12.7.1	Identificador único
Fuente	12.8.2	Identificador del registro original (cuando se trate de extractos)
Lengua	-	No existe
Relación	12.7.24	Vínculos con los registros relacionados

	MoReq	
Nombre del elemento del modelo Dublin Core	**Números de los requisitos**	**Descripción del elemento**
Cobertura	-	No existe
Derechos	12.7.25	Restricciones derivadas de la propiedad intelectual

2 Correspondencia con el modelo de metadatos de Pittsburgh

Los elementos de los metadatos descritos en el capítulo 12 reflejan el modelo de metadatos de Pittsburgh (véase la referencia [9] del Anexo 1). En la tabla se muestra una posible correspondencia, a título ilustrativo. No obstante, tal correspondencia no es exacta, debido a las diferencias existentes entre MoReq y el estudio de Pittsburgh en cuanto a paradigmas y centros de atención. Por consiguiente, algunas de las correspondencias indicadas pueden depender de la interpretación realizada.

	Modelo de requisitos	
Descripción del modelo de Pittsburgh	**Números del requisito**	**Descripción del elemento**
Dimensión de gestión		
Registro	12.7.1 12.7.8	Identificador Fecha y hora
Identificador del registro	12.7.1	Identificador
Información sobre el descubrimiento y la recuperación	12.4.2 12.4.3 12.4.22 12.7.2	Nombre Referencias a palabras clave Palabras clave Tema
Dimensión de los términos y condiciones		
Estado de los derechos	12.4.8 12.4.9 12.4.10 12.7.9 12.7.10 12.7.11	Derechos de acceso de los grupos de usuarios Derechos de acceso de los usuarios Categoría de seguridad Derechos de acceso de los grupos de usuarios Derechos de acceso de los usuarios Categoría de seguridad

	Modelo de requisitos	
Descripción del modelo de Pittsburgh	**Números del requisito**	**Descripción del elemento**
Acceso	12.7.25 12.4.21	Restricciones derivadas de la propiedad intelectual Información sobre otros accesos
Uso	-	No existe
Conservación	12.4.17 12.5.1	Calendario de conservación Calendario de conservación
Dimensión estructural		
Identificación del fichero	-	No existe
Codificación del fichero	12.7.20 12.7.21 12.7.28 12.7.29	Firmas electrónicas (etc.) Autenticación de las firmas electrónicas Información sobre la encriptación Información sobre la filigrana electrónica
Reproducción del fichero	12.7.13	Metadatos de conservación
Reproducción del registro	12.7.13	Metadatos de conservación
Estructura del contenido	-	No existe
Fuente	12.7.27	Idioma

Anexo 6 - Procesamiento de la fecha

El SGRE debe procesar todas las fechas correctamente, con independencia del milenio, siglo o cualquier otra cuestión relacionada con la representación (véase 11.5.1). Este anexo presenta una exposición del requisito sobre el tratamiento de las fechas afectadas por el efecto 2000 que en caso necesario se puede adaptar a otras fechas. Esta norma es de especial pertinencia en los SGRE que pueden guardar entre sus metadatos las fechas de siglos anteriores o futuros.

El texto siguiente es una reproducción exacta y autorizada del Documento DISC PD2000-1:1998 de la BSI «Una definición de los requisitos de conformidad para el año 2000».

La conformidad con el año 2000 es la garantía de que la calidad de funcionamiento y la funcionalidad no se verán afectadas por las fechas, antes, durante ni después del año 2000.

En particular:

Regla 1 Ningún valor que se utilice para representar la fecha corriente ocasionará la interrupción de las operaciones.

Regla 2 La funcionalidad basada en las fechas debe mantenerse constante antes, durante y después del año 2000.

Regla 3 En todas las interfaces y los dispositivos de almacenamiento de datos, las fechas deben incluir el siglo, explícitamente o mediante un algoritmo inequívoco o reglas de inferencia.

Regla 4 El año 2000 debe reconocerse como año bisiesto.

.

Anexo 7 – Normas y otras orientaciones

En el presente anexo se enumeran las normas y otros recursos a los que se hace referencia en la especificación.

1 Normas

BS 4783
: Almacenamiento, transporte y mantenimiento de soportes para su uso en el tratamiento de datos y el almacenamiento de información (en varias partes).

BS 7978
: Integración para la conservación indefinida de documentos electrónicos y sus objetos asociados.

ISO 639
: Códigos para la representación de los nombres de lenguas.

ISO 3166
: Códigos para la representación de los nombres de los países.

ISO 8601
: Elementos de datos y formatos de intercambio - Intercambio de información - Representación de fechas y horas.

ISO 8859
: Tratamiento de la información; juegos de caracteres gráficos de 8 bits-byte.

ISO 9075
: Tecnologías de la información - Lenguajes de bases de datos - SQL.

ISO 10646
: Tecnologías de la información; juego universal de caracteres codificados en varios octetos.

ISO 23950
: Recuperación de información - Definición de servicio de aplicaciones y especificación de protocolos.

2 Otras directrices

90/270/CEE
: Directiva 90/270/CEE del Consejo, de 29 de mayo de 1990, referente a las disposiciones mínimas de seguridad y de salud relativas al trabajo con equipos que incluyen pantallas de visualización.

BSI DISC PD 0008
Código práctico para la admisibilidad jurídica y la fuerza probatoria de información almacenada en medios electrónicos.

BSI DISC PD2000-1:1998
Una definición de los requisitos de conformidad para el año 2000. (Disponible en la dirección de Internet: http://www.bsi.global.com).

3 Directrices sobre accesibilidad

Iniciativa SPRITE-S2
ACCENT – Apoyo y guía en la adquisición de sistemas y servicios de información y de telecomunicaciones
(http://www.statskontoret.se/accenteng.htm)

W3C Pautas de Accesibilidad del Contenido en la Web
(http://www.w3.org/TR/WAI-WEBCONTENT)

Directrices oficiales de Microsoft para desarrolladores y diseñadores de interfaces de usuario.
Capitulo 15, Consideraciones especiales sobre el diseño y la accesibilidad
(http://msdn.microsoft.com/library/books/winguide/ch15c.htm)

4 Directrices sobre la conservación a largo plazo

Proyecto InterPARES (http://www.interpares.org)

Proyecto PADI: Conservación del acceso a la información digital.
Biblioteca Nacional de Australia (http://www.nla.gov.au/padi/).

Public Record Office del Reino Unido
Guía sobre la gestión, evaluación y conservación de registros electrónicos. En particular véase el capítulo 5 del volumen 2.
(http://www.pro.gov.uk/recordsmanagement/eros/guidelines/default.htm).

Modelo de referencia para un sistema abierto de información sobre archivos.
Borrador que pretende convertirse en norma ISO. Durante la elaboración de la presente especificación podía consultarse en la dirección de Internet http://www.ccsds.org/documents/pdf/CCSDS-650.0-R-1.pdf