Pontificia Universidad Católica del Perú

Departamento de Humanidades

EL SISTEMA DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS Y LA AUTENTICIDAD DE DICHOS DOCUMENTOS

Adalgisa Abdala Bárcenas

Serie

Temas de Bibliotecología e Información

N° 16

Lima, 2012

Agradecemos a Beatriz Montoya Valenzuela, jefa del Archivo de la Universidad y a Marita Dextre Vitaliano, administradora del Archivo, por su valiosa ayuda en la revisión y corrección de este trabajo.

El sistema de gestión de documentos electrónicos y la autenticidad de dichos documentos / Adalgisa Abdala Bárcenas – Lima: Pontificia Universidad Católica del Perú. Departamento de Humanidades, 2012. 35 p., 21 cm. (Temas de Bibliotecología e Información; 16)

ARCHIVOS ELECTRÓNICOS - ADMINISTRACIÓN
RECURSOS DE INFORMACIÓN ELECTRÓNICA
INFORMACIÓN - SISTEMAS DE ALMACENAMIENTO Y RECUPERACIÓN
SISTEMAS DE INFORMACIÓN – SEGURIDAD
METADATOS
CD 974.4 A112

Hecho el Depósito Legal en la Biblioteca Nacional del Perú N° 2012-05199
Pontificia Universidad Católica del Perú
Av. Universitaria 1801, San Miguel, Lima 32, Perú
http://www.pucp.edu.pe

Tabla de contenido

Presentación

Con motivo de celebrarse las Bodas de Plata de la carrera de Ciencias de la Información de nuestra Universidad, del 9 al 11 de agosto de 2011 se realizó el "Taller de Archivos Electrónicos y Digitales", cuyo objetivo fue conocer y compartir los avances y buenas prácticas en el tratamiento archivístico de tales documentos. La organización de la actividad estuvo a cargo del Archivo de la Universidad y de la Sección de Bibliotecología y Ciencia de la Información, del Departamento de Humanidades.

El entorno tecnológico en el que la mayoría de sociedades se desenvuelve en la actualidad plantea una serie de retos al profesional de la información, quien cada día recibe y procesa una cantidad cada vez mayor de documentos en formato electrónico, sin que esté necesariamente preparado para afrontar tal situación dada la velocidad con que se operan los cambios. Cómo gestionar los documentos electrónicos, cómo enfrentar la obsolescencia tecnológica, qué medidas se deben tomar para garantizar la seguridad de los expedientes electrónicos, son algunos de tales desafíos. Con el afán de contribuir a la difusión de estos importantes temas del quehacer profesional, nuestra serie reproduce, en esta oportunidad, el texto de la conferencia que, en el marco del Taller, ofreció la Ing. Adalgisa Abdala Bárcenas, quien es Directora del Departamento de Gestión Documental del Banco de la República de Colombia; se ha desempeñado como docente de la Pontificia Universidad Javeriana en las especializaciones de Archivística y Redes de Información Documental; y en el diplomado de Gestión de Información. Igualmente, ha sido docente de la Universidad de la Salle tanto en la Facultad de Sistemas de Información y Documentación, como en la División de Formación Avanzada en la Especialización de Información y Gerencia de Documentos.

Esperamos que la lectura del texto sea una invitación no sólo a conocer los avances que se operan en los archivos electrónicos y digitales, sino también a tomar conciencia de la importancia que reviste su adecuada gestión y preservación.

Aurora de la Vega
Coordinadora
Sección de Bibliotecología
y Ciencia de la Información

EL SISTEMA DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS Y LA AUTENTICIDAD DE DICHOS DOCUMENTOS

Adalgisa Abdala Bárcenas[1]

Considero importante iniciar este trabajo con la premisa de que gestionar adecuadamente los documentos requiere el mismo esfuerzo independientemente del soporte en el que estos residan, de tal manera que cuando se revisan temas como los que me atañen realmente encontrarán que las metodologías, programas, ciclo vital de la información, rigurosidad en la gestión, organización, valoración, clasificación, disposición final, etc., son exactamente iguales en el mundo físico y en el mundo electrónico.

Igualmente, quiero iniciar con una segunda premisa referente a no exigirle a la tecnología cubrir para los documentos electrónicos aspectos que hoy no se les exige a los documentos en papel.

I. Problemática de la gestión documental en el entorno tecnológico

1. Aquella relacionada directamente con las diferentes etapas del ciclo vital de los documentos electrónicos:

Producción documental

a. **Se reemplaza el soporte papel por el soporte electrónico en la generación de documentos formales y oficiales** sin exigencia (o evaluación) de los mismos aspectos de formalización del documento físico (firma, numeración, fecha, contenido, etc.), sin establecer si la tipología es de uso general dentro de la organización y por ende no se

1 Directora del Departamento de Gestión Documental. Subgerencia de Gestión de Riesgo Operativo del Banco de la República, Bogotá, Colombia.

controla para una misma tipología de conservación en soporte físico y electrónico, modificando muchas veces (o ignorando) el valor de la información por el cambio de soporte que elude las políticas, estándares y procedimientos establecidos para el soporte papel, sin la claridad respecto del trámite en su totalidad y los documentos que lo soportan o sustentan.

b. **En la producción documental, ya sea generación o recepción, no se sabe qué ni cuánto, ni cuándo.** Para los documentos electrónicos no se aplican los conceptos de numeración, radicación o registro, indización, tipologías documentales definidas y catalogadas en la Tabla de Retención Documental (TRD).
c. **No se incorpora en los documentos electrónicos la imagen corporativa ni se mantiene la misma formalidad de los contenidos que se aplican en el mundo físico.** En general la información electrónica pareciera generada de una manera más informal (correos electrónicos) y sin incorporar a su contenido aquellos elementos de la imagen institucional de la organización.
d. **No existen para los documentos electrónicos políticas ni estándares de descripción (metadatos), ya sea sobre información externa o interna contenida en el archivo.** Una vez generado el archivo no se establecen los metadatos mínimos de contexto para oficializar el documento y muchas veces dentro de su contenido se omite este tipo de información importante. Ej: la información del destinatario y/o del remitente se pierde puesto que muchos de los archivos no contienen esta información ni tienen un documento de presentación del mismo, únicamente se logra establecer por el medio de envío (correo electrónico).

Distribución, divulgación y publicación

a. **No existen controles o políticas respecto a lo que se distribuye, divulga y publica.** Aquellos empleados con cuentas de correo individual pueden remitir archivos hacia el exterior de la entidad sin estar autorizados para ello (ej. sin tener firma autorizada); existe mayor riesgo en la no reserva de la información por la facilidad en la generación de

altos volúmenes de información, facilidad de acceso y distribución o copia (USB, CD, DVD, etc.) de la misma; se corre el riesgo de publicar información «no oficial».

b. **No se tienen herramientas que permitan establecer las publicaciones históricas y su vigencia de publicación.** Se corre el riesgo de no lograr establecer las fechas de publicación y de que no se conserve la historia de los archivos publicados.
c. **Los controles de distribución de documentos electrónicos, en caso de existir, son externos a los documentos.** Generalmente no se tienen establecidos controles que garanticen la fecha y hora de recepción, despacho y entrega de archivos electrónicos que a futuro permitan certificar su validez.
d. **No existen políticas claras de divulgación de la información que tiene destinatarios específicos.** Generalmente se modifican procedimientos de distribución física de documentos por divulgación de documentos electrónicos sin clasificar la información respecto a su reserva, confidencialidad, privacidad, etc.

Trámite

a. **No es fácil realizar el seguimiento a un documento electrónico.** Dado que no existen los procedimientos en la recepción o generación de los mismos, este proceso no se puede realizar, lo que dificulta establecer el avance del trámite.
b. **No se tiene la vinculación entre los documentos de un mismo trámite.** No se tiene establecido cómo se conforma un expediente que contenga información híbrida (electrónica en diferentes tipos de repositorios vs. física) lo que imposibilita reconstruir la totalidad del trámite.
c. **No es fácil identificar la versión final, oficial e íntegra de un archivo electrónico.** No existe el concepto de «registrar un documento» de tal manera que se establezca como «oficial» dentro de la organización, no se determinan los criterios que permitan definir un documento como «original» y cuáles como copias electrónicas.
d. **Si no se cuenta con las herramientas de seguridad necesarias, se**

dificulta establecer si un archivo electrónico fue modificado. Generalmente los archivos electrónicos no se firman electrónicamente para garantizar su integridad o se establecen procedimientos de seguridad informática que eviten o registren eventos de modificación.

Almacenamiento, recuperación o consulta

a. **No existen estándares de clasificación, descripción y ubicación lo que dificulta el acceso a los documentos electrónicos.** No existe unicidad de criterios en cuanto a clasificación, ubicación (PC, servidor, otro medio), nombres de archivo, estructuras estándares, etc.
b. **No se aplica el concepto de tradición del documento (originales de archivo).** No se tiene una política de conservación ni de lo generado por la entidad ni de lo recibido, de tal manera que se conserve el documento electrónico que permitirá a futuro dar aval de «originalidad».
c. **Los documentos electrónicos se conservan simultáneamente en diferentes repositorios** generando redundancia de información y generalmente no se tiene claridad sobre la versión final oficial.

Disposición final

a. **La información en soporte electrónico no se valora con la misma rigurosidad que en soporte papel.** El valor que la información electrónica tiene o no se ha identificado, o si existía en soporte papel y en dicho soporte estaba valorada, no se aplicaron los tratamientos y políticas archivísticas por estar ahora en otro tipo de soporte, o se deja esta responsabilidad a las áreas de tecnología acorde con las políticas de respaldo (backup) establecidas; es decir, los tiempos de retención dependen de las condiciones tecnológicas (espacio, respaldo, etc.) y no de la valoración de la información.
b. **No se establecen las estrategias y procedimientos que garanticen la conservación de los documentos electrónicos y su futura recuperación.** Hay información electrónica almacenada sin definición de sus políticas archivísticas. Existe vulnerabilidad de los medios y del

cambio tecnológico en hardware y software. Se confía suficientemente en las políticas de «backup».

c. **El proceso archivístico de transferencia no se realiza y en caso de que sí se haga no se aplica la misma rigurosidad del mundo físico (papel).** Se entiende la transferencia como la migración de información a medios de mayor capacidad de almacenamiento, menor costo y tiempo de recuperación.

d. **El proceso archivístico de evaluación y eliminación no se realiza y en caso de que sí se haga no se aplica la misma rigurosidad del mundo físico (papel).** El descarte de la información electrónica se realiza por aspectos técnicos y no asociados a la valoración de la información y consiste en el borrado o sobre escritura de archivos en los medios de almacenamiento.

2. Aquella relacionada directamente con la seguridad:

a. **Existe dificultad para garantizar los aspectos de seguridad en el tiempo.** Vincular la información de seguridad con los datos, definirles el mismo tiempo de retención y lograr descifrar la información de los elementos de seguridad vinculados a los empleados de la organización.

b. **Existen aspectos por resolver desde el punto de vista tecnológico para garantizar los aspectos de seguridad de los documentos electrónicos:**
   - ¿A qué se le considera documento?
   - ¿Cuáles son los documentos de archivo (archivo, registro de una base de datos, transacción, documento ofimático (ej: office), archivo de imagen, formulario, etc.)?
   - ¿Cómo garantizar la integridad de los contenidos?
   - ¿Cómo garantizar la confidencialidad y reserva de la información?
   - ¿Cómo se vincula en el tiempo el contenido con el productor del mismo?

3. Aquella relacionada directamente con la tecnología:

   a. **La interpretación de lo que está realmente almacenado depende del software y hardware que permiten su edición o visualización.**

La tecnología almacena la información de una manera diferente a la visualización de la misma, los archivos realmente no existen como «entidades» físicas, sino como contenido binario (registro de 1´s y 0´s) con información referencial que los vinculan entre sí y etiquetas que especifican el principio y el final de un archivo. Los archivos electrónicos solo podrán ser visualizados si las herramientas tecnológicas cuentan con los visores apropiados y solo podrán ser editados si se tiene el software en la versión e idioma correspondiente (o una versión superior).

b. **La obsolescencia tecnológica puede ocasionar que los archivos electrónicos no puedan ser accedidos en el tiempo**. Entre otros tenemos los medios de almacenamiento, los sistemas operativos, los sistemas de información, los dispositivos de acceso a los medios de almacenamiento (*drive*), etc.
c. **Dificultad en la protección de la propiedad intelectual y de los derechos de privacidad.** La facilidad que provee la tecnología para manejar altos volúmenes de información y reutilizar la información.

II. El documento electrónico

Más que la definición de documento electrónico lo importante dentro de la gestión documental es establecer claramente a qué tipo de información electrónica se clasificará como documento electrónico y cuál será considerada como documento electrónico de archivo.

Se debe diferenciar aquella información electrónica que se modifica con el tiempo de aquella que es estática, una vez que se genera como la «oficial», por cuanto es en esta última donde residirá el subconjunto de los documentos electrónicos de archivo.

La información electrónica que reside en las diferentes bases de datos de la organización solo podrá ser considerada como documento de archivo cuando se garantice que la misma es «estática e inmodificable» en el tiempo, por ejemplo: lo que se exporta a un archivo electrónico en otro formato (ej. un reporte o un *archive*).

Igualmente, se debe diferenciar claramente la información que se almacena con fines de continuidad, es decir, las cintas de respaldo o de backup, de la conservación con fines archivísticos, por cuanto para efectos de continuidad son las áreas de tecnología las que establecen los horarios de recogidas y restauraciones, así como las políticas de copiado, borrado, sobreescritura y destrucción de cintas; mientras que son las áreas de gestión documental las que establecen en la Tabla de Retención Documental (TRD) los tiempos de retención que se deben garantizar para la información electrónica de archivo.

Para establecer los documentos electrónicos de archivo que se deben conservar y a los cuales se les asociará una entrada en la TRD se debe realizar un análisis de la producción documental a la luz de los procesos de negocio; es decir, todos aquellos documentos que entran al proceso se generan como intermedios en las actividades del mismo y salen del proceso; también se deben establecer las características que dentro de la organización definen un «documento electrónico de archivo» para que estas sean conocidas por todos los generadores de información. Dentro de las características están:

- Cuáles van a ser los formatos de archivos electrónicos aceptados como documentos de archivo.
- Cuál es el documento original que se conservará como evidencia.
- Cuál será el contenido de los archivos electrónicos aceptado como «documento de archivo». Deben ser documentos con contenidos autointerpretables, es decir, que la comprensión del contenido no dependa de la existencia de un sistema de información que decodifica la información sino que un «humano» pueda entenderlo o tenga acceso a las herramientas que le apoyen en la interpretación.

III. El expediente electrónico

- Los expedientes electrónicos deben contener los datos y los metadatos de cada uno de los documentos y se debe establecer dichos contenidos desde el momento en que se inicia la producción documental de un determinado trámite.
- Su organización y estructura deben reflejar el trámite que soporta.

- Al igual que en el mundo físico, el expediente electrónico debe contener el conjunto de documentos «ordenados», ya sea lógicamente (es decir a través de hipervínculos a apuntadores a los documentos independientemente de dónde estos residan) o virtualmente (es decir todos los archivos de un mismo expediente ubicados en el mismo espacio de almacenamiento electrónico).
- Algunos estándares para conservación son:
  - ISO 14721 OAIS Sistema de Información de Archivos Abiertos (Open Archival Information System)
  - ISO 9005 PDFA 1.4 Formato de Conservación de Documentos Electrónicos.

IV. El archivo electrónico

Es el almacenamiento y conservación de documentos generados por medios electrónicos, garantizando los aspectos de seguridad, acceso, disponibilidad, integridad y autenticidad. Al igual que en el mundo físico es muy importante para una adecuada gestión de archivos establecer:

- **El sistema archivístico.** Se refiere al establecimiento del modelo de gestión de información, sus componentes y su interrelación para definir cuáles serán los esquemas de clasificación, control, organización, descripción y almacenamiento de documentos, cómo se realizarán las transferencias y los descartes en el mundo electrónico y a qué se le denominará copia técnica de archivo en el mundo electrónico.
- **Centros de archivo.** Dado que en el mundo físico a la áreas de gestión documental les compete definir la infraestructura, las condiciones de los depósitos y muebles de archivo, el dimensionamiento y las unidades de conservación apropiadas, se deben establecer claramente las competencias en el mundo electrónico por cuanto el «centro de cómputo» de las organizaciones generalmente es «uno» y su administración

depende de las áreas de tecnología, tales como: definición de los repositorios oficiales de conservación, de los medios de conservación y consulta para los documentos de archivo, generación de copias de respaldo a los medios que almacenan los documentos de archivo y definición de los procedimientos de revisión y migración.

- **Servicios de archivo.** En el mundo electrónico se debe redefinir tanto los servicios como la prestación de los mismos de tal manera que esté, documentado y establecido el acuerdo de servicio para cada uno; qué se entiende en el mundo electrónico para los siguientes servicios y cómo se prestarán en la organización:
  - Préstamo
  - Entrega y devolución de originales
  - Copia de documentos
  - Autenticación de documentos
  - Consultas de información transferida

V. La gestión de la información

El adecuado manejo de la información en una organización definitivamente depende del apoyo que la alta gerencia le otorgue al desarrollo e implementación del Programa de Gestión de Documentos Electrónicos (PGDE) avalándolo, asignando los recursos (personas y económicos), invirtiendo en un cambio cultural que permita su interiorización individual que garantice el cumplimiento y ajuste a las leyes y regulaciones, y que le facilite y le aporte a los procesos de negocio de la organización, dejando claridad total de que la información corporativa es de la empresa y no de las personas que la producen.

Debe establecerse y administrarse un adecuado sistema de gobierno de la información que establezca los lineamientos que rigen el ciclo vital de la información y sean los pilares para su adecuada gestión. Dicho sistema debe generar, normar y divulgar los principios y políticas, asignar las responsabilidades en el uso de la información mediante la definición de roles y perfiles, tanto para las diferentes instancias que conforman dicho gobierno como para todos los productores de información y definir claramente su

interacción. Uno de los primeros desafíos que debe abordar es el de establecer una Tabla de Retención Documental (TRD) orientada a procesos y que contemple el total de la información de la organización independientemente del soporte.

Se deben definir las estrategias que permitirán tanto el desarrollo del PGDE como su implementación, de tal manera que se tenga la menor resistencia posible al mismo, la mayor productividad en la operatividad de la organización y se cumpla el objetivo con la información. Es necesario establecer la forma de garantizar la articulación entre los procesos, los riesgos, la continuidad, la seguridad y la información, no solo a nivel de políticas y de procedimientos sino de desarrollo interdisciplinario de las iniciativas que permitan su integración. Es importante definir las estrategias de «inicio» al PGDE respecto al apoyo de terceros (contratación para gestión de cambio, levantamiento de información, establecimiento de metodologías, desarrollo de documentos de requerimientos para adquisición de tecnologías, etc.), si se iniciará por áreas claves, temas o trámites claves, procesos claves, etc., cómo se incorporan dentro del PGDE los sistemas de información y las tecnologías de la información ya existentes e implementadas en la organización, y cuáles serán los subprogramas de gestión documental que se atacarán y en qué orden de prioridades.

Se debe definir el modelo de gestión de información que la organización tendrá, el cual debe contemplar el ciclo de vida de los documentos, el acceso a los documentos, la orientación a procesos (transversales o departamentales), a funciones (estructura orgánico-funcional) y a los repositorios oficiales de almacenamiento y conservación. Como ejemplo tendríamos el que la organización defina si toda su gestión será electrónica (o no) y en caso afirmativo, si todos los documentos físicos deben digitalizarse, que defina si se tendrá acceso en línea a la visualización de los documentos electrónicos o si será solo referencial y con alguna autorización posterior se podrá visualizar su contenido, que defina si orientará su gestión a procesos o a funciones, que establezca cuál y dónde deberá residir la información oficial (Pc's, cd's, servidores de archivo, cintas, dispositivos externos, etc.).

Se deben establecer aquellos aspectos que permitan la operacionalidad del modelo en el «día a día» detallando la infraestructura funcional, operativa, técnica y tecnológica que soportará lo previamente definido. Se deben instaurar los estándares y esquemas de clasificación (taxonomía) y descripción (tanto el nombre de los archivos como los metadatos), la arquitectura tecnológica (producto Management, estándares de la industria de IT y la automatización de flujos de trabajo) y las herramientas y métodos que permitirán realizar los procesos de archivos (descarte, transferencia, disposición final), conservar y consultar la información y automatizar la TRD. Dentro de los productos management están records management; document management; e-mail management; content management, etc.

Un caso de negocio real y de impacto permitirá evidenciar las ventajas y dificultades de implantar el PGDE en la organización, para lo cual se debe establecer cuál caso evidenciará un retorno a la inversión (ROI: *Return of Investment*). Este porcentaje cuantitativo permitirá evidenciar qué tan eficiente es el gasto que se le pide a la organización realizar respecto al beneficio que obtendrá, en particular revisado sobre la información (compartida, oportuna, vigente, correcta, etc.) y los nuevos servicios de información. Igualmente, haciendo evidentes los beneficios al acceder, controlar, ubicar y recuperar la información.

Establecer claramente los requerimientos funcionales, tecnológicos, de seguridad y de implementación del PGDE; y finalmente garantizar un continuo y efectivo mantenimiento al programa implementado mediante indicadores de gestión que permitan evidenciar la productividad.

Es muy importante mencionar que muy pronto la gestión documental pasará a ser un aspecto más a tener en cuenta en el funcionamiento orientado a la mejora continua de cualquier sistema organizacional, en el sentido que va a ser un «sistema de gestión» certificable dentro de los sistemas de gestión (como los son hoy los sistemas de Gestión de Calidad ISO 9001, Gestión de Seguridad de la Información ISO 27001 y Gestión del Medio

Ambiente ISO 14001). Se están desarrollando las ISO de los sistemas de gestión para la información las cuales permitirán certificar dicha gestión (es decir, es un estándar de rango MMS – Management System Standard). Ya están disponibles para consulta la ISO 30300 «Fundamentos y vocabulario» y la ISO 30301 «Requerimientos».

VI. Seguridad de la información

a) Generalidades de seguridad de la información:

1. Es necesario que los pilares o principios de seguridad se garanticen durante todas las etapas del ciclo vital de los documentos electrónicos:

   Disponibilidad - Confidencialidad - Integridad - Confiabilidad

2. Cada pilar de seguridad debe garantizar durante el ciclo vital los siguientes aspectos:

   a. **Disponibilidad.** Significa que la información exista, se pueda ubicar, recuperar, visualizar e interpretar. Que no se presenten interrupciones en el servicio de consulta de la información que impidan el acceso a los documentos y que en cada consulta específica se garantice la recuperación de la totalidad de la información de un trámite a la que cada usuario tiene acceso.
   b. **Confidencialidad.** Que se mantenga la reserva propia de la información en cada etapa de su ciclo vital, de tal manera que sea accedida únicamente por las personas autorizadas y que se minimicen (o invaliden) las posibilidades de que sea interceptada.
   c. **Integridad.** Que se tenga identificado cuál es y dónde está ubicado y referenciado el documento electrónico «original», y que se garantice que está completo en su contenido individual y completo el trámite en la cantidad total de documentos electrónicos que participaron en el mismo. Igualmente, que el contenido no ha sido modificado, ni que se han fabricado

documentos electrónicos que realmente no existieron durante el trámite. Igualmente establecer en cualquier etapa del ciclo vital quién fue el creador del documento electrónico.

d. **Confiabilidad.** Un documento podrá ser considerado confiable, solo si existe un procedimiento preciso, claro y debidamente aprobado que autentique los procedimientos de generación de la información, su conservación temporal cuando fuere necesario y su almacenamiento definitivo que garantice que el mismo es oficial dentro de los procesos de la organización.

3. En cuanto a los diferentes servicios de seguridad se deberían garantizar los siguientes aspectos:

   a. **Autenticación.** Este servicio debe estar integrado con los mecanismos de autenticación a la red interna de la organización y por lo tanto al directorio activo del sistema de red utilizado.
   b. **Autorización (roles, perfiles y controles de acceso).** Este servicio debe permitir de manera fácil la creación y configuración de los roles y perfiles que sean necesarios dentro de la implantación y parametrización de una solución de gestión documental.
   c. **No repudiación.** Este servicio debe permitir demostrar que la información involucrada en un evento corresponde a quien participa en el mismo, quien no podrá desconocer su intervención en dicho evento.
   d. **Auditabilidad y observancia.** Este servicio debe permitir registrar los principales eventos (acciones y actividades) sobre la información; es decir, que permita auditarlos, así como realizar el monitoreo y la revisión periódica de los mismos.

b) Seguridad de la información durante su ciclo vital

Los aspectos de seguridad de la información enunciados deben garantizarse durante cualquier etapa del ciclo vital de los documentos

electrónicos, independientemente del soporte en el que resida y del formato del archivo. Igualmente, asegurar que la gestión documental se realice con o sin el apoyo de una tecnología determinada. Estos aspectos de seguridad deben existir en la documentación del proyecto por cuanto involucran a las personas, la tecnología, los procedimientos y la reglamentación, de tal manera que se pueda garantizar tanto su aplicación como la posibilidad de demostrarla. Si bien se aplican durante todas las etapas del ciclo vital, se presentan principalmente en las etapas de almacenamiento y consulta de los documentos electrónicos.

Desde el punto de vista tecnológico, la implementación de un Sistema de Gestión de Documentos Electrónicos (SGDE) apoyado en tecnología debe contar con un módulo que permita administrar la seguridad por el administrador del sistema. Se deben poder aplicar los criterios de seguridad a nivel de: documento, carpeta, proceso y serie documental, así como por individuo, rol, estructura jerárquica y organización. Igualmente, se debe dejar rastro o evidencia de los principales eventos o acciones a nivel de: documento, su gestión (acceso y trámite) y su conservación, consulta o descarte.

Debe proveer integración con la plataforma de certificados digitales que utilice la organización, de tal manera que permita desencriptar, verificar firma y abrir una copia en texto claro de los archivos seleccionados, una vez que las personas que realicen la consulta se hayan autenticado previamente ante la entidad certificadora y estén autorizadas para acceder al archivo.

Los aspectos de seguridad deben estar disponibles durante el mismo tiempo en que se conserven los documentos electrónicos.

Dado que son activos dentro de una organización, el software, el hardware y la información se deben establecer aquellos aspectos importantes de seguridad que involucren dichos activos.

Amenazas: Son circunstancias que potencialmente causan pérdidas:

- Desastres naturales
- Errores humanos inadvertidos
- Fallas de hardware o software

Vulnerabilidad: Debilidad en el sistema de seguridad que descubierta causa pérdida (hackers o crakers).

Nivel de exposición: Una forma de posible pérdida.

Riesgo: La probabilidad de que la amenaza suceda.

Control: Medida de protección (acción, dispositivo, procedimiento, técnica) para minimizar o mitigar la materialización de los riesgos.

Acorde con lo anterior, existen amenazas a los sistemas de información o a la misma información electrónica tales como: **Interrupción** o denegación del servicio, borrado de datos, mal funcionamiento, pérdida del activo. **Intercepción,** robo, copia de programas, copia de datos. **Modificación** del activo. **Fabricación,** es decir adicionar registros, datos o transacciones.

En términos de seguridad informática se pueden utilizar las siguientes herramientas como métodos de defensa:

Encripción. Codificar o cifrar la información de tal manera que hace su contenido ilegible a un tercero. De esta manera invalida (no evita) las amenazas de intercepción, modificación o fabricación y garantiza la confidencialidad de la información. Puede ser:
Simétrica: utilizan la misma clave para encriptar y desencriptar.
Asimétrica: utilizan claves diferentes para encriptar y desencriptar.

Autenticación: Comprobar la identidad de un usuario.
SYK: Something you Know. Ej: password.
SYH: Something you Have. Ej: tarjeta o smart card.
SYA: Something you Are. Ej: mecanismos biométricos (retina, huella, voz).

Autorización (perfiles): Asignar permisos a un usuario autorizado sobre los recursos existentes con unas reglas pre-establecidas.

No rechazo (non-repudation): Probar y garantizar el origen de una acción.

Firmas electrónicas. Es un valor numérico codificado que se adhiere a un mensaje de datos. Cuando una persona registra una firma digital, recibe una llave pública que se distribuye a los interesados y una llave privada que nadie debe conocer y que permite al receptor probar la fuente y la integridad de los datos.

Para que una firma digital sea válida debe ser única, verificable, estar bajo control exclusivo del firmante, estar ligada a la información del mensaje y cumplir con la reglamentación correspondiente. Cada firma digital de una misma persona que se estampa en varios documentos es diferente, ya que corresponde a ese único documento.

El certificado de firma digital es un mensaje de datos firmado por la entidad certificadora que identifica a quien lo expide y al firmante e incluye la clave pública de éste.

Log´s de auditoría:

- Registros de eventos de un sistema
- Intentos exitosos y fallidos
- Imagen actual e imagen anterior
- Políticas de revisión periódica

Planes de contingencia: Son útiles para garantizar la continuidad en el negocio recuperándose rápidamente ante desastres. Requiere detallar un plan de recuperación de desastres y un plan de continuidad del negocio.

Políticas de control: Definen los lineamientos sobre las acciones de control de sistema; estas acciones fijan las características de un sistema que permiten a la administración ejercer una dirección de restricción sobre su comportamiento, uso o contenido:

- ❑ Segregación de funciones
- ❑ Controles al ingreso de datos
- ❑ Controles contra virus
- ❑ Controles de operaciones rechazadas o en suspenso
- ❑ Controles de procesamiento
- ❑ Controles al software
- ❑ Controles al hardware
- ❑ Controles a las instalaciones físicas
- ❑ Políticas de seguridad

Algunos estándares:

- ISO 27001: Sistema de Gestión de Seguridad de la Información.
- ISO/TR 15801: 2004 Electronic imaging - Information stored electronically - Recommendations for trustworthiness and reliability.
- ISO/TR 18492: 2005 Long-term preservation of electronic document-based information.
- ISO 19005-1: 2005 Document management - Electronic document file format for long-term preservation - Part 1: Use of PDF 1.4 (PDF/A-1).

VII. El Programa de Gestión de Documentos Electrónicos - PGD

El PGD debe formar parte de la Planeación Estratégica de la organización que comprende planeación, diseño, documentación y desarrollo, y del establecimiento de los subprogramas que se abordarán. Cada subprograma debe ser parte integral del proceso archivístico.

Etapas de un PGD[i]:

1. **Producción documental.** Generación de documentos de las instituciones en cumplimiento de sus funciones.
2. **Recepción de documentos.** Conjunto de operaciones de verificación y control que una institución debe realizar para la admisión de los documentos que son remitidos por una persona natural o jurídica.
3. **Distribución de documentos.** Actividades tendientes a garantizar que los documentos lleguen a su destinatario.

---

i Guía para la implementación de un Programa de Gestión Documental, Archivo General de la Nación - Colombia, Compilador Jorge William Triana Torres.

4. **Trámite de documentos.** Curso del documento desde su producción o recepción hasta el cumplimiento de su función administrativa.
5. **Organización de documentos.** Conjunto de acciones orientadas a la clasificación, ordenación y descripción de los documentos de una institución como parte integral de los procesos archivísticos.
6. **Consulta de documentos.** Acceso a un documento o grupo de documentos con el fin de conocer la información que contienen.
7. **Conservación de documentos.** Conjunto de medidas preventivas o correctivas adoptadas para garantizar la integridad física y funcional de los documentos de archivo, sin alterar su contenido.
8. **Disposición final de documentos.** Decisión resultante de la valoración en cualquier etapa del ciclo vital del documento, registrada en las tablas de retención y/o tablas de valoración documental, con miras a la conservación total, eliminación, y/o reproducción (que garantice la legalidad y perdurabilidad de la información).

Premisas para la implantación de un PGD

- **Información vinculada a los procesos, documentos en todos los soportes.** A la luz de los procesos de negocio se realizará el inventario de la información a partir del cual se realiza el cuadro de clasificación, se valora la información para establecer los tiempos de retención y se detalla aquella que tendrá fines de «archivo», por lo que el PGD debe contemplar todos los soportes (físico, técnico y electrónico), todas las etapas de la información y los diferentes repositorios de conservación. El inventario no solo debe registrar el «qué» sino debe cuestionarlo, es decir, cuál es realmente la información que DEBE ser creada en cada etapa (necesaria y suficiente), acorde con los requisitos legales, regulatorios, con las políticas organizacionales, y con las necesidades operacionales y administrativas de la entidad.

- **La información debe ser considerada como un «activo» más de la organización.** Los empleados deben reconocer que «no es» su información y conocer el «valor» de la misma.

- **Herramientas orientadas a los usuarios (procesos de negocio).** Los empleados aceptarán más fácilmente la gestión documental si logran ser

parte inherente de su quehacer dentro de los procesos y no como «tareas adicionales» a su labor en las que no logran establecer qué les aporta o genera valor a lo que hacen. Es indispensable que el usuario siga trabajando en el ambiente de trabajo que es conocido para él de tal forma que la implantación de las herramientas tecnológicas no tengan un impacto negativo.

- **Perfiles de acceso acorde con el ciclo de vida y los procesos.** Solamente se tendrán flujos documentales efectivos, si se logra tener los procesos modelados y documentados en herramientas dinámicas que garanticen su vigencia y actualización, es decir, en herramientas que exijan que los cambios ocurridos en la «vida real» queden inmediatamente contemplados en el modelo y en la documentación.

- **Procedimientos archivísticos a trámites cerrados.** Los tiempos para realizar cualquier procedimiento archivístico se cuentan a partir del cierre del expediente, el cual equivale al momento en que se cierra el trámite.

- **Principios de orden original y de procedencia.** Se deben garantizar los principios generales de la archivística en la gestión documental independientemente del soporte documental. Estos son **a. Principio de orden original.** Establece que los documentos deben organizarse de acuerdo con una secuencia lógica, según como surjan los trámites para los cuales han sido creados y/o recibidos, de tal manera que reflejan el desarrollo secuencial de las acciones. **b. Principio de procedencia.** Establece que para todos los documentos se identifica plenamente la dependencia productora (sea porque se los creó o los recibió desde el exterior para darles trámite). Este principio se aplica para la clasificación de los documentos, su transferencia y consulta.

- **Estándares de clasificación (taxonomías) y descripción (metadatos).** Los estándares que se establezcan deben estar definidos conjuntamente con los participantes de los procesos, deben ser socializados entre todos los que participan, aplicados y monitoreados para garantizar su cumplimiento. Si las herramientas tecnológicas permiten su automatización, se garantiza mayor efectividad para la gestión documental.

- **Definición de los documentos originales de archivo.** Es indispensable que la organización defina claramente cuáles, dónde y cómo están los documentos electrónicos que se consideran «originales» y sobre los que se podrá dar autenticidad y tendrán - [cuando se requiera] - valor probatorio. Cómo, en qué momento y bajo qué procedimientos se oficializará un documento y cómo desde su oficialización es válido para la entidad y para la estructura archivística, permitiendo identificar la serie que conformará y sus tiempos de retención.

- **Expedientes por trámite y procedimientos archivísticos a trámites completos.** Es importante que se establezca y reconozca la necesidad de vincular toda la información de un mismo trámite desde que este se inicia y hasta su finalización; lo anterior permitirá que los procedimientos archivísticos (descarte, transferencia, disposición final) se realice a «todos» los documentos del trámite.

- **Centralización normativa y descentralización operativa.** Es importante que exista dentro de la organización la dependencia funcional que realizará el monitoreo al cumplimiento de la normatividad expedida por las instancias de gobierno, por cuanto dicha operatividad depende de cada uno de los productores de información.

- **Almacenamiento de documentos normalizado, estandarizado y automatizado.** Dado que el proceso tiene información de las tipologías documentales, sus características básicas (metadatos) y las reglas de negocio a aplicar no se debe dejar al usuario la decisión de determinar cómo almacenar el documento (ubicación, formato, metadatos, etc.).

Programa de Gestión Documental acorde con las fases del ciclo vital de los documentos

Producción. Es la determinación de uso y finalidad de los documentos y la relación entre los documentos recibidos y enviados. Consta de los siguientes momentos:

Creación. Es la generación de documentos en cumplimiento de sus funciones:

- La totalidad de los documentos deben crearse desde una única interfaz para los usuarios.
- Se debe propender por contar con tipologías específicas para acciones específicas; es decir, eliminar documentos genéricos como el memorando (en los casos que aplique y definir la tipología más apropiada para contener la información que requiere el trámite).
- **Gestión de formas y formularios.** Se debe realizar el diseño, normalización, estandarización, catalogación, estructura del contenido y manejo de versiones de las tipologías documentales por proceso, dejando como únicas aquellas que son comunes a varios procesos, debe contemplar la catalogación de aquellos formatos que se generan de manera automática desde los sistemas de información corporativos y los que se publiquen en la Web, independientemente de que dichos formatos sean realizados de forma preimpresa o como plantillas electrónicas. Se debe centralizar esta gestión en la dependencia que tiene a su cargo la gestión documental. Deben existir plantillas electrónicas independientes de que el documento final se reproduzca en soporte papel o permanezca en soporte electrónico, dichas plantillas deberían publicarse garantizando la última versión y ser parte integral de la TRD. Para el efecto deberán existir plantillas estructuradas (formularios), semi-estructuradas (documentos de correspondencia) y no estructuradas (informes).
- **Racionalización de la producción documental.** Se deben establecer los tipos documentales, la cantidad de copias y el control de la producción de nuevos tipos de documentos. En el mundo electrónico es necesario determinar claramente el porqué se requieren copias de estos documentos, su ubicación, acceso y uso, igualmente se debe garantizar como mínimo «la copia» con fines archivísticos, la cual se convierte para la organización en el «original» de archivo.
- **Determinación de los soportes y sus características.** Soporte físico: tintas, colores, tamaños, diseño; electrónicos: formato del archivo, medio de almacenamiento, tamaño del archivo, periodicidad de generación y estructura. Debería propenderse a que todo documento que se cree quede radicado y se tenga establecido si será electrónico y/o físico (por tipología documental). Es decir, todo documento físico o electrónico debe tener un

identificador único que permita garantizar su «creación» como documento oficial y su ubicación durante el ciclo de vida.

- **Oficialización de un documento.** Se debe documentar dentro del proceso el evento y las acciones que oficializan un documento electrónico dentro de la organización. Cada documento creado en la organización debe tratarse durante su ciclo vital como una unidad; es decir, se deben identificar cuáles fueron los archivos anexos al mismo - [si existieron] -.
- **Identificación de los metadatos.** Aquellos que son comunes a la organización y particulares acorde con el proceso y la tipología documental que garanticen la recuperación del documento durante el ciclo vital:
    - Los que son propios del tipo documental y del sistema.
    - Los que son propios del contenido.
    - Los que son propios del proceso de negocio.
    - Los que son propios del proceso de archivo.
- **Diplomática documental.** En términos de formalidad, imagen corporativa, características internas y externas, tipo de letra, firmas autorizadas, etc.

Recepción. Es el conjunto de operaciones de verificación y control que una organización debe realizar para la admisión de los documentos que son remitidos por una persona natural o jurídica.

Gestión de correspondencia. Se deben establecer aquellas actividades tendientes a garantizar que los documentos lleguen a su destinatario de manera oportuna e íntegra:

- **Definición de las ventanillas y los medios oficiales de recepción y despacho.** Con el propósito de garantizar la realización de los procedimientos oficiales para recibir los documentos se deben establecer «ventanillas únicas» tanto para los documentos físicos como para los electrónicos; entrega y/o recibo de documentos personales, mensajería, fax, correo tradicional, apartado aéreo, correo electrónico, página web, trámite en línea y otros.
- **Recepción y radicación.** Se debe establecer y capturar la metadata de todo documento físico y electrónico que se reciba oficialmente, sea tanto

un documento externo que llega a la organización como de un documento interno que debe ser despachado al exterior de la misma. En el mundo electrónico se aplica para todos los canales de ingreso de información electrónica (correo electrónico, transferencia de archivos, etc.).

- **Distribución.** Es la identificación de la dependencia competente para realizar el trámite independientemente del destinatario de la comunicación. Comprende actividades como:
  - Clasificación de comunicaciones, enrutamiento de documentos a la dependencia competente, reasignación de un documento mal direccionado, registro de control de entrega de documentos.
  - En el mundo electrónico se debe decidir si lo que se envía son los hipervínculos a los documentos almacenados desde su creación o copia de los documentos.
- **Despacho.** Son los acuerdos de servicio, medios oficiales, pruebas de entrega conservadas con la comunicación. Comprende actividades como: control de comunicaciones oficiales despachadas, control del cumplimiento de requisitos del documento (ej: firmas autorizadas) y el registro de control de envío de documentos y entrega al destinatario final.

Trámite (uso). Es el curso del documento desde su producción o recepción hasta el cumplimiento de su función administrativa. Comprende:

- Definición de los periodos de vigencia y tiempos de respuesta.
- Vinculación de antecedentes y compilación de información.
- Documento de respuesta.

Gestión propia del proceso de negocio. Comprende:

- Modelamiento y automatización de flujos documentales.
- Identificación de documentos oficiales (esenciales, administrativos, técnicos) requeridos por el proceso (declaración).
- Relación con otros documentos (correspondencia, intermedios, salida).
- Qué actividades o eventos del proceso deberán considerarse dentro del flujo documental y por lo tanto conservarse conjuntamente con los documentos.

Organización

Es el conjunto de acciones orientadas a la clasificación, ordenación y descripción de los documentos de una organización como parte integral de los procesos archivísticos.

Descripción (metadatos[ii])

Se definen como aquella información que describe información, de tal manera que detallan el **contexto, contenido y estructura** de los documentos y permiten evidenciar la **gestión** durante todo su ciclo de vida (describir las políticas que rigen los documentos e identificar y describir los individuos, procesos y sistemas que los crean). Los metadatos permiten la accesibilidad y uso de los documentos a largo plazo, facilitan establecer su autenticidad, fiabilidad e integridad, protegiendo el valor de los documentos como prueba, favorecen la recuperabilidad, sostenibilidad e interoperabilidad de los mismos a través de los sistemas que los gestionan, proporcionan herramientas para generar los vínculos entre los documentos y el contexto de su creación y uso, y mantienen su estructura y legibilidad de una forma fidedigna e inteligible, permiten identificar el entorno tecnológico en que se crearon y los sucesivos en que han sido utilizados garantizando una migración eficiente y completa.

Si bien la gestión documental en soporte tradicional ha incluido tradicionalmente los metadatos, en el entorno electrónico las características de los documentos deben estar **explícitamente** documentadas debido a que no pueden deducirse del contexto en el que se han generado; igualmente se deben asignar roles y responsabilidades tanto para quienes definen, asignan y promulgan el esquema de metadatos a utilizar como a todos los empleados de la organización que creen, capturen o gestionen documentos.

Es importante definir aquellos metadatos que serán comunes a la

ii Presentación INDRA titulada «Los elementos de implantación más desarrollados: el esquema de metadatos ISO 23081, 28 de noviembre de 2005 de María del Valle Palma Villalón. INDRA es la multinacional de Tecnologías de la Información número uno en España y una de las principales de Europa y Latinoamérica.

organización (metadatos institucionales). Para que realmente el uso de metadatos aporte a la gestión documental estos deben utilizar una terminología y vocabulario controlado, definido en catálogos de información, (para los institucionales), debe definirse los estándares para los metadatos que son específicos a cada proceso y gestionarse mediante la promulgación y revisión de la normatividad que los rige y de la implementación de las estructuras que los incorporan, para así lograr una arquitectura de información unificada.

Categorías de metadatos[iii]. Pueden ser:

- **Descriptiva o de contenido.** La información describe el contenido y es utilizada para facilitar y mejorar la búsqueda y recuperación de información por parte del usuario.
- **Estructural.** La información relaciona el documento con otros, ej: un documento dentro de un folder, dentro de un expediente, dentro de un trámite.
- **Administrativa o de uso.** La información es utilizada para gestionar y controlar el acceso al documento (oficialización, acceso, revisión, utilización y almacenamiento).
- **Gestión archivística.** Está conformada por la clasificación, conservación, preservación y la disposición final.

Clasificación (taxonomía)

Es la definición de la estructura y organización jerárquica bajo las cuales se clasificarán los documentos garantizando así una categorización de la información para ubicar correctamente la información que apoya un mismo trámite o designa un mismo concepto, de tal manera que se debe establecer la relación de equivalencia entre todos los términos de la taxonomía y los procesos de la organización.

La organización de la información conducirá a la formación de un archivo que: es soporte de las operaciones, facilita la rendición de cuentas, contiene la

iii La norma **ISO 23081/2004** es una guía para entender, implantar y usar los metadatos en el marco normativo de la ISO 15489.

memoria institucional, simplifica el trabajo y fomenta una mayor productividad permitiendo que los empleados disminuyan el tiempo dedicado a obtener la información que necesitan.

Se debe establecer un vocabulario común y compartido que los empleados puedan utilizar para nombrar y organizar sus documentos.

Existen diferentes tipos de taxonomías, tales como:

Taxonomía temática. Los documentos se clasifican acorde con el tema. Tiene como ventaja que es reconocida fácilmente por la mayoría y existen esquemas y estructuras predefinidas; tiene como desventaja que requiere de un conocimiento y entendimiento detallado de la terminología utilizada en la organización o la herramienta tecnológica debe soportar un amplio tesauro.

Taxonomía jerárquica. Los documentos se clasifican acorde con la dependencia productora. La ventaja es que el productor tiene muy clara esta información; pero como desventajas se encuentran los cambios de estructura organizacional, ya que obligan al mantenimiento de la taxonomía, aquellos documentos compartidos son difíciles de clasificar y en el futuro no es clara la dependencia que debió producir el documento.

Taxonomía funcional. Los documentos se clasifican acorde con las funciones y/o actividades que los producen.

Las series documentales definidas deberán corresponder a los procesos que se identifican para el cumplimiento de las funciones de la organización, las cuales deberán contener los diferentes expedientes que generan los trámites.

Consulta

Se refiere al acceso a un documento o grupo de documentos con el fin de conocer la información que contienen. En la consulta de documentos electrónicos se deben definir los siguientes aspectos:

- El establecimiento de las herramientas de consulta y los instrumentos de recuperación como guías, inventarios, catálogos e índices y la actualización permanente de estos instrumentos.

- Si se permitirá la consulta en línea de los productores de la información, independientemente de la etapa en que esta se encuentre, o si se requerirá una solicitud de consulta a los archivos para otorgar acceso.
- Tanto en etapa de gestión como en etapa inactiva, se debe garantizar la disponibilidad de los expedientes o de las fuentes de información completas y asociadas al trámite que las generó.
- Se requiere que los perfiles de acceso a la información se modifiquen acorde con la etapa del ciclo de vida en que se encuentren los documentos de tal forma que permita ampliar la consulta a los usuarios de la siguiente etapa, así:
  - Durante la **etapa de producción,** estos deben ser consultados por las personas que intervienen en el proceso (los creadores de los documentos y/o las áreas de correspondencia o despacho).
  - Posteriormente, para su **trámite**, deben ser consultados por los destinatarios de los mismos y por todos los responsables de su trámite.
  - Luego, en la **etapa activa**, por las personas que manejen los archivos en esta etapa activa.
  - Finalmente, si son transferidos a la **etapa inactiva** por los responsables del archivo en esta fase.
- Una vez ubicada la información se debe garantizar su recuperación, visualización e interpretación.
- Determinación de la necesidad y precisión de la consulta; determinación de competencia de la consulta; condiciones de acceso; disponibilidad de información en términos de restricciones por reserva o por conservación; reglamento de consulta; evaluar de qué tipo de información se debe dejar rastro y registro de su acceso y consulta.
- Redefinir en el mundo electrónico los conceptos de préstamo, de entrega de los originales, de devolución de los documentos.

Conservación

Es el conjunto de medidas preventivas o correctivas adoptadas para garantizar la integridad física y funcional de los documentos de archivo, sin alterar su contenido.

- **Repositorios oficiales y formatos de los archivos.** Es indispensable establecer los repositorios oficiales de conservación en etapa de gestión y en etapa inactiva, así como los formatos y características de seguridad de los archivos electrónicos que se aceptarán en esta última etapa.
- **Continuidad versus archivo.** Se tiene que diferenciar los medios y los procedimientos para el almacenamiento de información con propósitos de continuidad y con propósitos de archivo como:
  - Programas de mantenimiento de las unidades de almacenamiento.
  - Copias.
  - Diferenciar responsabilidades respecto al mantenimiento de los espacios físicos, instalaciones eléctricas, iluminación, humedad y temperatura.
- **Conservación del contexto de los archivos.** Es necesario garantizar la conservación del contexto de los archivos: metadatos, el archivo, su ubicación física, el medio de almacenamiento físico y lógica: la ruta (path) de ubicación del archivo.

Disposición final

Se debe culminar con la decisión resultante de la valoración en cualquier etapa del ciclo vital del documento, registrada en las Tablas de Retención Documental (TRD) Tablas de Valoración Documental (TVD) con miras a la conservación total, eliminación, selección y/o reproducción que garantice la legalidad y perdurabilidad de la información. Comprende:

- **Valoración.** En el proceso de valoración, que permite establecer los tiempos de retención de los documentos, es importante diferenciar cuáles serán los documentos de archivo; es decir, aquellos que realmente soportan el desarrollo de las funciones de la organización de aquellos que no lo son y que por lo tanto son de apoyo, control o evidencia de acciones diferentes, sin querer decir que por esta razón dejen de contener información importante para el desarrollo del proceso.
- **Herramientas TRD o TVD.** Es importante que una vez establecidos los tiempos de retención (previo proceso de valoración) se cuente con una herramienta que permita automatizarlos.

- **Conservación total.** Si bien esta valoración permite identificar aquellos documentos con valor permanente para la conservación del patrimonio, es importante que se deje la evidencia entre las áreas involucradas (productores, tecnología, gestión documental) de los riesgos reales que implican en el entorno tecnológico comprometerse a tiempos «permanentes».
- **Descarte.** Se debe dejar constancia de la realización de este proceso de archivo y establecer cómo se ejecutará en el entorno tecnológico: reutilización del medio (reciclaje o sobre escritura), destrucción del medio y/o de la información contenida. Igualmente se debe establecer un procedimiento que permita realizar lo propio en las copias de continuidad.
- **Sistemas de control para la selección:** técnicas de muestreo, expurgos.
- **Reproducción que garantice la legalidad y perdurabilidad de la información:** medios alternos de conservación.

Seguridad de los documentos

Directrices para garantizarla en cada etapa del ciclo vital:

- Protección (integridad, disponibilidad).
- Confidencialidad (encriptación) o encriptación (encripción).
- Conservación y preservación (migración, copias).
- Reproducción y duplicación.
- Inspección y mantenimiento de instalaciones, control de condiciones ambientales, limpieza y control de plagas.
- Prevención de desastres.
- Planes de contingencia (copias de seguridad, protección contra incendios, robos, inundaciones, catástrofes naturales, atentados, guerras).
- Sensibilización y toma de conciencia.

Normalización

Asociada a los componentes del programa de gestión y los procesos:

– El gobierno de los Estados Unidos ha adoptado la norma ISO 15489-1 y

15489-2 como base para su norma de 'Records Management'.
- Análisis de los procesos de trabajo para la gestión de documentos ISO 26122.
- Guía de aplicación para la redacción de normas en relación a los requisitos de gestión de documentos en dichas normas ISO 22310.

Asociada a la captura de documentos desde soportes físicos:
- Guía de implementación para la digitalización de documentos ISO 13028.

Asociada al software que cumple los requisitos de ISO 15489:
- Dod 5015.2-std. Design criteria standards for electronic Records Management software applications.

Asociada a los metadatos:
- ISO 23081 (parte 1 y 2): Proporcionar un marco para crear, manejar y utilizar metadatos como datos que describen el contexto, contenido y estructura de los documentos y explicar los principios que los rigen.

Asociada a la legislación:
- En Estados Unidos se aprobó «The sarbanes-oxley Act» conocida como SOX.

Asociada al modelo:
- Moreq1 y Moreq2: Modelo de requisitos para la gestión de documentos electrónicos de archivo.

Cibergrafía: páginas WEB

MODELOS DE GESTIÓN, ESTÁNDARES, AGREMIACIONES Y MEJORES PRÁCTICAS

- La norma ISO 30301 punto a punto: http://www.iso30300.es/
- Modelo de requisitos para la gestión de documentos electrónicos de archivos. Especificación MoReq. Versión marzo 2001. <http://www.csi.map.es/csi/pg5m52.htm>
- Documentos electrónicos. Manual para archiveros. CIA. Madrid: Ministerio de Cultura, D.L. 2006 <http://www.mcu.es/archivos/docs/documentosElectronicos.pdf>
- NATIONAL ARCHIVES, The U.S. National Archives and Records Administration (NARA). <http://www.archives.gov/>; febrero 2012.
- Global community of information professionals AIIM,<http://www.aiim.org/>.
- Professional association and the authority on managing records and information (ARMA INTERNATIONAL) – paper and electronic. <http://www.arma.org>
- The Workflow Management Coalition(WFMC) <http://www.wfmc.org/>
- Gestión Documental Orientada a Procesos: http://www.archivobogota.gov.co/libreria/pdf/gestidoc_enfoc_procesos.pdf/

METADATOS

- Metadata for Preservation, CEDARS Project Document AIW01,: http://www.ukoln.ac.uk/metadata/cedars/AIW01.html/
- Metadata for digital preservation: an update: http://www.ariadne.ac.uk/issue22/metadata/

SEGURIDAD

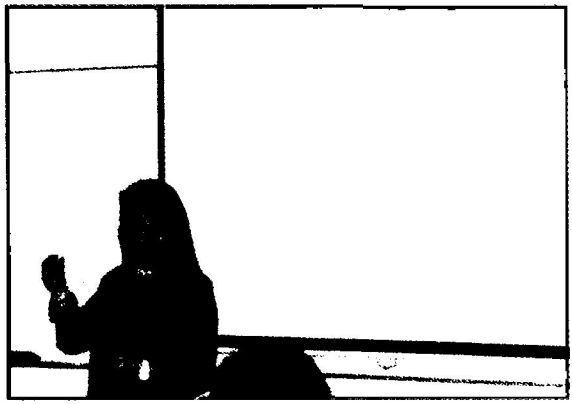
- Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades. Madrid: Ministerio de Administraciones Públicas, Secretaría General Técnica. 2004. <http://www.csi.map.es/csi/pg5c10.htm>

PRESERVACIÓN

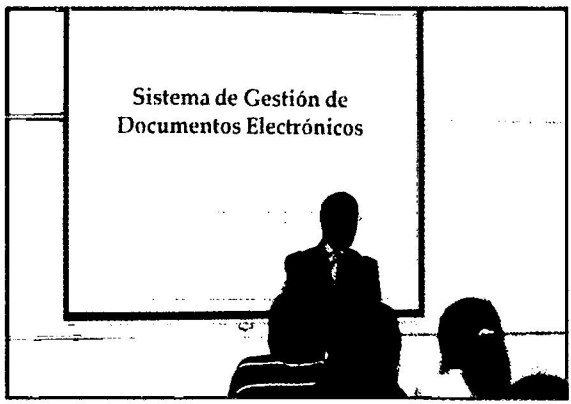
- The Preservation of the Integrity of Electronic Records: http://www.interpares.org/ubcproject/index.htm

TECNOLOGÍAS DE LA INFORMACIÓN

- Tech Republic Whitepapers <http://www.techrepublic.com/whitepapers?tag=wpbn>
- Workflow And Reengineering International Association, <http://www.waria.com/index-waria.html>
- Society of American archivists (SAA) <http://www2.archivists.org/>
- Noticias Tecnología: <http://www.diarioti.com>



Ingeniera Adalgisa Abdala en el Taller.



El Dr. Carlos Fosca, vicerrector administrativo de la Universidad, se dirige a los participantes en la inauguración del Taller.