Revista Andaluza de Archivos

La conservación a largo plazo de documentos electrónicos: normativa ISO y esfuerzos nacionales e internacionales

Alejandro Delgado Gómez
Servicio de Archivo y Bibliotecas del Ayuntamiento de Cartagena
3000 Informática
Archivo Municipal. Plaza del General López Pinto s/n. 30201-Cartagena
alejandro@ayto-cartagena.es

Resumen

Ponencia presentada en las Jornadas sobre *Normalización en la Gestión de los Documentos en los Archivos* celebradas en Sevilla entre los días 24 y 26 de septiembre de 2007. Tras ofrecer una definición de la noción de documentos digitales y establecer unos criterios para la conservación de los documentos electrónicos, se abordan las principales iniciativas desarrolladas en este sentido por la ISO: La norma *ISO-15489* y los informes técnicos *ISO/TR 15801:2004: recomendaciones para la veracidad y fiabilidad de información almacenada electrónicamente* e *ISO/TR 18492:2005: conservación a largo plazo de información electrónica basada en documentos*, por último se hacen dos recensiones sobre la norma *ISO 19005-1:2005: PDF/A-1* y el borrador *ISO/NP 26102:Requisitos para la conservación a largo plazo de documentos electrónicos*.

Abstract

Speech given at the Conferences on Standardization of Archival Document Management, held in Sevilla, 24-26 September 2007. After presenting a definition of the basics on digital documents and setting the criteria for the preservation of electronic documents, the following initiatives, developed by the ISO within this context, were addressed: The technical standard *ISO-15489* and technical reports *ISO/TR 15801:2004: Electronic imaging -- Information stored electronically -- Recommendations for trustworthiness and reliability* and *ISO/TR 18492:2005: Long-term preservation of electronic document-based information*, and finally, two critical revisions of the standard *ISO 19005-1:2005: PDF/A-1* and rough draft *ISO/NP 26102: – Information and Documentation – Requirements for Long-Term Preservation of Electronic Records*.

Palabras clave: Normalización, Preservación digital, Gestión electrónica de documentos, Patrimonio documental

Keywords: Standardization, Digital Preservation, Electronic Recordkeeping, Documentary Heritage

1. Introducción

La presente exposición se aplica a la descripción de algunos de los esfuerzos de la Organización Internacional de Normalización (ISO) en lo relativo a la conservación de documentos electrónicos de archivo. Puesto que, a nuestro juicio, estos esfuerzos son, por una parte, aún insuficientes, como intentaremos explicar a lo largo de la exposición; y, por otra, se inscriben en el contexto más amplio de los numerosos proyectos de conservación digital emprendidos por gobiernos, universidades y otras instituciones públicas y privadas, tanto a nivel nacional como internacional, haremos mención también, bien que de manera breve, a algunos de estos proyectos, particularmente los que se adecuan a criterios que en general están siendo considerados como más adecuados que otros, y que indicamos más adelante.

En primer lugar, procedemos a un intento de definición de documento electrónico de archivo y de conservación a largo plazo. A pesar de la exclusividad de ambos conceptos, que daría pie para una discusión de al menos las cuatro horas que dura esta sesión, proponemos, con fines puramente prácticos, definiciones convencionales sobre las que se podría concebir un alto grado de acuerdo. En segundo lugar, y también con el apoyo de garantía literaria suficiente, procedemos a sugerir algunos criterios que podrían utilizarse para dilucidar los motivos por los que ciertas nociones de conservación de documentos electrónicos son mejores que otras. En tercer lugar, intentamos hacer frente a algunos de los esfuerzos normativos de ISO, particularmente aquellos que en su momento el Grupo de Trabajo Conjunto (JWG) del Subcomité 3 (SC3) del Comité 171 (TC171) y el Subcomité 11 (SC11) del Comité 46 (TC46) de ISO consideraron como centrales para el empeño de la conservación digital. Nos enfocamos de manera específica sobre ISO/TR 15801, ISO/TR 18492, y, de manera breve, puesto que es cualitativamente distinta, a ISO 19005/A, que por lo demás son los esfuerzos sobre los que está trabajando el Subcomité 1 (SC1) del Comité 50 (CTN50) de Aenor. En el mismo bloque hacemos mención al proyecto normativo ISO/TR 26102, abordado por el citado SC11, y que en el momento de redactar la presente exposición se encuentra aún muy lejos, en nuestra opinión, de ver la luz como norma consolidada. Aunque a lo largo de la exposición de estos documentos intentamos centrarnos en su contenido, eludiendo las valoraciones críticas, también intentamos ponderar, a la luz de otros proyectos, el valor archivístico, mayor o menor, de cada una de las normas citadas. Estos proyectos son, por ejemplo, el marco conceptual de alto nivel de los proyectos Internares (1), el testbed Digital Longevity del Archivo Nacional de Holanda (2), las recomendaciones prácticas del proyecto ExpertiseCentrum eDavid (3), o la implantación específica de un método de conservación en el Archivo Nacional de Australia, mediante herramientas libres como DPR, Xena y Quest (4). Se trata simplemente de muestras seleccionadas entre los múltiples proyectos de conservación digital emprendidos por diversas instituciones, algunos de los cuales tienen reflejo, o han sido tomados en consideración por, las normas citadas. Por último, exponemos algunas conclusiones que, siempre a nuestro juicio, pueden resultar de utilidad.

2. Definición de documento electrónico y de conservación a largo plazo

Como se indicó, en la actualidad existen tantas definiciones de documento electrónico y de conservación a largo plazo como paradigmas, escuelas de pensamiento o corrientes de práctica. Su discusión consumiría un tiempo del que carecemos, por lo que haremos uso de definiciones convencionales, asumiendo que existe un alto grado de acuerdo acerca de las mismas.

Así, el Proyecto InterPARES define, de manera neutra, el documento electrónico u objeto a conservar como "un documento analógico o digital que es portado por un conductos eléctrico y

requiere el uso de un equipo para ser inteligible por una persona" (5). Un documento digital, de acuerdo con el mismo proyecto, se define como "un documento cuyo contenido y forma se codifican utilizando valores numéricos discretos (tales como los valores binarios 0 y 1), más que un espectro continuo de valores (como los generados por un sistema analógico)" (6). Estas definiciones son lo suficientemente neutrales como para permitirnos percibir el amplio y diverso rango de objetos que se esconden tras la aparentemente única noción de documento electrónico: un documento redactado mediante procesador de textos, el PDF de ese documento, una hoja de cálculo, una firma (creada según diversos procedimientos) para validar aquel documento, un correo electrónico, una tarjeta de crédito, otra firma sobre una PDA sin teclado, un sitio web o ciertos componentes o páginas de ese sitio web, dependiendo de la perspectiva que se adopte; una base de datos, compuesta de tablas, instrucciones SQL, vistas, índices, etc.; un conjunto de bases de datos conectadas; un schema XML y las referencias al mismo desde aquel sitio web; una grabación de video o de sonido digitales; un sistema de posicionamiento geográfico o un sistema de georeferencia; un sistema de realidad virtual, un juego interactivo, etc. En realidad, no existe nada similar al "documento electrónico" en nuestro complejo siglo veintiuno: aquello a lo que llamamos documento electrónico está constituido por una amplia diversidad de objetos muy disímiles, para cuya conservación probablemente será preciso aplicar criterios específicos. No obstante, estos criterios específicos, como intentaremos explicar a lo largo de la presente exposición, debieran apoyarse en modelos conceptuales de alto nivel que garantizaran que, al menos, se está obrando de acuerdo con normas, políticas y estrategias bien acordadas y probadas.

Es en este sentido en el que el citado proyecto InterPARES define el término conservación: "El todo de principios, políticas y estrategias que controla las actividades diseñadas para asegurar la estabilización física y tecnológica de los materiales (datos, documentos o documentos de archivo) y la protección de su contenido intelectual" (7).

Por supuesto, más allá de estas declaraciones genéricas, el esfuerzo de conservación debe reflejarse en implantaciones prácticas específicas. Con todo, como se ha dicho, estas implantaciones prácticas deben basarse en modelos de amplio alcance cuyos criterios de valoración abordamos en lo que sigue.

3. Criterios para valorar los modelos de amplio alcance de conservación a largo plazo

En la presente exposición adoptamos el punto de vista de que los documentos electrónicos no se diferencian, en cuanto a su finalidad, de los documentos analógicos; es decir, los documentos electrónicos deben conservarse como evidencia de actos a efectos de responsabilidad y memoria, manteniendo propiedades que, por convención, podrían ser las indicadas para cualquier tipo de documento en la norma ISO 15489, es decir, un documento electrónico de archivo debe ser auténtico, fiable, íntegro y disponible (8). Este debiera ser el primer criterio para ponderar un marco de amplio alcance, es decir, su capacidad para conservar la evidencia asociada a los documentos electrónicos, conservando sus propiedades fundamentales.

A pesar de que sus finalidades son idénticas, los documentos electrónicos se diferencian de los documentos analógicos, principalmente, y desde el punto de vista archivístico, por el hecho de que, tal y como indicara David Bearman, son entidades lógicas, no físicas (9). Por supuesto, dicha afirmación no puede pasar sin discusión. En realidad, los documentos electrónicos no sólo son entidades lógicas; también son entidades físicas (de lo contrario, como asevera Luciana Duranti, no haría falta conservarlos) (10), y, en la articulación de Kenneth Thibodeau, también entidades conceptuales. De acuerdo con esta articulación, "un objeto físico es

simplemente una inscripción de signos sobre algún soporte físico. Un objeto lógico es un objeto que es reconocido y procesado por un software. El objeto conceptual es el objeto tal y como es reconocido y comprendido por una persona, o en algunos casos reconocido y procesado por una aplicación informática capaz de ejecutar transacciones" (11).

Lo que significa la afirmación, por parte de David Bearman, de que los documentos electrónicos son entidades lógicas no es que carezcan de componentes físicos y conceptuales, sino más bien que estos otros componentes son en gran medida de fácil conservación, o al menos de conservación mucho menos difícil que la de los componentes lógicos, a efectos de conservación. Los componentes conceptuales son un resultado del proceso de conservación, no el objeto mismo del proceso; es decir, conservamos documentos electrónicos para que una persona o aplicación pueda recuperarlos de manera reconocible y hacer uso de ellos, a partir de una adecuada política de conservación de los componentes físicos y lógicos. Por su parte, la conservación de los componentes físicos es similar a la de los documentos analógicos: simplemente se inscriben los datos sobre el soporte que en cada momento goce de mejor reputación –un CD-ROM, un DVD, un disco duro externo- y se "almacenan" estos soportes en condiciones de temperatura, humedad, etc., adecuadas. Desde una perspectiva positivista, tal y como la que se deriva de algunas propuestas anteriores de ISO y, en cualquier caso, de la percepción de parte de la profesión informática, esto debiera ser suficiente. Sin embargo, y es en este sentido en el que la afirmación pionera de Bearman resulta crucial, la mera conservación de datos, sin la conservación de la lógica que rigió su comportamiento y uso, devuelve un resultado carente de significado y, por tanto, inutilizable.

Por ejemplo, nuestro Centro de Proceso de Datos inició una política de transferencia de sus bases de datos al Archivo consistente en el envío de CD-ROM's que contenían ficheros dmp. Los datos estaban ciertamente allí, y el Archivo podía conservarlos en adecuadas condiciones de temperatura y humedad, e incluso proceder a una política de refresco de soportes en períodos normalizados. Sin embargo, para saber qué contenían, era necesario abrir tales ficheros dmp con un software propietario cuya durabilidad se desconocía, y, una vez abiertos, era imposible saber qué significaban los datos de las tablas, porque se ignoraba la aplicación de la que procedían, el comportamiento o la funcionalidad de tales datos en esa aplicación, e incluso el significado del nombre de los campos.

Para conservar estos datos de manera significativa, el Archivo ha emprendido, en colaboración con el Centro de Proceso de Datos, la elaboración de un protocolo de conservación de documentos electrónicos basado en el Testbed Digital Longevity, del Archivo Nacional de Holanda (12), y que implica la conservación de los tres componentes convencionales de todo documento –contenido, contexto y estructura-, además de los componentes derivados de su carácter electrónico, es decir, la forma (13) o representación y el comportamiento o lógica. Por tanto, un segundo criterio para ponderar los modelos conceptuales en uso será su capacidad para conservar inextricablemente vinculados, todos los componentes del documento electrónico: contenido, contexto, estructura, forma y comportamiento. Este, por otra parte, parece ser también el punto de vista en el excelente y exhaustivo trabajo del especialista Ross Harvey: en un entorno electrónico no conservamos artefactos, conservamos información (14).

Por último, como tercer criterio, y contra una creencia bastante generalizada en nuestra sociedad y en nuestros entornos de trabajo, la tecnología no lo puede hacer todo, no hace nada parecido a la magia. Como ha indicado, desde el propio punto de vista de la tecnología, Clifford Lynch, en lo que concierne a la fiabilidad de los documentos electrónicos conservados, la tecnología puede ciertamente hacer muchas cosas, pero, en último extremo, la fiabilidad de un documento electrónico conservado depende del grado de confianza que una sociedad determinada esté dispuesta a asumir (15).

Esto no es nuevo, por supuesto, y ha venido sucediendo desde tiempos inmemoriales con los documentos analógicos: las transacciones privadas falsas se convertían en auténticas al cruzar el umbral del *Tabularium* en la Antigua Roma; durante la Edad Media, las partes interesadas en una transacción no requerían el documento "perfecto", para ellas era suficiente que los datos quedaran reflejados en la *imbreviatura* del notario; el papado justificó durante siglos su poder temporal basándose en el estructuralmente válido documento de la Donación de Constantino, cuya falsedad de contenido desveló el humanista italiano Lorenzo Valla, etc. Así, pues, la conservación auténtica de documentos electrónicos no depende sólo de criterios tecnológicos, sino de las condiciones de admisibilidad que una sociedad dada esté dispuesta a asumir (16). En nuestra sociedad, podemos acordar, por convención, y para entornos organizativos, que estas condiciones vienen dadas por ley: por ejemplo, la reciente Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica; el Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos; la Ley 59/2003, de 19 de diciembre, de firma electrónica; y muchas otras disposiciones de distinto rango a las que se puede acceder, por ejemplo, desde el sitio web del Consejo Superior de Administración Electrónica (17).

Establecidos estos criterios de ponderación, por supuesto discutibles pero que proporcionan un marco de referencia, pasemos a considerar algunos de los modelos de amplio alcance, y derivados prácticos de los mismos, enunciados en la introducción de la presente exposición.

4. Los esfuerzos de la Organización Internacional de Normalización (ISO) en lo relacionado con la conservación de documentos electrónicos

En lo que se refiere a la conservación a largo plazo de documentos, tanto analógicos como digitales, los esfuerzos de ISO tienen una larga historia, evidente, por ejemplo, en el trabajo del TC171 (Aplicaciones de gestión de documentos) y sus tres sub-comités (calidad, cuestiones de aplicación y cuestiones generales), más un grupo asesor. Aunque el citado Comité mantiene relaciones, tanto con el TC46 (Información y documentación) como con organismos del estilo del Consejo Internacional de Archivos (ICA) y la Federación Internacional de Asociaciones e Instituciones de Bibliotecas (IFLA), su empeño ha estado siempre más orientado a la conservación del artefacto que a la conservación de la lógica, particularmente en el entorno analógico, como demostrarían, por ejemplo, sus muchas normas acerca de la gestión de la conservación en microformas.

Sin embargo, en fecha reciente, las relaciones entre el TC 171 y el citado SC11 (Gestión de archivos/documentos) ha producido algunos resultados, si no impecables, al menos mejor informados desde el punto de vista archivístico. Así, por ejemplo, el grupo de trabajo conjunto TC171/SC11 produjo un borrador de cuerpo central de normas técnicas a ser tomadas en consideración a efectos de conservación, en el que, junto a normas técnicas especialmente dependientes de la conservación de los datos, incluía las dos partes de ISO 15489, así como dos informes técnicos, ISO/TR 15801 e ISO/TR 18492, que tomaremos en consideración algo más adelante. En la actualidad el grupo de trabajo conjunto está colaborando en el desarrollo de PDF, bajo el mando del SC2 (Cuestiones de aplicación) del TC171.

Por su parte, el SC11 ha producido un borrador de norma archivística acerca de la conservación a largo plazo de documentos electrónicos (18). Sin embargo, como toda norma, precisa de un, a nuestro juicio, todavía largo proceso de depuración, de tal manera que

referirse en este momento a su contenido resulta en el mejor de los casos aventurado. Con todo, y puesto que en algún momento será la norma ISO de conservación archivística de documentos electrónicos, una breve aproximación a su estructura actual, con todas las precauciones que sean del caso, no parece del todo inoportuna.

Analizamos, pues, el contenido de los tres productos normativos del TC171 asociados a la conservación a largo plazo en entornos electrónicos que guardan una relación más estrecha con los requisitos archivísticos de conservación y que en este momento se están considerando de una u otra manera a nivel nacional; así como el actual borrador de norma ISO 26102. Metodológicamente, se expone el contenido de los documentos, atendiendo en el menor grado posible a valoraciones críticas, que esperamos se deriven a lo largo de la exposición de su contraste con otros proyectos marcadamente archivísticos.

5. ISO/TR 15801:2004: recomendaciones para la veracidad y fiabilidad de información almacenada electrónicamente (19)

De acuerdo con la propia justificación del informe técnico que nos ocupa, el uso como evidencia legal de documentación creada, capturada o almacenada de manera electrónica es una realidad creciente. De ello se deriva la necesidad para las organizaciones de gestionar esta documentación electrónica utilizando procedimientos que garanticen su admisibilidad legal. El informe técnico se aplica a la descripción de algunos de estos procedimientos, de manera específica aquellos que se derivan del contexto tecnológico de la documentación. Básicamente, pues, el informe técnico propone las condiciones que se han de dar para garantizar técnicamente que ciertos tipos de documentos electrónicos no se han modificado desde el momento de su creación o captura; así como para garantizar que, si el documento electrónico procede de un documento físico fuente, es una reproducción verdadera y fiable de ese documento fuente.

En cuanto a su alcance, el informe técnico se define adecuado para entornos de sistemas de gestión de la información que almacenan documentación electrónica y en los que las condiciones de veracidad, fiabilidad, autenticidad e integridad son importantes. Es decir, básicamente el informe técnico se aplica a la documentación electrónica que puede ser requerida como evidencia legal en algún momento.

El informe técnico se estructura en una introducción, que establece los principios generales, y ocho capítulos. Los tres primeros capítulos son los convencionales en cualquier documento ISO: alcance, normativa de referencia y vocabulario. Los restantes cinco capítulos se aplican a discutir los principios que deben regir los siguientes aspectos: políticas de gestión de la información, deber de custodia, procedimientos y procesos, tecnologías capacitadoras y pista de auditoría. Estos capítulos tienen un nivel de detalle diferente, siendo los dos primeros de carácter más programático y, por tanto, menos extensos; y los tres últimos de carácter más técnico y, por tanto, más detallados.

El capítulo acerca de políticas de gestión de la información del informe técnico parte de la premisa de que la información es uno de los capitales más importantes de cualquier organización. Como tal, la información tiene que gestionarse –clasificarse, estructurarse, validarse, ser asegurada, ser valorada, supervisarse... El modo en que se gestiona la información debe quedar reflejado en un documento de política de gestión de la información, cuyos requisitos analiza el capítulo 4 del informe técnico.

Un documento de política de gestión de la información debe ser apoyado y aprobado por los niveles más altos de gestión de la organización. De igual modo, debe revisarse

periódicamente. Tal documento debe contener al menos secciones que especifiquen los siguientes aspectos:

- Información cubierta por el documento. Para ello, la información debe agruparse por tipos, de tal manera que la política para toda la información dentro de un tipo sea coherente.
- Política respecto a soportes de almacenamiento. De acuerdo con los requisitos legales de admisibilidad jurídica y con las propias necesidades funcionales de la organización, el documento debe indicar qué soporte de almacenamiento se utilizará para qué requisitos de la organización. Los requisitos son, por ejemplo, las condiciones de acceso, los requisitos de seguridad o los períodos definidos de retención. Cada uno de estos requisitos puede exigir un tipo diferente de soporte de almacenamiento –papel, microforma, CD-ROM- para diferentes etapas de la vida de los documentos.
- Política respecto a formatos de ficheros de imagen y controles de versión. De igual modo, para cada requisito, función o tipo de documento, puede que se requiera un diferente formato de fichero de imagen, así como documentación relevante acerca de políticas de migración y de compresión, y de controles de versión, con el fin de garantizar la usabilidad de los ficheros a largo plazo.
- Política respecto a las normas relevantes de gestión de la información. El documento debiera contemplar toda la normativa relevante, que puede tener carácter legal a nivel nacional o internacional; carácter técnico, o carácter industrial. Un ejemplo sería el cuerpo normativo ISO 9000. Indíquese que la consideración a la normativa de tipo jurídico y técnico es una constante a lo largo de los diferentes capítulos del informe técnico.
- Políticas de retención y destrucción. De acuerdo con el informe técnico, debiera establecerse un programa de retención para cada tipo de documento. En dicho programa debieran participar tanto todos los departamentos relevantes de la organización, como los adecuados asesores legales. El programa de retención debiera aplicarse a toda la documentación producida por la organización, debiera revisarse periódicamente, y debiera prever procedimientos controlados de destrucción.
- Responsabilidades para chequear el cumplimiento de esta política. Finalmente, el documento de política de gestión de la información debe incluir un apartado en el que se defina quiénes son los responsables individuales o corporativos de chequear el cumplimiento de los requisitos establecidos en los anteriores apartados, la admisibilidad legal de tales requisitos, y las revisiones periódicas del documento.

En cuanto al principio de deber de custodia, y de acuerdo con el capítulo 5 del informe técnico, éste se refiere a la responsabilidad de la organización respecto al valor de la información que está almacenando, y debe quedar controlado mediante procedimientos que establezcan una cadena de responsabilidad y asignen responsabilidades para todas las actividades de gestión de la información a todos los niveles; de igual modo, la organización debe ser consciente de los cuerpos legislativos y reguladores pertinentes, así como mantenerse al tanto del desarrollo técnico, procedimental, regulador y legislativo en su área de trabajo. Por último, la organización debe desarrollar e implantar una política de seguridad de la información. Este último deber es especialmente importante, y el informe técnico lo desarrolla del modo que se expone a continuación.

Puesto que toda la información es susceptible de sufrir pérdidas o cambios accidentales o maliciosos, es necesario definir medidas que permitan reducir estos riesgos y proteger la autenticidad de los documentos. Estas medidas tiene que ser coherentes con los niveles de seguridad asignados a los documentos, así como con una evaluación de los riesgos y de los costes asociados a la eliminación de tales riesgos. La definición de medidas de seguridad debe contemplar igualmente la capacidad para disponer de los documentos en cualquier momento y utilizar procesos de copia de seguridad.

Antes de definir una política de seguridad de la información, la organización debiera llevar a cabo un análisis estructurado de riesgos, cruzando variables tales como el valor de la información, la vulnerabilidad del sistema o la probabilidad de un ataque. Una vez descubiertos de manera específica los riesgos que corre la información, es posible redactar un documento donde queden reflejadas las medidas de seguridad a adoptar. En este sentido, el análisis de la política de soportes de almacenamiento y de copia de seguridad resulta esencial.

Igualmente, antes de redactar el plan de seguridad de la información, la organización debiera considerar sus relaciones con otras entidades y atender a los intereses de éstas. Tales organizaciones pueden ser órganos gubernamentales, órganos externos de auditoría, asesores legales, leyes nacionales e internacionales, sector industrial, la comunidad, la organización como un todo, un departamento o un individuo.

De igual modo, la organización debiera considerar la posibilidad de buscar asesoría externa respecto a cuestiones legales, regulaciones administrativas, regulaciones fiscales, o regulaciones especiales. Los resultados de estos análisis externos debieran incorporarse al documento de política de seguridad.

La política de seguridad de la información debe quedar reflejada en un documento que contenga como mínimo los siguientes apartados:

- alcance de la política,
- declaración de los objetivos de gestión con respecto a la seguridad,
- declaraciones específicas de política,
- requisitos de las diferentes categorías de clasificación de la información,
- definición y asignación de responsabilidades respecto a la seguridad de la información,
- política para tratar las brechas en la seguridad, y
- política respecto al cumplimiento de las normas relevantes.

Por lo demás una política de gestión de seguridad de la información debe contar con una infraestructura de seguridad que se plantee los siguientes objetivos:

- aprobación y revisión de la política de seguridad de la información,
- chequeo de las amenazas a la seguridad de la información,
- chequeo y revisión de las brechas en la seguridad, y
- aprobación de las principales iniciativas para mejorar la seguridad de la información.

En relación con la política de seguridad de la información, la organización debe considerar la necesidad de redactar un plan de continuidad de sus actividades, o un plan de recuperación de desastres, que permita seguir trabajando en el supuesto de que aparezca un problema que comprometa el trabajo regular. Por supuesto, este plan de continuidad debe garantizar que la integridad de la información almacenada no puede ponerse en cuestión.

La sección 6 del informe técnico se aplica a los procedimientos y procesos que la organización debiera implantar y revisar. La primera herramienta de la que una organización debe disponer es el manual de procedimientos, en el que queden explicados todos los procedimientos relativos al funcionamiento y uso del sistema. Por supuesto, este manual debe ser rápidamente accesible a todos los usuarios del sistema. De igual modo, la organización debe llevar a cabo los programas de formación necesarios para que su personal entienda y cumpla el manual de procedimientos.

El manual de procedimientos debe contemplar al menos los contenidos que se explican a continuación.

Captura de documentos. Los procedimientos implicados en la captura de imágenes pueden incluir:

- la preparación del documento,
- el batch del documento,
- la fotocopia,
- el escaneado, y
- el control de calidad de la imagen.

Por su parte, los documentos fuente pueden estar en soporte papel o en microforma.

Escaneado de documentos. El informe técnico dedica un buen número de páginas a la definición de recomendaciones para el escaneado de documentos. En lo que se refiere a este procedimiento general, el manual de procedimientos debe incluir recomendaciones acerca de buenas prácticas al menos respecto de los siguientes procedimientos:

- preparación de los documentos,
- batch de los documentos,
- fotocopia,
- escaneado, y
- procesamiento de imágenes.

El informe técnico detalla algunas de tales buenas prácticas para cada uno de los procedimientos, de manera especial aquellas que analizan la calidad de la fuente para obtener un buen resultado, el peligro que pueden sufrir ciertos documentos frágiles si se les somete a estos procesos, gestión de un tratamiento que preserve en la medida de lo posible la autenticidad de los documentos, y control de la calidad de las imágenes.

Captura de datos. Los datos incorporados al sistema pueden ser:

- Por una parte, de nueva creación –tecleados directamente, obtenidos mediante código de barras, OCR/ICR, o mediante procesos combinados. Si bien la exactitud de la captura no siempre se puede garantizar por completo, sí deben definirse recomendaciones para al menos controlar la calidad de los datos capturados, revisar que el nivel de exactitud conseguido se mantiene, y mantener a su vez un registro de estos controles de calidad y exactitud.
- Por lo demás, puede que los datos no sean de nueva creación, sino que procedan de una migración. En este caso debe garantizarse igualmente que los datos se transfieren sin pérdida de integridad, o al menos con pérdidas razonables y, por supuesto, debidamente documentadas.

Indización. En la medida en que es el procedimiento que permite recuperar los documentos, la indización resulta de importancia vital, tanto si se trata de indización manual, automática o combinada. En cualquiera de estos casos, deben documentarse detalladamente los procedimientos en uso, y el índice o los índices debe(n) quedar almacenados al menos durante tanto tiempo como los documentos a los que hacen referencia. De igual modo, las reconstrucciones de los índices y las enmiendas a los mismos deben quedar documentadas. Finalmente, los errores en los índices pueden dar como resultado el que no se pueda recuperar la documentación asociada. Por tanto, el control de calidad de la exactitud de los índices resulta imprescindible.

Procedimientos de salida autenticados. En ocasiones se necesitan copias, en papel o en forma electrónica, de los documentos, a efectos de evidencia legal. Dependiendo de cómo se

obtengan y autentiquen estas copias, cumplirán o no su cometido. Debe tenerse en cuenta que los requisitos legales pueden diferir en distintos contextos, así como el hecho de que lo que resulta aceptable en la práctica cotidiana puede no serlo jurídicamente. En cualquier caso, los procedimientos de autenticación deben quedar documentados.

Transmisión de ficheros. La transmisión de ficheros puede producirse en el interior del sistema o entre el interior y el exterior.

- En el primer caso, se puede hablar de transmisiones en redes de área local, movimientos entre los subsistemas de almacenamiento bajo control del sistema; o transferencias entre subsistemas de almacenamiento bajo control del operador. En cualquier caso, la integridad de los ficheros no debe quedar comprometida durante el proceso de transmisión.
- En lo que se refiere a la transmisión externa, ésta se realiza a través de redes remotas y entre sistemas diferentes. El procedimiento debe garantizar igualmente la integridad de los ficheros transmitidos, ya en tiempo real, ya mediante procesos diferidos como el correo electrónico. El informe técnico establece recomendaciones acerca de la integridad, la no alteración y los metadatos –como la fecha y la hora- del fichero; no acerca del servicio mismo de transmisión.

Retención de la información. Como principio general, debiera respetarse la política de retención de la documentación de la organización. Sin embargo, en algunos casos ciertos documentos deben retenerse durante más tiempo que el establecido en la política general. Algunos ejemplos son un documento fuente de calidad tan pobre que no puede obtenerse una copia legible por máquina; o un documento fuente que se conserva para reducir la posibilidad de que se sugiera que la imagen se hizo deliberadamente ilegible; o un documento físico que contiene notas o enmiendas que no pueden identificarse como tales en la imagen escaneada; o un documento que se encuentra implicado en un litigio en curso.

Destrucción de la información. Los procedimientos para la destrucción de la documentación al final de su período de retención deben quedar documentados. De igual modo, deben incorporar las oportunas medidas de seguridad, adecuadas al nivel de sensibilidad de la información que se destruye. Por último, ningún documento fuente debe destruírse, hasta que haya terminado el proceso de copia en imagen.

Sistema de copia de seguridad y recuperación. El informe técnico proporciona recomendaciones detalladas acerca de los procedimientos y garantías para llevar a cabo procesos de copia de seguridad fiables, recuperables y de los que no se pueda argumentar que no conservan la autenticidad de la información. En general, para permitir el funcionamiento de la organización en el caso de pérdida o corrupción de datos, deben llevarse a cabo periódicamente copias de seguridad de éstos y de sus datos asociados –por ejemplo, índices y pistas de auditoría. Las copias deben almacenarse en línea y fuera de línea, y los procedimientos de recuperación deben quedar debidamente documentados. En el caso de que se produzcan transformaciones estructurales durante el proceso de copia, también deben documentarse. Por último, el sistema debe disponer de herramientas de verificación de la corrección de la copia y de la integridad de los procesos de recuperación.

Mantenimiento del sistema. También deben quedar documentados los procesos de mantenimiento correctivo y preventivo, que deben ser llevados a cabo sólo por personal cualificado y capaz de asegurar que el funcionamiento no se deteriora hasta tal punto que la integridad de los datos capturados, creados o almacenados pueda resultar afectada.

Seguridad y protección. De especial importancia, de acuerdo con el informe técnico, es la gestión del mantenimiento en lo relativo a los sistemas de escaneado y a los procedimientos

de seguridad y protección, incluídos los métodos de encriptación y las firmas digitales, a los que dedica un alto grado de detalle.

Uso de servicios externos. Si se contratan servicios externos, el contrato debe asegurar al menos que los procedimientos usados por el proveedor para garantizar la autenticidad de los documentos son los mismos que hubiera utilizado el cliente; y que el cliente puede demostrar el cumplimiento de los requisitos de autenticidad, incluso muchos años después de que el proveedor haya cesado en sus actividades. Por lo demás, el informe técnico detalla numerosas prácticas procedimentales, muchas de las cuales debieran incorporarse, directamente o editadas, a los contratos de prestación de servicios. Finalmente, el informe toma en consideración tanto el uso de medios de transporte de documentos, como de archivos remotos fiables.

Flujo de tareas. Si la organización incorpora un sistema de flujo de tareas, entendiendo por tal un sistema que facilita la automatización de los procedimientos usados en las actividades de la organización, este sistema debiera quedar documentado, y especificadas las fases del ciclo de vida de la definición de procesos, que incluyen definición, desarrollo, implantación, retirada y modificación.

Marcas de fecha y hora. Deben documentarse los procedimientos para un chequeo regular de los relojes del sistema, a efectos de exactitud de fecha y hora. Los errores en los sistemas de fecha y hora también deben documentarse, y estos procedimientos sólo deben ser llevados a cabo por personal autorizado, aunque el informe técnico considera la posibilidad de contratar los servicios de una tercera parte fiable, en aquellos casos en los que la determinación exacta de la fecha y hora tenga un profundo valor legal.

Control de versión. En lo relativo al control de la versión, el informe técnico aplica tres diferentes puntos de vista:

- Desde el punto de vista de la información, puesto que en el curso de las actividades de la organización pueden generarse distintas versiones de un documento, estas versiones deben quedar claramente identificadas y enlazadas unas con otras.
- Desde el punto de vista de la documentación, cabe la posibilidad de implantar sistemas de control de la versión, de tal manera que siempre queden documentados aspectos como las diferentes versiones realizadas, en qué momento, bajo qué políticas y procedimientos, y cuál es la versión considerada válida en un momento determinado, incluso muchos años después de su realización.
- Desde el punto de vista de los procedimientos y procesos, el informe prescribe que todos ellos debieran implantarse de acuerdo con un procedimiento aprobado de control del cambio.

Mantenimiento de la documentación. Puesto que los requisitos tecnológicos o legislativos pueden cambiar en el curso del tiempo, es preciso llevar a cabo el mantenimiento del manual de procedimientos. Los procedimientos de mantenimiento, por su parte, también deben quedar incluídos en el manual; y los procedimientos que aseguran que la documentación está actualizada deben a su vez documentarse. Por último, estos procedimientos de documentación debieran incorporarse a los procesos de gestión documental de la organización.

El capítulo 7 del informe técnico se aplica a la descripción de las tecnologías que hacen posible la utilización de los procedimientos definidos en los restantes capítulos, y se divide en los siguientes apartados:

Manual de descripción del sistema. El manual de descripción del sistema debe incluir las descripciones de todos los elementos de hardware, software y redes del sistema, así como los

detalles de configuración y el modo en que interactúan. De igual modo, debe detallar cualquier cambio en el sistema.

Consideraciones sobre soportes y subsistemas de almacenamiento. La organización debe tomar en cuenta que, dependiendo de las necesidades funcionales y de los requisitos de autenticidad, almacenamiento, etc., el tipo de subsistema y de soporte de almacenamiento disminuirá o incrementará el riesgo de que los ficheros de imagen almacenados puedan ser modificados de manera inadvertida o maliciosa.

Niveles de acceso. Los diferentes niveles de acceso también deben quedar debidamente documentados en el manual. El informe técnico reconoce como convencionales los siguientes niveles de acceso:

- gestor del sistema,
- administrador del sistema,
- mantenimiento del sistema,
- autores o generadores,
- almacenamiento e indización de la información, y
- recuperación de la información.

Evidentemente, sólo el personal autorizado en cada nivel debe tener acceso a las funciones de ese nivel.

Chequeos de la integridad del sistema. De acuerdo con el informe técnico, deben proporcionarse herramientas, dentro del sistema, que aseguren que la integridad de la información almacenada queda conservada a lo largo de todos los procesos del sistema, incluída la transferencia a y desde los soportes de almacenamiento. El informe detalla, como de especial interés, las herramientas de checksum, así como las firmas digitales y electrónicas, incluídas las llamadas firmas biométricas.

Procesamiento de imágenes. Es posible que, una vez efectuado el escaneado, se lleven a cabo procesos de post-escaneado, a efectos de mejorar la calidad de la imagen, su presentación y posibilidades de salida. Estos procesos se pueden llevar a cabo mediante diversas técnicas de hardware y/o software. Estas técnicas deben utilizarse con precaución, dado que pueden eliminar o alterar aspectos esenciales relacionados con la autenticidad de la imagen; y, en cualquier caso, deben quedar, una vez más, debidamente documentadas.

Técnicas de compresión. El uso de técnicas de compresión para reducir el tamaño de los ficheros, antes o durante su almacenamiento, contribuye a mejorar la eficacia del sistema. El informe técnico menciona los dos tipos básicos de compresión, con y sin pérdida. Con independencia del sistema que se utilice, éste, así como sus atributos, deben quedar documentados de manera cuantitativa, e incluir el algoritmo utilizado para calcular la pérdida. Esta información puede almacenarse como parte del fichero o de sus datos asociados, o en un log independiente.

Incrustación de formularios y eliminación de formularios. Algunas aplicaciones eliminan de manera automática los formularios o plantillas de las imágenes antes de su almacenamiento. Otras los conservan de manera independiente, antes de la construcción del documento. En cualquier caso, en tanto se conserven las imágenes, deben conservarse también identificadores de, y relaciones con, las plantillas o formularios con las que fueron creados, así como una copia de tales plantillas o formularios. De igual modo, debe conservarse el registro de los formularios que fueron eliminados, y este registro debe estar asociado a la imagen.

Consideraciones acerca del entorno. De acuerdo con el informe técnico, la organización debe documentar aspectos tales como las recomendaciones del fabricante del hardware en relación con el entorno operativo de todos los componentes del sistema y de los soportes de almacenamiento; así como los procedimientos de chequeo regular de estos soportes para prever su deterioro y el traslado de la información que contienen.

Migración. En el supuesto de que la información vaya a ser almacenada durante largos períodos de tiempo, es necesario prever los adecuados procesos de migración, desde el comienzo del funcionamiento del sistema. Los procesos de migración, de acuerdo con el informe técnico, pueden implicar tanto cambios de soporte, como cambios de hardware y/o software. El plan de migración debe considerar el uso de formatos de almacenamiento normalizados, así como la migración, no sólo de los ficheros, sino también de sus metadatos, índices y pistas de auditoría, sin pérdida de integridad.

Borrado y/o destrucción de información. El informe técnico dedica un amplio apartado a la definición de buenas prácticas en los procesos de borrado de información, de acuerdo con un programa de retención; al tratamiento de las excepciones; a la destrucción física de los soportes cuando no es posible un simple borrado; y a los procesos de marcado de la información borrada o a borrar.

El informe técnico incorpora un denso capítulo 8, aplicado a la definición de procedimientos de gestión de las pistas de auditoría, de acuerdo con la siguiente estructura.

En lo que se refiere a las consideraciones generales, el informe toma en cuenta las siguientes:

Datos de la pista de auditoría. De acuerdo con el informe técnico, si se precisa de información a efectos de evidencia, será probablemente necesario aportar además información de apoyo, como la fecha de creación o los cambios de soporte. Este tipo de información se almacena en la pista de auditoría, que es el conjunto de datos necesarios para facilitar un registro histórico de todos los eventos significativos asociados a la información almacenada y al sistema de gestión de esa información. En el informe, este tipo de datos se divide en dos categorías: datos sobre el sistema y datos sobre la información almacenada.

Creación. Por principio, la pista de auditoría debiera ser generada automáticamente por el sistema, aunque cabe la posibilidad de que se genere de manera manual. En este caso, incluso más que en el primero, debe quedar documentado el procedimiento de creación.

Fecha y hora. Todos los registros de datos de la pista de auditoría deben tener asociadas una fecha y una hora, que deben ser la fecha y la hora del evento que se almacena en la pista. Por lo demás, la fecha y la hora deben ser lo suficientemente exactas como para que cualquier investigación pueda rastrear el curso de los eventos.

Almacenamiento. En lo referente al almacenamiento de la pista de auditoría, ésta debe conservarse al menos tanto tiempo como la información a la que hace referencia. Además, debe incorporarse como un tipo específico de documento al documento sobre políticas. Por último, debe evitarse que la pista de auditoría se sobreescriba a sí misma una vez alcanzado cierto volumen.

Acceso. De acuerdo con el informe técnico, debe ser posible acceder a los datos de la pista de auditoría sólo en los momentos relevantes, y sólo las personas relevantes, incluídos auditores externos.

Seguridad y protección. Puesto que la pista de auditoría es la garantía de la autenticidad de la información almacenada en el sistema, debe garantizarse la integridad de dicha pista. Es decir:

- los niveles de seguridad en su tratamiento deben ser los adecuados, impidiendo modificaciones,
- deben realizarse copias de seguridad periódicas de la misma,
- debe gestionarse como un documento vital para la organización y de acuerdo con los métodos de gestión documental de ésta, y
- debe almacenarse en soporte externo no re-escribible.

En lo que se refiere al sistema, el informe toma en consideración los siguientes apartados:

Consideraciones generales. Los registros de la pista de auditoría relativos a información sobre el sistema proporcionan datos sobre la pista de auditoría, y sobre los procesos de migración y conversión.

Datos sobre la pista de auditoría. De acuerdo con el informe técnico, para todos los datos de la pista de auditoría del sistema debe ser posible identificar los procesos implicados y la fecha y la hora del evento. Adicionalmente, pueden resultar necesarios otros datos, como la persona que terminó y/o empezó el trabajo, o qué persona preparó qué documentos.

Migración y conversión. En el supuesto de que la información se haya trasladado de un dispositivo de almacenamiento a otro, deben almacenarse en la pista de auditoría los detalles acerca de este proceso de migración. En cualquier caso, debe poder demostrarse mediante la pista de auditoría que cualesquier datos asociados al fichero –como sus metadatos o índices- también han sido migrados sin pérdida de integridad.

En cuanto a la información almacenada, el informe se refiere a:

Consideraciones generales. Los registros de la pista de auditoría relativos a datos sobre la información almacenada proporcionan datos sobre la captura de información, la información en batch, la indización, el control del cambio, el uso de firmas digitales, la destrucción de información y los flujos de tareas.

Captura de información. Los datos almacenados en la pista de auditoría acerca del proceso de captura debieran incluir:

- el momento de la captura,
- la persona,
- el dispositivo de captura, y
- el tipo de original.

Además debieran incluirse detalles acerca de:

- la identificación del documento o fichero,
- el proceso de marca de fecha y hora,
- la referencia al batch,
- el número de páginas o registros de datos,
- la aprobación del chequeo del control de calidad,
- el identificador de cada uno de los ficheros o documentos que se indizaron,
- el identificador del usuario o del puesto de trabajo, y
- el almacenamiento.

Téngase en cuenta que estos datos pueden llegar a ser fundamentales para demostrar la integridad de un documento, de manera que a este respecto la exhaustividad resulta pertinente.

Información en batch. En el caso de que los datos se capturen en batch, el informe técnico recomienda que la pista de auditoría almacene los siguientes datos:

- identificador único del batch,
- identificador de operador,
- tipo de material escaneado,
- cantidad de material en el batch,
- detalles acerca del procesamiento de imagen.

Con estos datos en la pista de auditoría debiera ser posible verificar:

- que se han llevado a cabo todas las actividades requeridas para ese batch,
- que se pueden detectar anomalías,
- que existe un desajuste entre el número de páginas almacenadas y el número de páginas escaneadas,
- que se han completado los procedimientos de control de calidad, y
- que se ha completado el procesamiento de las excepciones.

Indización. La pista de auditoría debe reflejar la fecha y hora de creación, modificación y borrado de un índice; así como un identificador de los documentos o ficheros que han sido indizados. En cualquier caso, estos datos deben servir para demostrar que el índice se ha venido usando correctamente.

Control del cambio. Si se realizan cambios a la información almacenada, la pista de auditoría debe reflejar la naturaleza del cambio, y la persona o programa que lo realizó.

Firmas digitales. En el supuesto de que se utilicen firmas digitales, la pista de auditoría debe conservar los siguientes datos:

- identificación del fichero,
- certificación de la identificación,
- identificación de la autoridad autenticadora,
- fecha y hora de la firma,
- acuse de recibo, y
- prueba de validación.

Destrucción de información. En la pista de auditoría deben conservarse los datos relativos a la destrucción de documentos fuente después del escaneado del documento, la destrucción de información al final del período relevante de retención, y la autorización para esta destrucción.

Flujos de tareas. Si se utilizan sistemas de flujos de tareas, en la pista de auditoría debiera quedar el registro del momento en que se define un nuevo proceso, o en que se cambia una definición existente. Estos son unos datos mínimos, y, dependiendo el nivel de exhaustividad del resto de los datos del sistema de flujo de tareas utilizado, así como de las necesidades de la organización, se puede llegar al extremo de anotar en la pista de auditoría cada paso que se dé en el flujo de tareas.

6. ISO/TR 18492:2005: conservación a largo plazo de información electrónica basada en documentos (20)

Si ISO/TR 15801 aborda la conservación de documentos electrónicos meramente desde el punto de vista del "almacenamiento", con el objetivo de defender intereses organizativos, y para documentos de los que se pueden pensar que tienen un análogo en papel, es decir, documentos que se pueden congelar o de los que se puede obtener una imagen, ISO/TR 18492 va mucho más allá, al concebir, desde su propia introducción un modelo de documento que responde al criterio de ser información registrada, sin especificar el tipo o soporte de documento, que tiene necesidades de recuperación y acceso, igualmente no necesariamente dependientes de los intereses organizativos. Reconociendo tanto el problema de la obsolescencia de hardware, software y soportes, como el enorme volumen de esfuerzos realizados para obtener resultados prácticos en lo que concierne a la conservación de documentos electrónicos a largo plazo, el informe técnico declara como su finalidad la publicación de un marco amplio para el desarrollo homogéneo de políticas y estrategias de conservación. Aunque algunos de sus planteamientos son cuestionables desde el punto de vista archivístico, debe reconocerse la influencia en el informe que nos ocupa de la cooperación con profesionales de la archivística, y su atención a los criterios de ISO 15489.

Como en el caso de ISO/TR 15801, exponemos el contenido de ISO/TR 18492, renunciando provisionalmente a las valoraciones.

Los cuatro primeros capítulos del informe son genéricos, comunes a todas las normas ISO, aunque en este caso resulta de relevancia indicar que la normativa de referencia incluye menciones tanto a las dos partes de ISO 15489 como a la parte en aquel momento aprobada de ISO 23081. Tan relevante o más es la mención a la necesaria cooperación con archiveros. De igual modo, cabe mencionar que el carácter declarado de marco amplio queda reducido, ya en la primera línea del capítulo de alcance, al re-definirse el propio informe como guía metodológica y práctica. Curiosamente, el informe incluye, como anexo no normativo, referencias bibliográficas de distinto tipo, algo que no es muy frecuente en el marco ISO.

El resto del informe se divide en tres densos capítulos (5-7), dedicados, respectivamente, a cuestiones conceptuales acerca de la conservación a largo plazo, la definición de una estrategia de conservación, y el desarrollo de tal estrategia.

El capítulo 5 (Conservación a largo plazo) del informe, comienza con una reflexión acerca de la importancia para las organizaciones, que utilizan de manera creciente evidencia sólo en forma electrónica, de seguir manteniendo accesible la información generada con este fin y de manera fidedigna por diferentes aplicaciones, y de la necesidad de desarrollar estrategias de conservación y recuperación a largo plazo. Para el desarrollo de una estrategia tal, en el mismo capítulo se definen de manera detallada seis componentes clave de la misma.

En primer lugar, la información debe seguir siendo legible en el futuro, lo cual implica cuatro opciones. Partiendo del hecho de que la información electrónica es una secuencia de bits, éstos deben ser accesibles al menos en alguno de los siguientes sistemas informáticos: el que la creó en primer lugar, el que la almacena actualmente, el que accede a ella actualmente, o el que se utilizará en el futuro para almacenarla.

Lo cierto es que, de acuerdo con el informe, la información almacenada en soportes digitales puede llegar a ser ilegible en el futuro, básicamente por dos motivos:

- la exposición a condiciones de almacenamiento hostiles y condiciones ambientales pobres, o
- la obsolescencia de los soportes, o incompatibilidad entre el mismo y el hardware de que se dispone en cada momento.

Con buen criterio, el informe prevé que la tecnología no va a sufrir ningún proceso de paralización, es decir, los soportes seguirán envejeciendo, de tal manera que la transferencia a soportes nuevos será un proceso continuo e inevitable. De igual modo, asocia el problema de la legibilidad al del uso de formatos abiertos y neutrales con respecto a la tecnología.

El segundo componente de la estrategia de conservación se refiere a la inteligibilidad de la información, es decir, si la información esá constituída por secuencias de bits, y si un ordenador ha de "entender" adecuadamente estas secuencias, también deben conservarse las instrucciones o cualquier tipo de documentación que ayude al ordenador a esta comprensión acerca del modo en que las secuencias de bits se comportaron, por ejemplo, los metadatos incluídos en, o vinculados a, un documento redactado con un procesador de textos.

El tercer componente de la estrategia, de acuerdo con el informe, es la posibilidad de identificar la información conservada. Un objeto discreto de información debe ser identificable porque, a diferencia del entorno en papel, los objetos digitales y sus componentes se almacenan en un ordenador de manera aleatoria, se pueden utilizar componentes en más de un objeto, y objetos en más de un proceso. Por tanto, aquellos objetos de información que deban reproducirse de manera adecuada para un usuario deben tener algún tipo de identificador único, por ejemplo un título o un ID.

El siguiente componente de la estrategia que considera el informe es la recuperabilidad, en la medida en que carece de sentido conservar algo que no se puede recuperar y ver de nuevo. De acuerdo con el informe, la recuperabilidad es dependiente del software, porque se logra mediante el vínculo de la estructura lógica de los objetos de información con su ubicación física en un depósito. Por una parte, dicho vínculo se encuentra en componentes tales como registros de las bases de datos, estructuras de directorios, o cabeceras. Por otra, la interpretación tanto de la estructura lógica de la información como de los registros de los vínculos se lleva a cabo mediante aplicaciones, dispositivos, sistemas de ficheros o sistemas operativos específicos. Sin embargo, el uso de formatos que garanticen la compatibilidad retrospectiva podría en cierta medida mantener bajo control esta dependencia del software.

El informe también considera un componente básico de la estrategia de conservación a largo plazo la comprensibilidad de la información. Esta comprensibilidad no se refiere sólo a los seres humanos, sino también a los ordenadores. De manera muy significativa e importante para la archivística, el informe considera que para que la información sea comprensible en este doble sentido no basta con conservar sólo su contenido, también deben conservarse sus contextos de creación y uso, es decir, sus metadatos, que son los que añaden significado al contenido informativo. El informe recoge explícitamente nuestra aserción inicial de que, en el entorno electrónico, el significado viene dado por la lógica del objeto, más que por su contenido. De la conservación del contexto de creación y uso se deriva el que también deban conservarse los vínculos con otros objetos de información recogidos en lugares diferentes y por diversos procedimientos.

Por último, una estrategia de conservación a largo plazo debe considerar la autenticidad de la información conservada. La información auténtica se define, en términos muy similares a ISO 15489, como aquella que es lo que pretende ser, información fiable que a lo largo del tiempo no ha sido alterada, cambiada ni de otra manera corrompida. Para conseguir esta autenticidad el informe detecta tres puntos críticos:

- La transferencia y custodia. En el entorno de producción, de acuerdo con el informe, es muy difícil prevenir la alteración de la información. Por tanto, la estrategia de conservación debe proporcionar mecanismos de transferencia a una tercera parte fiable y responsable de mantener la información que le llegue del entorno de producción inalterada.

- El entorno de almacenamiento. De igual modo, debe preverse un entorno de almacenamiento estable y no hostil para los soportes de conservación.
- El acceso y la protección. La información, de acuerdo con el informe, debe contar con restricciones de acceso bien definidas, así como con medios para protegerla de alteración accidental o maliciosa. Algunas de estas protecciones vienen dadas por la tecnología, como los soportes magnéticos y ópticos no reescribibles, las arquitecturas cliente-servidor seguras de sólo lectura, algoritmos de compresión que funcionen como huellas digitales, etc.

El capítulo seis del informe está dedicado a la definición de los elementos de que debe constar una estrategia de conservación a largo plazo. En términos generales, asegurar que se conserva información exacta, fiable y veraz significa que ésta puede ser leída e interpretada por una aplicación informática, que puede ser representada de manera comprensible para humanos, y que se conserva tanto el contenido como el contexto y la estructura lógica y física que tenía la información cuando se creó o recibió.

A partir de la asunción de que las tecnologías y los soportes tienen un alto nivel de obsolescencia, el informe identifica tres actividades primarias para prevenir esta obsolescencia, y que están en la base de cualquier estrategia de conservación a largo plazo:

- Renovación de los soportes,
- Migración de información, y
- Emulación para sistemas obsoletos, procedimiento que el informe no toma en consideración.

El informe trata detalladamente, no obstante, la renovación de los soportes y la migración de la información, así como, aunque no la menciona como actividad primaria en la introducción, la asignación de metadatos. Siguiendo el propio orden del informe, exploramos estas tres estrategias a continuación.

En primer lugar, y dada la limitada durabilidad de los soportes, debe procederse a la renovación periódica y normalizada de los mismos, es decir, al reformateado o la copia de las secuencias de bits que conforman la información.

En el caso del reformateado, se pasa de un tipo de soporte a otro, lo que implica el cambio en la secuencia de bits, aunque no en el contenido de la información ni en la representación de la misma. El reformateado debiera ser, y de hecho casi siempre lo es, independiente de la aplicación que creó la información. Existen al menos tres motivos por los que debiera procederse al reformateado de información: su transferencia a un depósito, la actualización de los equipos o de los soportes de almacenamiento, y la programación del reformateado para hacerlo coincidir con la esperanza de vida prevista de los soportes.

El informe presta especial consideración al asunto de la selección de los soportes de almacenamiento, y lista un conjunto de características a tener en cuenta en el momento de realizar esta selección:

- alta capacidad de almacenamiento;
- alta tasa de transferencia de datos;
- esperanza de vida mínima proyectada de veinte años;
- presencia establecida y estable en el mercado;
- posibilidad; y
- adecuación.

Por otra parte, el reformateado puede implicar el cuestionamiento de la autenticidad de la información reformateada. Existen políticas de control de calidad que contribuyen a minimizar esta posibilidad de cuestionamiento, y que incluyen elementos tales como:

- identificación del(de los) individuo(s) que realmente ejecutaron el proceso;
- la fecha en que tuvo lugar;
- el formato de los datos;
- la comparación de valores como claves de redundancia cíclica u otros, para confirmar que no ha habido cambios;
- la comparación visual de varias instancias reformateadas de la información basada en documentos con sus contrapartida en el antiguo formato;
- el seguimiento y la documentación de errores y pérdidas irrecuperables de información;
- la revisión del uso de procedimientos establecidos por parte de terceras partes fiables; o
- el tratamiento de la documentación acerca del reformateado como metadatos vinculados a la propia información reformateada.

De acuerdo con el informe, los procesos de reformateado también deben estar sometidos a procedimientos de seguridad que prevengan el desastre o la intrusión humana. Identifica como posibles procedimientos de seguridad los siguientes:

- Instalación de "cortafuegos" de sólo lectura, y acceso sólo a individuos autorizados.
- Alojamiento de los soportes en un área bloqueada y segura, o cámara con acceso controlado.
- Almacenamiento de una copia de seguridad de los soportes en una localización separada de la original.
- Uso de dos tipos diferentes de soportes de almacenamiento para copias originales y de seguridad, para minimizar el riesgo de obsolescencia tecnológica inesperada.

Alternativa o complementariamente al reformateado pueden utilizarse procedimientos de copia de la información. A diferencia del reformateado, la copia implica la transferencia de la información a nuevos soportes con el mismo formato, de tal manera que no existe pérdida de contenido, contexto y estructura.

De igual manera que existían motivos para adoptar medidas de reformateado, existen también tres motivos que justifican el llevar a cabo procesos de copia: la transferencia, el error en los soportes, si se detecta durante actividades de verificación; y la programación periódica y normalizada, si los soportes aún son de uso, pero se prevé que éstos están sometidos a envejecimiento.

Aunque, como se indicó, la copia, a diferencia del reformateo, no implica alteración de la secuencia de bits, el proceso de copia también puede generar alteración accidental o maliciosa. Para minimizar el riesgo de que se ponga en cuestión la autenticidad de la copia, deben emprenderse controles de calidad que, como en el caso del reformateado, incluyan documentación acerca de las tareas y los participantes implicados en el proceso de copia. Esta documentación es absolutamente similar a la descrita para los controles de calidad del reformateado. De igual modo, son en todo similares los procedimientos de seguridad recomendados durante el proceso de copia.

Como se dijo, aunque el informe no los menciona como actividad primaria de una estrategia de conservación, dedica sin embargo una breve sección entre la de reformateado y copia y la de migración, a la actividad de asignación de metadatos, interpretando metadatos como información acerca del contexto de creación y uso de la información, que sirve para identificar, recuperar y conservar ésta en forma auténtica. Muchos metadatos se generarán de forma

automática, mientras que otros, con independencia de que futuros desarrollos de la tecnología permitan su automatización, deben introducirse manualmente, especialmente aquellos que dependen de políticas archivísticas de clasificación, valoración, recuperación, etc. En cualquier caso, lo que interesa es que estos metadatos sean recuperables ellos mismos, y que a partir de ellos se pueda recuperar la información con la que se vinculan. Deseablemente, de acuerdo con el informe, los metadatos debieran ser interoperables y reutilizables en diferentes entornos.

Tras la breve sección acerca de metadatos, el informe que nos ocupa se aplica a describir los procesos de migración que, según se indicó más arriba, constituyen otra de las actividades primarias de cualquier estrategia de conservación. Estos procesos de migración se abordan desde la perspectiva de cuatro retos a los que deben hacer frente los responsables de conservar información electrónica en forma auténtica, y que son:

- La variedad de implantaciones específicas de software y formatos que utilizarán organizaciones e individuos, y la dificultad de acceder al soporte técnico de todos ellos;
- La dependencia del software de al menos parte de la información electrónica;
- La rapidez con la que el mercado desplazará sistemas operativos y aplicaciones de software, substituyéndolos por otros nuevos; y
- La existencia de sistemas de información históricos u obsoletos sin posibilidades de migración automática.

El informe plantea, a partir de estos cuatro retos, una estrategia de conservación que sea capaz de migrar con éxito información de un entorno a otro diferente, sin pérdida de contenido ni de contexto, y con la menor pérdida posible de estructura.

Para ello deben tomarse en consideración diferentes cuestiones, siendo la primera de ellas la dependencia del software. Si se genera información haciendo uso de una aplicación específica o propietaria, es muy posible que esta información no se pueda utilizar en otros entornos, o que se utilice a cambio de sacrificar parte de su estructura, aunque esto implica una alteración de la información. En términos del informe, ni siquiera es una copia de la información original, sino nueva información, por lo que resulta necesario documentar el proceso que la ha generado, y autenticar nuevamente su contenido, ya se trate de documentos análogos a los documentos en papel, que podrían, por ejemplo, imprimirse, o bases de datos cuyas tablas hubieran perdido los vínculos, que quedarían documentados mediante metadatos.

Otra cuestión que debe examinarse es la de la migración de la información a versiones nuevas del mismo software o de un software a otro distinto. En el primer caso, debiera requerirse del proveedor que la migración respetara todos los componentes de la información. En el segundo, debiera preverse el que el antiguo software disponga de propiedades de exportación y el nuevo de propiedades de importación, así como la posibilidad de utilizar pasarelas entre formatos propietarios.

Una tercera cuestión es la de la necesidad de migrar formatos propietarios, obsoletos, no consolidados, etc., a un número reducido de formatos normalizados que faciliten la gestión de la conservación de la información electrónica, por ejemplo, XML, PDF, TIFF, JPEG.

Una cuestión particularmente importante es la de la migración de sistemas, sobre todo antiguos, que no tienen propiedades de exportación ni de compatibilidad retrospectiva, ni pueden hacer uso de pasarelas para la interpretación de formatos propietarios en entornos diferentes al de origen. Aunque el desarrollo de la tecnología previsiblemente hará desaparecer este riesgo, tales sistemas sin embargo existen, y la información que contienen deben migrarse a sistemas nuevos. En tales casos, cierta pérdida de información será inevitable, por

lo que los procesos de control de calidad y de documentación del proceso son incluso más relevantes que en las situaciones descritas anteriormente.

El informe que nos ocupa sugiere una aproximación a la migración basada en diez pasos, que pueden verse modificados en función de situaciones específicas. Estos diez pasos son:

- Análisis del sistema de información antiguo, incluídos la fundamentación de sus funcionalidades, el modo en que se capturan metadatos y la relación de éstos con la información a la que se refieren, y las relaciones entre la propia información.
- La descomposición de la estructura del sistema de información antiguo, que será posible si el sistema y los interfaces de usuario, los módulos de aplicación, el servicio de base de datos y la base de datos misma son componentes separados e independientes; no será posible si los interfaces, las aplicaciones y los servicios de la base de datos están enlazados en un módulo; y será parcialmente posible si los interfaces y la base de datos son independientes, pero la aplicación y los servicios de la base de datos forman un solo módulo.
- Diseño de los interfaces de destino.
- Diseño de las aplicaciones de destino.
- Diseño de la base de datos de destino.
- Instalación y comprobación del entorno de destino.
- Creación e instalación de pasarelas, asegurando el mayor grado posible de exactitud y coherencia en la réplica de funcionalidades del sistema de origen.
- Migración de la base de datos de origen.
- Migración de las aplicaciones de origen.
- Migración de los interfaces de origen, lo cual no siempre será posible ni deseable, en la medida en que los interfaces han evolucionado hacia desarrollos gráficos.

El último capítulo (7) del informe se dedica al desarrollo de una estrategia de conservación a largo plazo, tomando en consideración el desarrollo de una política de conservación, el control de calidad, la elaboración de políticas de seguridad y el control ambiental.

La política de conservación específica de una institución debiera quedar reflejada en un documento que contuviera los siguientes elementos:

- la identificación de los fines de la conservación de información auténtica;
- la descripción del tipo de custodia que el depósito lleva a cabo sobre la información;
- la descripción de las buenas prácticas a las que el depósito se adhiere;
- la identificación de las circunstancias, métodos y fundamentación de las actividades de migración;
- la explicación de los tipos de auditoría a ejecutar; y
- la aclaración de los roles del personal del depósito y de las responsabilidades externalizadas.

En lo que concierne al control de calidad, el informe insiste en los procedimientos de documentación explicados más arriba, a efectos sobre todo de evidencia legal.

Con respecto a las acciones de seguridad, a las que el informe confiere una extrema importancia, se toman en consideración las siguientes: el control del acceso a la aplicación, el control del acceso físico, y la protección contra pérdidas, para cada una de las cuales detalla cuidadosos procedimientos.

La institución debiera contar con un documento de política de seguridad con al menos los siguientes componentes:

- las medidas de seguridad utilizadas durante la transferencia de información al depósito;
- los procedimientos de control del acceso y la supervisión de esos procedimientos;
- la localización de las instalaciones para minimizar el peligro de pérdida debida a desastre natural;
- un plan para recuperación de desastres;
- la adhesión a normas reconocidas relativas al tratamiento de soportes;
- la provisión de instalaciones secundarias para las copias de seguridad de los soportes y los procedimientos de recuperación de desastres.

Por último, el informe hace breve mención a algunas medidas de control medioambiental para la protección de los soportes, a saber:

- provisión de un entorno de almacenamiento en el que la temperatura y la humedad relativa estén controladas;
- provisión de un sistema de filtración de aire para evitar partículas de polvo y contaminantes gaseosos;
- prohibición del consumo de comida y bebida, y de fumar;
- implantación de un programa para leer anualmente una muestra estadística de la información, con el fin de identificar pérdidas de información reales o inminentes.

8. ISO 19005-1:2005: PDF/A-1 (21)

En la presente exposición prestaremos muy poca atención a la norma ISO 19005-1, que está destinada, por lo demás, a convertirse en la primera de un conjunto de normas, no porque carezca de interés, sino porque, por diversos motivos, queda fuera del alcance del objeto de la exposición, que son las normas de conservación archivística. En primer lugar, la norma ISO 19005-1 es un documento extremadamente técnico, destinado a ser comprendido e implantado por profesionales de la informática, no de la archivística. Se apoya, con ligeras modificaciones, en el formato PDF de Adobe, lo cual ya apunta hacia otro buen motivo por el que no debiera considerarse una norma de archivo, aunque concurra por supuesto a una buena política de conservación archivística: PDF, como la propia norma declara, está destinado a congelar imágenes de documentos, de tal manera que el proceso de documentar, es decir, el conjunto de todos los componentes que discutimos al comienzo, no queda recogido, ni siquiera en los metadatos anidados en el fichero. Por tanto, PDF es una buena implantación para conservar documentos similares a papel, así como para autenticarlos (con el matiz, ya indicado en la norma) de que no todos los procedimientos de firma electrónica son compatibles con PDF. El formato no es adecuado para documentos dinámicos y disímiles del papel, ni para la garantía de autenticidad a largo plazo. No obstante, es una implantación específica útil para los fines indicados y, en combinación con otras tecnologías, como XML, contribuye a la creación y gestión de buenos sistemas de conservación archivística. Esta es la aproximación emprendida en su día, por ejemplo, por la prestigiosa iniciativa VERS (Victorian Electronic Records Strategy) (22).

9. ISO/NP 26102: Requisitos para la conservación a largo plazo de documentos electrónicos

En el marco de la familia de normas derivadas o consecuencia de ISO 15489 se enmarca el proyecto ISO 26102, destinado a establecer un conjunto de requisitos para la conservación a largo plazo de documentos electrónicos. En efecto, las menciones a la conservación en ISO 15489-1 e ISO 15489-2 son muy breves, y se refieren más bien a las acciones relacionadas con la disposición, durante el período de mayor actividad de los documentos. Por lo demás, el

objetivo de ISO 15489 no es de manera específica los documentos electrónicos (23). Aunque se trata de menciones importantes, en la medida en que incorporan la conservación a la fase misma de diseño del sistema y de vida activa del documento, y en la medida en que ha servido hasta cierto punto de guía para la redacción de ISO/TR 18492, están ausentes de la norma, probablemente porque no es su objetivo, directrices específicas y detalladas acerca de los procesos de conservación a largo plazo de documentos electrónicos.

No parece por tanto inadecuada, en el contexto de la familia de normas ISO asociadas a ISO 15489, la redacción de un texto dedicado específicamente a los requisitos de conservación de tales documentos. Este es el objetivo de ISO 26102, promovida por la delegación sudafricana del SC11. Puesto que todo proceso de preparación de una norma es muy lento, en el momento de redactar la presente exposición, ISO 26102 se encuentra aún en fase de borrador y de comentarios y, a nuestro juicio, se encuentra aún lejos de alcanzar una versión definitiva. Esto no significa que no se alcance, sino más bien que describir documentos no terminados constituye un riesgo que no debiéramos afrontar, por cuanto se pueden dar por sentados criterios que sufran posterior modificación. Con todo, una enunciación simplemente de la estructura del borrador podría resultar en cierto modo clarificador, siempre que se tenga en cuenta la provisionalidad de tal aproximación.

Así, en su actual fase de desarrollo, ISO 26102 se divide en once capítulos, más un apéndice temporal, y otro apéndice prometido pero no elaborado. Además de los capítulos convencionales de alcance, referencias normativas y términos y definiciones, los capítulos de la norma, que pretenden ser paralelos a los de ISO 15489, son los siguientes: beneficios de la conservación de documentos electrónicos, entorno regulador, políticas y responsabilidades; un extenso capítulo sobre requisitos de conservación de documentos electrónicos, con una primera cláusula relativa a los principios que deben satisfacer los programas de conservación de documentos electrónicos, incluídos los objetivos del almacenamiento, las políticas de migración, las estrategias de almacenamiento de metadatos, y las auditorías de conformidad; y otra cláusula acerca de las características del documento en el contexto de conservación, incluídos el aseguramiento de la autenticidad del documento en el momento de la captura, el uso de documentos electrónicos en procesos legales, y la prevención de acceso no autorizado a los documentos. El siguiente capítulo aborda los procesos de gestión de la conservación y los controles de los documentos electrónicos, incluídos la valoración, la ingesta, el almacenamiento, la planificación de la conservación, las acciones de conservación, el acceso, la disposición, los procesos de documentación y, particularmente, la gestión de metadatos. Sigue un capítulo acerca de la implantación de los requisitos de conservación en los sistemas de documentos, incluídos los requisitos de los soportes de almacenamiento, los de seguridad, los de conservación de metadatos, la gestión del riesgo, el mantenimiento y los costes. Los dos últimos capítulos, muy breves, están dedicados a la supervisión y auditoría, y a la formación, respectivamente.

Por supuesto, del simple enunciado del título de los capítulos resulta muy difícil deducir el valor de su contenido, pero, insistimos, éste es provisional y, por tanto, entrar en su descripción y su valoración resulta un riesgo. No obstante, esperamos que se deduzca al menos la exhaustividad con la que el borrador de norma pretende abordar todos aquellos aspectos relacionados con la conservación de documentos electrónicos.

10. Conclusiones

Excluído, por los motivos que hemos indicado, el borrador de norma ISO 26102, la aportación de ISO a la conservación a largo plazo de documentos electrónicos es, en términos generales, limitada. Sus aproximaciones se basan preferentemente en la conservación de los datos y en la creencia de que el documento se puede congelar tecnológicamente de alguna manera. Sin

embargo, los documentos electrónicos son objetos cada vez más dinámicos, con lógicas más complejas, que ni siquiera la más archivística de las normas descritas, como es ISO/TR 18492, toma en consideración. En efecto, aunque les dedica una breve sección, la norma parece no tomar en serio la fundamental importancia de los metadatos a efectos de conservación, no de los datos (a lo largo de interminables procesos de migración no es concebible que los datos sean conservables), sino de su significado. No obstante la visión positivista y orientada a la satisfacción actual de los intereses de las organizaciones, las normas descritas aportan sustantivos procedimientos y notables técnicas para garantizar, dentro de ciertos plazos y/o para ciertos tipos de documentos, una conservación auténtica. Sin embargo, en el entorno digital y desde el punto de vista del archivo, la conservación de documentos electrónicos no es en primer lugar la conservación de los datos o el contenido, sino la conservación de la lógica y del significado, componentes cuyo valor las normas descritas minimizan. La esperada norma ISO 26102 debiera contribuir a poner en un lugar central estos componentes esenciales, así como los metadatos que los reflejan.

Notas

(1) Cfr.: *InterPARES: International Research on Permanent Authentic Records in Electronic Systems*. URL. http://www.interpares.org (Consulta: 13-10-2007)

(2) Cfr.: Digital Longevity. URL: http://www.digitaleduurzaamheid.nl/index.cfm?paginakeuze=286 (Consulta: 13-10-2007)

(3) Cfr.: Expertisecentrum eDavid. URL: http://www.expertisecentrumdavid.be/eng/index.php (Consulta: 13-10-2007)

(4) Cfr., por ejemplo, Software. URL: http://www.naa.gov.au/records-management/secure-and-store/e-preservation/at-NAA/software.aspx (Consulta: 13-10-2007)

(5) InterPARES 2 Project: Terminology Database. URL: http://www.interpares.org/ip2/ip2_terminology_db.cfm (Consulta: 1-9-2007)

(6) Ibid.

(7) Ibid.

(8) *ISO 15489-1:2001: Información y documentación – Gestión de documentos. Parte 1: Generalidades*. Ginebra: Organización Internacional de Normalización, 2001. P. 10-11.

(9) Bearman, David: "Item Level Control and Electronic Recordkeeping". En: *Archives & Museum Informatics*. Vol. 10, n. 3. P. 195-245. URL: http://www.archimuse.com/papers/nhprc/item-lvl.html (Consulta 1-8-2007)

(10) Duranti, Luciana: "La cuestión fundamental: ¿en qué entidades digitales se concreta la memoria del futuro?". Originalmente publicado en: *Archivi & Computer*, 2 (2005) 5:30. También disponible en: http://archivo.cartagena.es/recursos/texto0_Duranti-Torino-trad.pdf (Consulta: 1-9-2007)

(11) Thibodeau, Kenneth: "Overview of Technological Approaches to Digital Preservation and Challenges in Coming Years". En: *The State of Digital Preservation: An International Perspective: Conference Proceedings Documentation Abstracts*, Inc. Institutes for Information

Science. Washington, D.C. April 24-25, 2002. Washington D.C.: Council on Library and Information Resources, 2002. P. 4-31.

(12) *From digital volatility to digital permanence: Preserving databases. The Hague: Digital Preservation Testbed*, 2003. En general, todos los documentos del testbed holandés asumen esta noción. URL: http://www.digitaleduurzaamheid.nl/bibliotheek/docs/volatility-permanence-databases-en.pdf (Consulta: 25-8-2007)

(13) Ketelaar, Eric: "Time future contained in time past: Archival science in the 21st century". En: *Journal of the Japan Society for Archival Science*. N. 1 (2004). P. 20-35.

(14) Harvey, Ross: *Preserving Digital Materials*. München: K.G. Saur, 2005.

(15) Lynch, Clifford: "Authenticity and Integrity in the Digital Environment: An Exploratory Analysis of the Central Role of Trust". En: *Authenticity in a Digital Environment*. Washington D.C.: Council on Library and Information Resources, 2002. P. 32-50

(16) Para una discusión más detallada, confróntese, por ejemplo, Delgado Gómez, Alejandro: *El centro y la equis: una introducción a la descripción archivística contemporánea* (en prensa)

(17) http://www.csi.map.es/csi/pg3413.htm (Consulta: 1-9-2007)

(18) *ISO/NP 26102: Information and documentation -- Requirements for long-term preservation of electronic records*.

(19) *ISO/TR 15801:2004: Electronic imaging -- Information stored electronically -- Recommendations for trustworthiness and reliability*. Ginebra: Organización Internacional de Normalización, 2004. La presente sección se basa en un curso ya pronunciado para Aedocdigital.

(20) *ISO/TR 18492:2005: Long-term preservation of electronic document-based information*. Ginebra: Organización Internacional de Normalización, 2005.

(21) *ISO 19005-1:2005: Document management -- Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1).* Ginebra: Organización Internacional de Normalización, 2005.

(22) Victorian Electronic Records Strategy (VERS) –URL: http://www.prov.vic.gov.au/vers/vers/default.htm

(23) Confróntese cláusula 8.3.7 de la norma citada, así como la cláusula 4.3.9, especialmente 4.3.9.2, de la segunda parte: *UNE-ISO/TR 15489-2: Información y documentación – Gestión de documentos. Parte 2: Directrices*. Madrid: AENOR, 2006