Propuesta de Recomendaciones *para la* Gestión y Conservación *del* Correo Electrónico *en las Universidades Españolas*

Grupo de Trabajo Documentos Electrónicos de la Conferencia de Rectores de Universidades Españolas

ÍNDICE

1. Introducción.

El correo electrónico es hoy por hoy la aplicación más utilizada de la World Wide Web. Constituye una herramienta de comunicación, accesible a usuarios de todos los niveles, que permite el intercambio de mensajes electrónicos entre personas distantes en el espacio y en el tiempo. Las ventajas del correo electrónico sobre otras herramientas de comunicación son varias: rapidez, permanencia, y escaso o nulo coste de distribución, fundamentalmente; además de la posibilidad de adjuntar a los mensajes otra información sonora y visual, e incluso enlaces a recursos web. Esto ha convertido al correo electrónico no sólo en la forma de comunicación más habitual entre instituciones, sino también en el medio de comunicación más utilizado entre departamentos o unidades de la misma organización.

El correo electrónico tiene, sin embargo, una peculiaridad: su potencial permanencia lo sitúa a medio camino entre el carácter efímero de las telecomunicaciones y la constancia de los documentos escritos, lo que ha provocado que a menudo se consideren los mensajes de correo como una herramienta de uso personal y no como parte de la información corporativa. Para evitar esto y determinar su estatus dentro de la organización, instituciones de todo el mundo, incluidas universitarias, han publicado recomendaciones de uso del correo electrónico en consonancia con sus contextos legales y administrativos, y coherentes con sus proyectos de implantación de administración electrónica, así como con sus políticas de gestión y conservación de documentos digitales.

Este tipo de recomendaciones ayudan al personal a gestionar el correo de forma apropiada, consistente y eficaz; reducen el riesgo de pérdidas de información; y previenen al usuario con respecto a sus derechos (fundamentalmente su derecho de acceso y de protección de la intimidad/inviolabilidad de la correspondencia) y obligaciones (gestión de los correos como parte de la documentación producida por la entidad). Mediante un adecuado uso del correo se evitan inconsistencias en la documentación, desfases, vacíos y duplicaciones innecesarias. Por otro lado, la ausencia de una política institucional de prácticas de creación y gestión perpetúa la percepción de que el correo electrónico es una cuestión individual. El establecimiento de recomendaciones y guías de buenas prácticas no sólo conciencia de que el correo electrónico es una herramienta de trabajo, sino que ayuda a crear mensajes más consistentes.

Aunque muchas instituciones cuentan con unas recomendaciones relativas al uso y gestión del correo electrónico, que incluyen política de uso y privacidad, son pocas todavía las que han desarrollado políticas corporativas adecuadas de organización y conservación. La mayoría de las organizaciones se limitan a realizar copias de los correos (*back ups*) en los propios servidores, proceso que no cumple con las condiciones mínimas que permitan el acceso a esta documentación a medio o largo

plazo, quedando muchas veces la decisión de su conservación o eliminación en manos de los usuarios finales.

El objetivo de este trabajo es el establecimiento de unas líneas básicas que ayuden a las instituciones universitarias a diseñar sus propias políticas de gestión y conservación del correo electrónico. Este tema ya fue abordado por el grupo de trabajo de documentos electrónicos de la CAU en el documento "La Gestión de los Documentos Electrónicos: Recomendaciones y Buenas Prácticas para las Universidades", pero se ha considerado oportuno volver a hacer hincapié sobre la cuestión, especialmente desde la perspectiva de su vinculación con la implantación de la administración electrónica en los centros de enseñanza superior, teniendo en cuenta las implicaciones administrativas, legales y técnicas.

2. Estatus y problemática del correo electrónico.

Antes de abordar la cuestión del estatus documental del correo electrónico y la problemática de su gestión y conservación, resulta conveniente hacer algunas aclaraciones conceptuales. El **término** "correo electrónico" engloba al menos tres distintas acepciones[1]:

- es un medio de comunicación y de transmisión de información.

- es una herramienta que permite la transmisión de ficheros desde una dirección virtual a través de redes telemáticas y su recepción en otra u otras direcciones de forma tal que sea legible en la pantalla del receptor[2]. Un sistema de correo electrónico incluye los programas, las redes y los ordenadores (servidores y ordenadores personales) que posibilitan el intercambio de información en forma de ficheros. Este intercambio de información comienza con la composición misma del mensaje. Cuando los campos de la cabecera (asunto y destinatario) se completan y el usuario envía el correo, esta información se convierte en un fichero de formato normalizado especificado en la *Request for Comments* 2822 (RFC 2822), I*nternet Message Format*[3]*.* Utilizando una conexión de red, la aplicación cliente (Mail User Agent) conecta con un agente de transporte (Mail Transfer Agent) que opera en el servidor de correo, al que proporciona la identidad del emisor. A partir de este momento, la entrega del correo está bajo el control del servidor. Utilizando los servicios del sistema de nombre de dominio (Domain Name System), el servidor determina el servidor o los servidores de correo del destinatario o de los destinatarios. Si los buzones del emisor y el receptor están en el mismo servidor, el mensaje se entrega utilizando un agente local de entrega (Local Delivery Agent), si están en servidores diferentes el proceso de envío se repite de un agente de transporte a otro hasta que llega al buzón del destinatario[4].

---

[1] BANÚS GIMÉNEZ, Teresa y CORTÉS LONGARES, Marta: El Correu Electrònic: un Problema a Resoldre. En Lligall, n.25 (2003).

[2] Pueden proporcionar una serie de características añadidas, incluidas interfaces gráficas de usuario, herramientas avanzadas de edición y gestión de documentos, servicios de transmisión segura, directorios de usuarios, autenticación de mensajes, confirmación de entrega (acuse de recibo o de depósito) y/o de lectura (acuse de lectura).

[3] La RFC 2822 proporciona un estándar de transmisión de mensajes de texto, pero no es aplicable a mensajes que incorporan adjuntos. Utilizando la cabecera del mensaje, las especificaciones MIME (Multipurpose Internet Mail Extensions[3]), permiten la descripción de la estructura de cualquier tipo de fichero (imágenes, ficheros de audio, archivos multimedia, programas ejecutables,…).

[4] Los estándares de transporte se establecieron para garantizar la integridad y la interoperabilidad entre distintos programas de correo. En el escenario más sencillo, un mensaje es enviado de un usuario local a otro y el agente local es el responsable de su depósito en el buzón del receptor. En el caso de receptores externos, se necesitan agentes de transporte para enviar el mensaje que, en ocasiones, dependiendo de los

- también es el propio mensaje transmitido de un ordenador a otro mediante un programa de correo electrónico. Independiente de la aplicación utilizada para generarlos, los mensajes de correo se componen de dos elementos básicos: la cabecera y el cuerpo del mensaje. En el nivel más básico, la cabecera contiene información esencial sobre el mensaje (fecha, emisor, receptor, ruta de entrega, asunto e información sobre el formato), mientras que el cuerpo del mensaje incluye el contenido del mismo. La cabecera contiene información sobre el remitente, el destinatario, el asunto tratado o la fecha del envío. El cuerpo es el texto que el usuario teclea en el mensaje, que puede ser desde un texto sencillo en código ASCII hasta texto enriquecido. A estos dos componentes básicos puede añadirse un tercero: ficheros adjuntos y metadatos sobre estos ficheros. Los adjuntos pueden incluir cualquier tipo de archivo, desde un documento de texto hasta imágenes, ficheros multimedia, programas ejecutables o enlaces a páginas web[5].

Así pues, como cualquier otro documento digital, un mensaje de correo consiste en un conjunto de hardware, software y ficheros de información. En el caso del correo estos elementos se combinan entre sí de forma tal que pueden ser legibles por el emisor y el destinatario en el monitor de sus ordenadores.

La norma ISO 15489 define "documento" como "cualquier información creada, recibida y mantenida como evidencia e información por una organización o persona, en la consecución de sus obligaciones normativas o en las transacciones comerciales". Veamos en qué medida los mensajes de correo pueden considerarse documentos siguiendo esta definición:

- los mensajes de correo son "información creada o recibida por una organización o persona". Teniendo en cuenta este aspecto, los mensajes de correo electrónico podrían tener el estatus de "documento".

- "mantenida como evidencia": la fiabilidad del proceso o del sistema empleado para producir los documentos y no la tecnología utilizada es lo que determina la evidencia de los mismos. Las propias organizaciones han de establecer las condiciones de autenticidad que eleven el mensaje de correo a evidencia. Para ello tienen que mantener el contenido, la estructura y el contexto en que fueron generados.

- "en la consecución de sus obligaciones normativas o en las transacciones comerciales": cualquier mensaje de correo electrónico que se utilice como apoyo en un procedimiento dentro de una organización podría ser considerado "documento" (las políticas de gestión de los correos electrónicos deberían establecer qué correos electrónicos son documentos dentro de la organización y cuáles no).

El estatus del correo electrónico ha sido ampliamente debatido en Estados Unidos durante toda la década de los noventa. Tanto es así que algunos autores lo han

---

tipos de sistema implicados, pueden soportar distintas implementaciones de un mismo mensaje, usando distintos protocolos. El más común de estos protocolos es el Simple Mail Transfer Protocol (SMTP) que es el estándar para enviar mensajes a través de la red Internet. Una vez que el mensaje es recibido en el servidor del destinatario, el usuario puede acceder a su buzón a través de distintos métodos, siendo el más común el acceso directo. Para evitar los riesgos que este acceso suponía, se desarrollaron los protocolos Post Office Protocol (POP) y Internet Message Access Protocol (IMAP).

[5] Estos tres significados del término no se dan de forma aislada, sino entremezclada y, en ocasiones, simultánea. Sólo haremos la distinción entre ellos cuando consideremos que puede darse lugar a confusión.

calificado de "agujero negro"[6] de las políticas de gestión documental. Para intentar aclarar esta cuestión, la abordaremos desde tres puntos de vista: organizativo, legal y técnico.

Punto de vista organizativo

Desde el punto de vista organizativo, la utilización del correo electrónico ha contribuido sin duda a agilizar el intercambio de información en las instituciones, así como a facilitar el contacto entre los trabajadores y entre éstos y los usuarios finales de sus servicios. El entorno académico es un buen ejemplo de ello, pues el correo electrónico se ha convertido en el medio más habitual de comunicación entre los distintos colectivos universitarios, pero, sobre todo, constituye una herramienta fundamental de contacto entre profesores y alumnos tanto en la formación a distancia como en la presencial. Sin embargo, como se ha señalado en la introducción, la propia indefinición del correo electrónico y su naturaleza a medio camino entre el medio de comunicación efímero y la herramienta susceptible de generar documentos de carácter más o menos permanente, constituye un primer obstáculo para su gestión y control. Una indefinición que afecta tanto a la utilización de la herramienta, como a los mensajes de correo generados por ella, y a la que se añade el uso privado que se hace a menudo de la misma.

En la mayoría de las organizaciones se recibe y envía un gran volumen de correos que incluyen mensajes publicitarios no solicitados (*spam*); bromas con amigos, familiares y compañeros; intercambio de ficheros de todo tipo, mensajes automáticos de confirmación, mensajes de foros de debate… En definitiva, el correo electrónico es utilizado en muchos casos como un **medio de comunicación de carácter privado**. Esto conlleva varios problemas desde una perspectiva institucional: el tiempo invertido por el trabajador para atender asuntos personales, el empleo de los equipos de la institución o la vulnerabilidad de la seguridad de las comunicaciones. Además, la ausencia de unas recomendaciones sobre el uso del correo provoca que muchos correos profesionales tengan el mismo aspecto y estén redactados en el mismo tono que los personales. Los usuarios no se detienen a considerar que muchos de los correos que emiten diariamente en el desarrollo de sus tareas contienen imprecisiones o expresiones incorrectas, que pueden dañar seriamente la imagen corporativa.

Además, amparados por una falsa ilusión de privacidad e intimidad, los **trabajadores** pueden verse envueltos en conflictos con la propia universidad/institución o con sus colegas, ya que aunque la mayoría de los países recogen en sus legislaciones la privacidad de las comunicaciones como un derecho fundamental, este derecho puede verse amenazado por la titularidad de la herramienta utilizada para el envío y la recepción de los mensajes[7].

---

[6] Sutton, Michael J.D.: *Document Management for the Enterprise: Principles, Techniques, and Applications* (New York: John Wiley & Sons, Inc., 1996), p. 100. Citado por Wallace, David Recordkeeping and Electronic Mail Policy: The State of Thought and the State of the Practice (consultado el 5 de abril de 2010).

[7] Considerado como un medio de comunicación entre individuos, el correo electrónico, como el postal, se encuentra protegido por el artículo 18.3 de la Constitución Española de 1978, que establece la inviolabilidad de las comunicaciones, lo que ha desatado una polémica en torno a la legalidad de la interceptación del correo y la propiedad de los mensajes que se transmiten por este medio de comunicación en el ámbito laboral. Algunos juristas proponen una nueva interpretación de la ley en le medida que consideran que el titular de la cuenta no es el dueño de la misma, sino la propia institución, que se la asigna al funcionario o trabajador para su uso y administración en nombre del cargo que desempeña y para fines estrictamente laborales. Un intento de solución a este problema ha sido el establecimiento de dos cuentas de correo: correo institucional y privado.

La consideración del correo electrónico como un medio de comunicación personal ha provocado también que la organización y el archivado de este tipo de ficheros electrónicos, quede al criterio de los usuarios. Incluso las organizaciones que han establecido unas normas para la utilización de esta herramienta han dejado a un lado la clasificación y el archivo de los ficheros generados por la misma, así como las recomendaciones relativas a la eliminación de la información almacenada en las carpetas personales o la gestión de cuentas de correo en caso de cambio en el puesto de trabajo (con la consiguiente pérdida de información para las decisiones administrativas). Los usuarios son en muchos casos los únicos responsables de la conservación de los mensajes enviados al no existir una política institucional que establezca condiciones y plazos de conservación.

La falta de conciencia de los **gestores**, también ha supuesto que el correo no se trate como un instrumento susceptible de generar documentos electrónicos íntegros y auténticos y de ahí que exista una cierta desconfianza en los usuarios. A pesar de que muchos mensajes de correo encajan perfectamente en la definición que de "documento" establece la norma ISO 15489, a menudo no se incluyen en las políticas institucionales de gestión de documentos, y, en consecuencia no se fijan normas para su clasificación, ni se dictan plazos para su conservación. Tampoco se estudian los requisitos técnicos para su conservación futura, ni las estrategias a seguir para ella, ni se diseñan procedimientos de recuperación de datos en caso de catástrofe (*disaster recovery plan*).

La falta de control y consiguiente pérdida información puede traer consecuencias legales, económicas (la ocupación de espacio en los servidores), y de imagen (pérdida de credibilidad, falta de transparencia, o deterioro en la provisión de servicios a los usuarios) inmediatas para nuestras instituciones. Además, a medio y largo plazo, podría verse seriamente afectada la conservación de correspondencia de figuras notables dentro del panorama científico, y gran parte incluso de la herencia cultural (las listas de distribución soportadas por las universidades y destinadas a la actividad docente e investigadora serían un buen ejemplo de esto[8]).

Por tanto, está claro que para conseguir una gestión eficaz en nuestras universidades, para mejorar la rendición de cuentas, el correo electrónico debe formar parte de la estrategia corporativa de información y gestión documental, de manera que todas las transacciones queden perfectamente documentadas independientemente del medio de comunicación que se utilice[9]. Para ello los mensajes electrónicos han de conservar su contenido, su estructura y el contexto en el que fueron creados, de forma tal que no puedan ser alterados o manipulados. En definitiva, es necesario tomar medidas para garantizar su autenticidad. Esto implica también una correcta gestión de la selección y el expurgo de los documentos que permita el aprovechamiento eficaz y eficiente de los recursos informáticos (hardware y software) al servicio de las organizaciones.

[8] La importancia de la comunicación informal creada en formatos digitales dentro del entorno científico es tratada en Lukesh, Susan: *E-mail and Potencial Loss to Future Archives and Scholarship or the Dog that Didn't Bark*
http://hofprints.hofstra.edu/13/01/Lukesh%2C_Susan_S._(1999)_E-mail_and_Potential_Loss_to_Future_Archives_and_Scholarship_or_The_Dog_that_Didn%27t_Bark._FirstMonday_4(9).htm (consultado el 5 de abril de 2010).

[9] La propia complejidad de los sistemas de correo (multiplicidad de tipos de ficheros que pueden adjuntarse, software y hardware diferentes en los ordenadores emisores y receptores, transmisión entre los servidores a través de redes telemáticas,…) ha convertido al correo electrónico en un auténtico percutor de las políticas de gestión y conservación de los documentos digitales en muchas organizaciones.

Las mejores prácticas para la conservación del correo electrónico todavía no han llegado a un consenso sobre cómo conseguir este objetivo. Sin embargo, la mayoría coincide en que las actividades de organización, las actividades culturales y los avances técnicos forman las tres áreas de impacto del éxito general de cualquier enfoque de conservación del correo electrónico.

Punto de vista legal

La mayoría de los países de nuestro entorno han desarrollado en sus derechos administrativos el *principio de documentación* de la actividad de los distintos organismos públicos, y cuentan con normativa concerniente a las condiciones de conservación de la documentación producida por dichos organismos, así como a los procedimientos a seguir en la destrucción de la misma. Muchas de estas normas se ocupan también de regular el acceso de los ciudadanos a los documentos de titularidad pública, fijando las condiciones y los límites de este derecho.

Sin embargo la doble naturaleza del correo que hemos visto en el apartado anterior (la consideración del correo electrónico como un medio de comunicación y como parte del sistema de información de la organización) lo convierte en una herramienta protegida por el derecho a la privacidad, contemplado en la Carta Magna europea y en la mayoría de las legislaciones nacionales de nuestro entorno. Con vistas a preservar este derecho en el nuevo contexto de la sociedad de la información se han ido desarrollando en los últimos años normas relativas al tratamiento de ficheros digitales y a la protección de datos personales que regulan las condiciones de seguridad de estos datos en los entornos automatizados[10] y que afectan también al tema que nos ocupa puesto que el correo electrónico se considera un conjunto de datos del usuario. El establecimiento de políticas claras de gestión, acceso y conservación de los mensajes de correo dentro de las organizaciones puede ayudar a evitar conflictos legales que supongan pérdidas económicas y deterioro de imagen.

En Estados Unidos la polémica en torno al estatus legal de los mensajes de correo producidos por la oficina presidencial se ha prolongado durante más de una década y ha llegado incluso a los tribunales de justicia[11] que han tenido que pronunciarse sobre el tema, dando lugar a una política de gestión del correo electrónico a nivel federal, que engloba desde la producción de los mensajes hasta su destino final (*General Retention Schedule 20*).

La legislación de los países integrantes de la Unión Europea no menciona el estatus del correo electrónico como documento público, aunque el derecho de acceso de los ciudadanos a la documentación administrativa, recogida en la mayoría de sus ordenamientos jurídicos, determina la exigencia de una gestión y conservación adecuadas de esta información[12].

---

[10] No entramos aquí en esta polémica aunque nos parece importante mencionarla para el objetivo de nuestro trabajo. Más información en: Digital Preservation Testbed. *From digital volatility to digital permanence* [en línea]*: Preserving email.* http://www.digitaleduurzaamheid.nl/bibliotheek/docs/volatility-permanence-email-en.pdf [Consulta: 2 marzo, 2010].

[11] En 1989 el periodista Scott Armstrong demandó a la oficina presidencial por el borrado de los correos electrónicos del gobierno de Ronald Reagan. La polémica ha sido recogida por Wallace en el artículo citado. La Federal Records Act obligaba a los funcionarios públicos a imprimir los mensajes de correo que pudieran considerarse documentos. Posteriormente se decidió borrar la versión electrónica de los correos, sin el consentimiento previo del NARA.

[12] Tampoco se recoge explícitamente en la Directiva 1049/2001 relativa al acceso del público a los documentos del Consejo.

- **Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco común para la firma electrónica.**

  Establece el marco jurídico europeo de la firma electrónica y de algunos servicios de certificación, con el fin de facilitar la utilización de la firma electrónica y de contribuir a su reconocimiento jurídico en los Estados miembros.

- **Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995** relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Constituye el texto de referencia, a escala europea, en materia de protección de datos personales. Crea un marco regulador destinado a establecer un equilibrio la protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea. La Directiva fija límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la protección de los mencionados datos.

- **Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002** relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

Nuestro país no cuenta con normas que traten de forma sistemática el tema de la validez, gestión y conservación de los mensajes de correo electrónico, ni de su estatus como documento administrativo. La legislación que le afecta más directamente se integra en el desarrollo de normas de procedimiento administrativo y de la aplicación de las nuevas tecnologías a dicho procedimiento (administración electrónica[13]). En líneas generales, podemos afirmar que la normativa española considera el correo electrónico como una herramienta susceptible de generar y transmitir documentos electrónicos con validez jurídica plena y establece los requisitos mínimos que serían exigibles para ello[14].

- **Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las administraciones públicas y de procedimiento administrativo común.**

  En el artículo 45 se establece que la Administración impulsará la utilización de los medios técnicos oportunos para el ejercicio de su actividad. También contempla la posibilidad de ofrecer a los administrados la utilización de medios electrónicos, informáticos y telemáticos para relacionarse con la misma, así como la capacidad de generar documentos válidos en soportes informáticos, siempre que quede garantizada su autenticidad, integridad y conservación. Dispone además que los programas y aplicaciones informáticas que se vayan a utilizar por las Administraciones en el ejercicio de sus potestades habrán de ser aprobados previamente por el órgano competente.

- **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal**.

  La Ley regula el tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar. Además de constituir un medio de comunicación, el correo electrónico se considera un conjunto de datos del usuario y, como tal, su manipulación se encuentra supeditada a las normas relativas a la protección de datos personales,

[13] Incluimos aquí las normas relativas a seguridad e interoperabilidad de las transacciones telemáticas en el ámbito del desarrollo del comercio y la administración electrónicos.
[14] En nuestro entorno de entidades administrativas reguladas por el derecho público (Ley de Procedimiento Administrativo) para que un documento sea considerado un documento administrativo con plena validez jurídica, tiene que ser "válidamente emitido".

pues los datos obtenidos a través de una cuenta de correo pueden proporcionar el perfil de un usuario, quedando vulnerada con ello su intimidad.

- **Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado**.
  El Real Decreto desarrolla el artículo 45 de la Ley de Procedimiento Administrativo en el ámbito de la Administración General del Estado. Se centra en la utilización de técnicas electrónicas, informáticas y telemáticas por parte de la Administración y establece los requisitos mínimos que han de cumplir los nuevos soportes, medios y aplicaciones. El artículo 5 contempla la comunicación a través de los medios informáticos entre las distintas entidades de la Administración General, y entre éstas y cualquier persona física o jurídica. Establece la posibilidad de utilizar programas y aplicaciones sin aprobación previa para tratamientos de información dentro de procedimientos que no supongan decisiones administrativas. El artículo 6 afirma que los documentos producidos por medios electrónicos serán válidos siempre que quede acreditada su integridad, conservación y la identidad del autor, así como la autenticidad de su voluntad, mediante la constancia de códigos u otros sistemas de identificación.

- **Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información.**

  Su Disposición Adicional Sexta ordena profundizar en la implantación del gobierno y la administración electrónica incrementando el nivel de participación ciudadana y mejorando la eficiencia de las Administraciones públicas.

- **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.**
  El Real Decreto regula en el ámbito de la Administración General del Estado, las notificaciones y los registros telemáticos. Modifica parcialmente el Real Decreto 263/1996, y especifica los términos en que han de habilitarse los sistemas de notificación telemática a los interesados. En su Artículo 12 contempla la necesidad de que todos los interesados que manifiesten su voluntad de ser notificados por medios telemáticos, dispongan de una dirección electrónica habilitada para ello y establece los requerimientos de la misma. También considera la sustitución de certificados en soporte papel por certificados digitales o por transmisiones de datos, y regula las condiciones de creación de registros telemáticos, así como sus funciones y requisitos de funcionamiento.

- **Ley 59/2003, de 19 de diciembre, de firma electrónica**

  Regula la firma electrónica, su eficacia jurídica y la prestación de los servicios de certificación que la avalan. Como se afirma en la exposición de motivos, la Ley pretende generalizar la confianza de los ciudadanos con respecto a las comunicaciones telemáticas, y favorecer así el desarrollo de la Administración y el comercio electrónicos. La Ley equipara la firma electrónica reconocida a la firma manuscrita y establece la equivalencia en valor y eficacia entre documentos en papel y documentos electrónicos autenticados con la firma digital. La firma electrónica “constituye un instrumento capaz de permitir una comprobación de la procedencia y de la integridad de los mensajes intercambiados a través de redes de telecomunicaciones”.

- **Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.**
  La Ley transforma la posibilidad de relacionarse con las administraciones públicas a través de medios electrónicos recogida en la Ley de Procedimiento Administrativo, en un derecho de los ciudadanos. Regula las comunicaciones electrónicas de los ciudadanos con las Administraciones y de éstas entre sí. En el artículo 27 del capítulo III,

"Comunicaciones electrónicas", se establece que el ciudadano puede elegir la manera de comunicarse con la Administración y los términos en que lo hará a través de las redes telemáticas. El capítulo IV "De los documentos y de los archivos electrónicos" establece las condiciones básicas de la emisión válida de documentos administrativos electrónicos contemplada en la Ley de Procedimiento Administrativo, así como los requisitos para su conservación.

- **Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.**
La finalidad de esta ley es muy concreta: poder identificar personas jurídicas y físicas en el caso de investigación de delitos. Aunque se centra en la telefonía fija y móvil, también incluye el correo electrónico. Establece la obligatoriedad de conservar los datos de identificación de los usuarios de correo electrónico así como la fecha, hora y duración de la comunicación. El período obligatorio de conservación será de 12 meses, pudiendo en determinados casos ampliarse hasta un máximo de 2 años. Sólo los agentes facultados para la investigación de delitos podrán acceder a estos datos.

- **Real Decreto 1720/2007, de 21 de diciembre, por el que se desarrolla la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.**
El Decreto modifica y amplía las medidas y niveles de seguridad recogidos en la Ley 15/1999 y establece la necesidad de documentar la seguridad del fichero por parte del responsable del mismo. Además, refuerza la información y obtención de consentimiento de los interesados en la recogida de datos personales y establece los requisitos para las transferencias internacionales de datos en función del país de destino y su nivel de protección.

- **Real Decreto 1671/2009 de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007 de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.**
Desarrolla la Ley 11/2007 en el ámbito de la Administración General del Estado haciendo especial hincapié en la regulación de la sede, la firma, el registro y el archivo electrónicos. El Título V "De las comunicaciones y las notificaciones" recoge las condiciones en que se realizarán las comunicaciones y notificaciones por vía telemática.

- **Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.**
Este Real Decreto tiene como finalidad crear las condiciones necesarias que garanticen la seguridad de los sistemas, de los datos, de las comunicaciones y de los servicios que permitan a los ciudadanos el ejercicio de derechos y cumplimiento de deberes a través de los medios electrónicos tal y como se establece en la Ley 11/2007. Dispone una serie de principios básicos y requisitos mínimos para desarrollar una política de seguridad en los medios electrónicos que permita la protección de la información. En el Anexo I se establecen las diferentes categorías en cuanto a nivel de protección de los sistemas de información. El Anexo II recoge las medidas de seguridad de dichos sistemas: la selección de las mismas, su marco organizativo, su marco operacional, los medios de protección de cada elemento del sistema (instalaciones e infraestructuras, recursos humanos, equipos, redes, soportes, aplicaciones; así como de la propia información y de los servicios); su desarrollo y su interpretación. El punto 5.8 dedicado a la protección de los servicios, hace referencia explícita al del correo electrónico:

"El correo electrónico se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

a) La información distribuida por medio de correo electrónico, se protegerá, tanto en el cuerpo de los mensajes, como en los anexos.
b) Se protegerá la información de encaminamiento de mensajes y establecimiento de conexiones.
c) Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto:
1.º Correo no solicitado, en su expresión inglesa «spam».
2.º Programas dañinos, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga.
3.º Código móvil de tipo «applet».
d) Se establecerán normas de uso del correo electrónico por parte del personal determinado. Estas normas de uso contendrán:
1.º Limitaciones al uso como soporte de comunicaciones privadas.
2.º Actividades de concienciación y formación relativas al uso del correo electrónico."

- **Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica**. Establece los criterios y las recomendaciones que garanticen la interoperabilidad entre las Administraciones Publicas y entre éstas y los ciudadanos, permitiendo el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos. Este Real Decreto trata la interoperabilidad de los sistemas de información y de los procedimientos soportados por aquéllos de forma global, abordándola en sus dimensiones organizativa, semántica y técnica. También atiende a la conservación de la información, según lo establecido en la Ley 11/2007, como manifestación de la interoperabilidad a lo largo del tiempo, lo que afecta de forma singular al documento electrónico al que se dedica el Capítulo X "Recuperación y Conservación del Documento Electrónico".

De la consideración o no de los mensajes de correo electrónico como "documentos administrativos electrónicos" y, en consecuencia, de su titularidad pública, se derivará la aplicación de la legislación relativa a la conservación y acceso.

La revisión de estas normas permite extraer algunas **conclusiones**:

- el correo electrónico, como aplicación telemática de envío y recepción de ficheros informáticos, está llamada a jugar un papel protagonista en cualquier proyecto de administración electrónica. Las distintas administraciones tendrán que establecer las condiciones de seguridad e interoperabilidad necesarias para su correcto funcionamiento.

- como ha sucedido con otros medios de comunicación y otros soportes, el valor evidencial de correo electrónico es algo que tendrá que establecerse con la práctica[15].

- en función de ese valor habrá que estudiar la inclusión o no de los correos electrónicos en el expediente electrónico, así como las condiciones de esa inclusión.

- el hecho de que se utilice el correo en partes del procedimiento administrativo que no supongan la toma de decisiones y, en consecuencia, no afecten directamente a los derechos de los ciudadanos, no los convierte en ficheros desechables, ni justifica que las organizaciones no los incluyan en sus políticas de gestión documental.

[15] Aunque el principio de equivalencia de soportes no aparece expresamente proclamado en la Ley 11/2007, puede inferirse del artículo 45.5 de la Ley 30/1992, así como de otros preceptos de la Ley 11/2007. Véase Gomero Casado, Eduardo y Martínez Gutiérrez, Rubén: Legislación de Administración Electrónica y de Protección de Datos (pág. 27). Tecnos, 2008.

- aunque no todos los mensajes de correo puedan considerarse documentos con validez jurídica plena, su información puede ser esencial para un funcionamiento eficaz de la organización. De ahí que deban establecerse unos requisitos de seguridad que garanticen un correcto uso y una adecuada conservación de la información que contienen.

Punto de vista técnico

Desde el punto de vista técnico, la consideración del correo electrónico como documento administrativo digital plantea los mismos problemas y las mismas necesidades que el resto de documentos electrónicos, con algunas peculiaridades, como el hecho de que los mensajes pueden incluir ficheros en multitud de formatos y de que la representación tanto del propio mensaje como de los adjuntos pueden variar en el ordenador del emisor y del destinatario, de ahí que el fichero de envío esté desarrollado expresamente para salvaguardar la interoperabilidad entre distintas plataformas y la seguridad en la transmisión.

Para funcionar eficazmente, el correo electrónico, como cualquier documento digital, incorpora elementos tecnológicos correspondientes a los conceptos jurídicos, que garantizan la integridad y seguridad, como la firma electrónica y el sellado temporal básicamente. La propia naturaleza del correo hace necesario añadir a estos elementos otros, como el no repudio en origen y destino, que permitan asegurar el envío y la recepción y/o lectura del mensaje (correo electrónico certificado)[16].

No se trata aquí de realizar un análisis diplomático del documento electrónico, ni un estudio sobre los requisitos tecnológicos que puedan garantizar la autenticidad e integridad de un mensaje de correo. En primer lugar porque ya existe literatura profesional sobre la materia[17], y en segundo lugar porque excede el objetivo de este trabajo. Como se recoge más arriba, la evidencia de los documentos la determina la fiabilidad del proceso o del sistema empleado para producirlos y no la tecnología utilizada. Existen actualmente recursos tecnológicos que permiten desarrollar procedimientos seguros para la producción de documentos íntegros y auténticos, y para su transmisión a través de las redes telemáticas, aunque la capacidad de la técnica, condicionada por la obsolescencia tecnológica y los imperativos del mercado, para garantizar estas características del documento a lo largo de todo su ciclo vital es más cuestionable[18].

Por ello, resulta oportuno recordar que la conservación a medio y largo plazo se logra mediante medios técnicos, pero debe determinarse de acuerdo con **principios y criterios archivísticos**, y que una adecuada conservación sólo puede alcanzarse mediante apropiadas políticas documentales que incluyan la identificación, organización, descripción y valoración, y que comprendan una apropiada gestión de los documentos

[16] El acuse de recibo o no repudio en destino, forma parte de una familia de servicios en los que dos o más partes desean intercambiar elementos electrónicos, con la particularidad de que ninguna de las partes quiere entregar su elemento sin tener la garantía de que recibirá el elemento correspondiente.
[17] Duranti, Luciana: *La Conservación a Largo Plazo de Documentos Electrónicos Auténticos: Hallazgos del Proyecto Interpares*. Ayuntamiento de Cartagena, 2005.
[18] El Modelo de Requisitos para la Gestión de Documentos Electrónicos (Moreq2) editado por el DLM-Forum recoge los requisitos y metadatos que deben capturarse de los mensajes de correo con vistas a su conservación a largo plazo.

desde el momento de su producción[19]. Algunos de los problemas que plantea el correo electrónico con respecto a las tareas archivísticas son:

Con respecto a la identificación, el correo electrónico plantea problemas específicos que van desde el establecimiento de criterios objetivos para diferenciar entre mensajes personales e institucionales, hasta la determinación de los distintos ficheros que componen un mismo mensaje. Por su parte, la descripción ha de basarse en la información de la cabecera del fichero de transmisión, que constituirá la principal fuente de metadatos, aunque no la única.

En relación a la organización, los correos electrónicos plantean cuestiones concretas como su integración contextual dentro del expediente o su clasificación en directorios y subdirectorios que reproduzcan los correspondientes cuadros de clasificación. Parece un principio admitido por la literatura profesional, que los correos y sus documentos adjuntos han de ser archivados junto con otros documentos electrónicos, dentro de las series a las que pertenezcan. Esta acción supone su exportación desde la aplicación de correo electrónico, a la ubicación que alberga el sistema de clasificación, bien sea el pc del usuario o el programa de gestión de documentos. En este último caso, ambas aplicaciones deberían estar integradas, de manera que se almacenen de forma automática y eficiente. Parece aconsejable que el archivado se haga de forma más o menos inmediata para conseguir una mayor precisión en los metadatos, un reconocimiento de los mensajes y adjuntos como documentos de archivo en el momento de su clasificación, la posibilidad de consulta por terceros autorizados y una mayor seguridad con respecto a posibles pérdidas de información[20].

La valoración de los correos, como la de cualquier otro documento, habrá de efectuarse en relación con la información que contienen o el fin con que se generan, es decir, dentro de su contexto[21]. La valoración analizará junto con los documentos, el sistema de información utilizado para generarlos y habrá de producirse, para ser eficaz, en el momento de su producción.

El sistema más habitual de conservación del correo electrónico, la copia del servidor, no cumple con los requisitos archivísticos mínimos exigibles. Además, esta técnica implica que la conservación de muchos mensajes se deja en manos de los usuarios finales. Para garantizar la conservación inmediata y futura de los mensajes es importante establecer responsabilidades a distintos niveles.

Los distintos tipos de documentos digitales exigen distintos requisitos técnicos que juegan un papel esencial en la elección de una estrategia de conservación. El proyecto Testbed[22] ha llevado a cabo numerosas investigaciones sobre las características del correo electrónico desde el punto de vista documental. Apoyándose en ellas, ha identificado una serie de requisitos básicos que permiten garantizar la autenticidad del

---

[19] Un clásico sobre el papel del archivero en el entorno digital es el artículo de Hedstrom, Margaret y Wallace, David: *And the Last Shall Be First: Recordkeeping Policies and the NII*. En Journal of the American Society of Information Science, vol.50 núm.4, 1999.

[20] En la práctica existe también la opción de archivarlos en la propia aplicación de correo, aunque desde el punto de vista de una correcta gestión documental, no es la solución más deseable a medio plazo. Podría considerarse como una solución temporal.

[21] Serra Serra, Jordi: *Los Documentos Electrónicos: Qué Son y Cómo Se Tratan*: "el enfoque válido es aquel que se basa en los procesos y actividades de cada organización con independencia de la forma tecnológica que adopten" (pág.68).

[22] Sobre el proyecto Testbed véase: Digital Preservation Testbed. *From digital volatility to digital permanence* [en línea]:*Preserving email.*The Hague, April 2003. http://www.digitaleduurzaamheid.nl/bibliotheek/docs/volatility-permanence-email-en.pdf

correo (contexto, contenido, estructura, apariencia y comportamiento) y asegurar su conservación a medio y largo plazo. Estos requisitos se definen como se recoge a continuación.

Contexto[23]: casi toda la información relativa al contexto inmediato de los mensajes de correo está en la cabecera. Se incluyen aquí la dirección de correo del remitente; la dirección de correo del destinatario o de los destinatarios; en el caso de los correos salientes, la fecha y hora de envío; en caso de los correos entrantes, la fecha y hora de la recepción; el asunto, la configuración de seguridad y confidencialidad y el nombre y el formato de los ficheros adjuntos. Estos datos están normalmente incluidos en el fichero de transmisión, aunque no todos las aplicaciones muestran íntegramente esta información.

Contenido: el contenido del correo va en ocasiones acompañado de ficheros adjuntos. La conservación a largo plazo permitirá la recuperación tanto del contenido del mensaje como de los adjuntos. El proyecto Testbed ha identificado los siguientes requisitos mínimos de autenticidad para el contenido de un correo electrónico:

- el contenido real debe ser siempre legible.

- los adjuntos deben también conservarse.

Estructura[24]**:** la estructura se refiere a la organización del mensaje, la interpretación o el orden de los componentes del correo. Cualquier cambio en la estructura o en el contenido pueden afectar a la interpretación del mensaje. Para que un mensaje conserve su autenticidad, su estructura debe conservarse fielmente.

Apariencia: la apariencia del correo no es la más importante de sus características. A menudo varía en función de la aplicación con la que sea ejecutado. En relación con este elemento, el proyecto Testbed no exige que la apariencia del mensaje sea idéntica a la original, pero no debe alterar el significado del mismo. Con respecto a los adjuntos, su posición en el mensaje puede variar también, pero debe mantenerse la indicación de los mismos en el mensaje.

Comportamiento: el comportamiento asociado con el correo electrónico se refiere, en primer lugar, a la posibilidad de abrir los adjuntos. En segundo lugar a la posibilidad de responder al mensaje o de reenviarlo. Ésta última no pertenece tanto al mensaje como a la aplicación, pero sin embargo, por la función propia del correo electrónico, es una cuestión importante a la hora de elegir un formato de conservación a corto y medio plazo, ya que el mensaje puede necesitar ser contestado o reenviado en las primeras fases de su ciclo vital, no así en la fase de conservación permanente.

El proyecto Testbed ha identificado los siguientes requisitos de autenticidad con relación al comportamiento de un mensaje de correo:

- debe preservarse la capacidad de abrir y acceder a los adjuntos utilizando el software apropiado.

[23] El manual *Electronic Records: a Workbook for Archivists* (editado por el Interntional Council on Archives) define el "contexto" como la información contextual del documento, como la relación del documento con otros documentos del mismo fondo y como la actividad en la que se generó el documento.
[24] Según *Electronic Records: a Workbook for Archivists* del Consejo Internacional de Archivos, la estructura se refiere a cómo el documento es registrado, lo que incluye el uso de símbolos, su presentación, formato, soporte, etc.

- debe preservarse la capacidad de abrir los enlaces web (incluyendo la url). No es necesario conservar el contenido de la web a la que se refiere el enlace.

- deben preservarse los enlaces a otros documentos.

Así pues, cualquier estrategia de conservación ha de tener en cuenta estos requisitos para garantizar la autenticidad e integridad de los mensajes de correo a lo largo del tiempo.

Ya nos hemos referido más arriba a la polémica surgida en Estados Unidos con respecto al borrado de los mensajes en los servidores de correo, tras el final del segundo gobierno del presidente Reagan. Dos décadas después, parece un principio admitido por toda la literatura profesional que el documento generado en formato digital, ha de conservarse en formato digital[25]. En un periodo activo de la documentación, los mensajes pueden mantenerse en el servidor o en las carpetas personales de los usuarios, pero ninguna de éstas dos ubicaciones son espacio de archivo, ni garantizan la conservación futura. Las **estrategias** más habituales actualmente para el mantenimiento a largo plazo de documentos electrónicos son hoy por hoy la migración[26] y la emulación[27].

La migración plantea dos problemas. Por un lado, en su forma más habitual el mensaje de correo se conserva en el formato propietario de la aplicación con que fue generado, lo que no es deseable para una conservación a largo plazo. Además, es un procedimiento que hay que repetir periódicamente, con la amenaza que ello supone para la autenticidad y la integridad del documento. En el caso de que la migración se realice a formatos normalizados, su eficacia dependerá del formato escogido, pero siempre debe procurarse que los formatos elegidos sean no propietarios.

La emulación parece una estrategia más eficaz para la conservación a largo plazo de los documentos digitales, pero resulta poco rentable en el caso del correo electrónico. Además es conveniente para sistemas en los que la apariencia original del documento tiene que permanecer intacta, cosa que no sería aplicable en el caso del correo, tal y como hemos comentado más arriba.

El proyecto Testbed recomienda la conversión a XML de los ficheros de transmisión como estrategia óptima para la conservación a largo plazo de los correos electrónicos. Esta técnica se vale de herramientas desarrolladas con este fin y puede aplicarse en dos entornos: conversión previa y conversión tras el uso. En ambos escenarios la herramienta debe permitir el añadido de metainformación que no figure en el fichero de transmisión, aunque lo ideal sería que las propias aplicaciones gestoras de correo, generasen los ficheros en XML y permitieran definir una serie de campos para la introducción de metadatos por parte del usuario. El objeto digital a conservar estaría compuesto por el fichero XML; el fichero de transmisión; el fichero de registro de auditoría de las acciones de conservación realizadas en el mensaje de correo

[25] Ley 11/2007 Artículo 31. Archivo electrónico de documentos.1.Podrán almacenarse por medios electrónicos todos los documentos utilizados en las actuaciones administrativas.
[26] La migración consiste en la transferencia de ficheros de un entorno de hardware y/o software a otro. Una variante de la migración es la conversión de un formato propietario a un formato que pueda ser utilizado en distintas plataformas sin pérdidas de información.
[27] La emulación consiste en el desarrollo de aplicaciones que imiten el entorno de software y/o hardware en que fueron creados los documentos y permitan así su recuperación y lectura sin pérdidas de información.

electrónico y los datos técnicos necesarios para su conservación; y los metadatos añadidos. Sólo así se podría asegurar su conservación a largo plazo[28].

A modo de resumen, recogemos a continuación algunas de las ventajas que supone el establecimiento de políticas institucionales de gestión del correo:

Desde el punto de vista organizativo:

- reduce las pérdidas de información.
- mejora la eficacia y la eficiencia de la institución.
- previene el uso fraudulento de los sistemas de correo.
- previene accesos no autorizados a la información.
- contribuye a garantizar que los mensajes con valor documental sean conservados de forma que sean accesibles en el futuro.
- contribuye a preservar la memoria institucional.

Desde el punto de vista legal:

- contribuye a cumplir con la legislación vigente en materia de procedimiento administrativo, y de acceso y conservación de la documentación.
- contribuye a cumplir con la legislación relativa a privacidad de las comunicaciones.
- minimiza los riesgos legales de la organización.

Desde el punto de vista técnico:

- garantiza la correcta organización de los mensajes y la integridad de los expedientes en entornos híbridos y digitales.
- asegura una correcta gestión de los mensajes de acuerdo con los criterios archivísticos que garanticen la autenticidad de la información almacenada a medio y largo plazo.

3. Asignación de responsabilidades

Para una correcta gestión y conservación del correo electrónico, es esencial que las políticas y directrices recojan las funciones y responsabilidades específicas de los distintos colectivos universitarios implicados. Cada uno de estos colectivos tiene que entender su papel y cómo encaja éste en el proceso general. Las políticas de gestión del correo tendrán que establecer esas responsabilidades, que suelen involucrar a cuatro grupos diferenciados:

- Las autoridades académicas
- Los archiveros y gestores de documentos
- Los servicios de informática y comunicaciones
- Los usuarios finales

Las autoridades académicas

Su labor principal reside en el establecimiento de políticas que transmitan a todos los colectivos de la Universidad implicados, la importancia del correo electrónico como documento administrativo con valor evidencial, lo que constituye un requisito básico para

[28] Algunas de las ventajas del XML como formato de conservación a largo plazo han sido recogidas por Boudrez en la publicación citada.

poder utilizar esta herramienta de forma eficaz. Entre las acciones concretas que deberían adoptar las autoridades académicas, estaría la de promover el diseño de directrices institucionales sobre el uso y conservación del correo electrónico dentro de los proyectos de impulso e implantación de administración electrónica, que transmitieran confianza y seguridad en la utilización del mismo.

Las autoridades académicas debían aportar en estas directrices:

- definición del marco legislativo y reglamentario que afecta a su uso: los potenciales usuarios deben ser advertidos del uso ilegal y sus consecuencias.
- información sobre la titularidad del sistema de mensajería y de las transacciones que se realizan a través del mismo.
- condiciones de uso del sistema de mensajería, incluyendo cualquier uso privado. Se podrían incluir aquí procedimientos a seguir en caso de ausencia prolongada del trabajador o cambio en el puesto de trabajo.
- recomendaciones y condiciones de utilización de la firma electrónica.
- información sobre la política y estrategia de gestión documental corporativa.
- información sobre las estrategias de conservación en la fase activa, semiactiva e inactiva de los mensajes de correo.
- asignación de responsabilidades en la determinación de qué mensajes deben ser conservados y cuáles pueden ser eliminados.
- asignación de responsabilidades en la captura de los mensajes electrónicos que deban ser incluidos en sistemas de gestión documental y elaboración de directrices de uso para apoyar este proceso.
- información pertinente sobre seguridad y acceso.

Su labor no acaba con la elaboración de políticas y procedimientos, sino que serían responsables tanto de la difusión, como de la evaluación periódica de dichas políticas con vistas a detectar posibles carencias u oportunidades de mejora. También sería definitiva su actuación en la promoción de grupos de trabajo multidisciplinares (juristas, especialistas en sistemas y redes informáticas, archiveros, gestores) para el desarrollo, difusión, aplicación y evaluación de las mismas, así como la planificación de actividades formativas destinadas a todos los colectivos de usuarios.

Los archiveros y gestores de documentos

Aunque elaborar la política institucional sobre la gestión del correo electrónico, no es su responsabilidad, el archivero puede jugar un papel importante en el diseño de la misma, asegurándose de que constituye una prioridad en las políticas documentales y haciendo especial hincapié en la conservación a largo plazo. Es imprescindible conseguir que este objetivo esté en la agenda de la institución. El archivero apoyará la integración de las directrices sobre gestión de correo electrónico en las políticas de gestión documental y aportará su experiencia en la resolución de problemas que puedan derivarse de ello, tanto en un entorno electrónico como híbrido.

Su participación en el rediseño de procedimientos adaptados a la gestión electrónica, y en la definición de catálogos de documentos, resulta definitivo para una identificación óptima de las series y de los documentos que las componen.

El establecimiento de los requisitos archivísticos que garanticen la integridad y autenticidad de los mensajes a lo largo de todo su ciclo de vida es otra tarea esencial de este colectivo. Como se ha señalado más arriba, la conservación a medio y largo plazo

se logra mediante medios técnicos, pero debe determinarse de acuerdo con criterios archivísticos.

Una adecuada conservación sólo puede alcanzarse mediante apropiadas políticas documentales. El archivero debe colaborar en el establecimiento de fórmulas que permitan la fácil clasificación de los correos, y su contextualización mediante una adecuada asignación de metadatos. La propia naturaleza del correo electrónico, hace recomendable que esta tarea se realice en el momento de generar el mensaje o en el de su recepción, de manera que el usuario final no tenga que añadir demasiados metadatos de forma manual, lo que repercutiría en su aceptación última del procedimiento. Deberá también determinar, en colaboración con las oficinas, qué metadatos deben ser registrados, diferenciando aquéllos que son importantes para su uso y la reutilización e interpretación de la información, y aquéllos que cada universidad necesita para la rendición de cuentas.

Su labor puede resultar especialmente relevante en el desarrollo de instrucciones concretas destinadas a los usuarios finales (véase Anexo I de este documento). Para ello trabajará en el análisis de la situación corriente, en la detección de las necesidades y carencias de los usuarios, así como en las actividades de formación dirigidas a los mismos. También promoverá la formación del personal de archivo en la política de gestión y conservación del correo electrónico, con el objetivo de convertir este servicio en un referente en materia de gestión de los documentos administrativos electrónicos. La intervención del usuario final en la decisión sobre la conservación o no de los mensajes resulta esencial. Por ello, el archivero ha de asumir un papel activo en la concienciación de que los mensajes que documenten actividades administrativas sean considerados documentos de archivo y se conserven con los debidos requisitos de autenticidad e integridad.

De igual forma es importante que el archivero mantenga un calendario de conservación actualizado para que los correos que formen parte de una determinada serie documental tengan asociados sus plazos de conservación y eliminación correspondientes. El calendario debería recoger también la política de acceso, relacionada con el formato de almacenamiento y la calidad de los metadatos que se apliquen.

Es fundamental que transmita a las oficinas la importancia de realizar una estrategia de selección de mensajes en las primeras fases, desde la misma aplicación de correo, cuando el formato original todavía está accesible, pues ello permitirá su conversión a un formato de conservación adecuado.

Cada paso dado en este sentido, debería quedar plasmado en un documento que refleje cuándo se debe aplicar cada opción, qué es lo ideal y qué lo aconsejable. Este documento será la base para un posterior seguimiento, ya que las tecnologías de la información cambian rápidamente y las políticas deberán ajustarse continuamente.

Los servicios de informática y comunicaciones

Como en cualquier política de gestión y conservación de documentos electrónicos, la participación de los servicios de informática y comunicaciones es esencial. Su colaboración es indispensable especialmente a la hora de garantizar la interoperabilidad y la seguridad de los sistemas de gestión de correo, así como la de los sistemas y formatos que se implanten para la conservación a medio y largo plazo. Su participación en tareas de asesoramiento e implantación de las técnicas criptográficas y los protocolos que garanticen la protección de la privacidad es definitiva.

Una de sus principales tareas consistirá en la parametrización, con la colaboración de los archiveros, tanto de los programas gestores de correo como de los destinados a la conservación. Es por esto que deberán diseñar el sistema de manera que el máximo de metadatos se asocien de forma automática a los mensajes a partir de la información incluida en el fichero de transmisión. Los informáticos deberán procurar que en los casos en que sea necesaria la asignación manual de metadatos, ésta se lleve a cabo de forma sencilla, mediante plantillas y valores por defecto o valores que puedan seleccionar fácilmente. Esto incrementa la uniformidad de los datos incorporados y reduce el riesgo de errores. Los metadatos sobre la clasificación y el contexto del mensaje, por ejemplo el expediente al que pertenece, deberían ser requeridos por el propio sistema centralizado de almacenamiento. El sistema deberá estar preparado para gestionar correctamente los documentos adjuntos. Para ello, todos los componentes (cuerpo del mensaje, documento adjunto y metadatos) deben estar perfectamente relacionados sin que esa conexión pueda perderse, añadiendo una serie de metadatos extra.

Deberán además asegurarse de que el sistema de conservación sea capaz de añadir un registro de auditoría en cada mensaje almacenado. Este registro deberá contener metadatos sobre el entorno electrónico: la versión de la aplicación utilizada, la versión del sistema de conservación en uso y el listado de acciones de preservación que se le han aplicado…

Es esencial también su participación en el diseño de procedimientos de migración de los documentos a los formatos de conservación y el apoyo técnico en las transferencias que se realicen a la aplicación correspondiente. A falta de políticas de conservación correctamente diseñadas, su intervención en la prevención de eliminaciones accidentales, mediante las copias de seguridad de los servidores, es crucial.

El sistema de almacenamiento necesitará también un buen sistema de búsqueda y recuperación de la información, preferentemente en el formato utilizado por la aplicación de correo electrónico estándar o bien a través de un visualizador.

Otra tarea en la que pueden participar es en aplicar las normas de imagen institucional a la apariencia de los mensajes. La conservación del correo electrónico a largo plazo depende mucho de la forma en que se haya creado el mensaje. Al usuario final se le puede ayudar dándole una serie de pautas y herramientas informáticas. Estas herramientas también pueden servir para dar una apariencia y estilo institucional a los mensajes oficiales, es decir, dar una estructura fija y apariencia como la fuente utilizada, los colores, los logos…

Al diseñar y configurar el sistema de conservación, han de ser consideradas las siguientes cuestiones prácticas:

- *Seguridad*: el acceso al sistema de almacenamiento central tendrá que ser cuidadosamente controlado para evitar el daño accidental o deliberado de la información almacenada (creación de un sistema de clasificación de acceso, véase también ISO 15489)
- *Copia de seguridad*: deben diseñar una estrategia de copia de seguridad adecuada para que el sistema pueda ser reintegrado si se produce un fallo, tanto si es de forma involuntaria o deliberada, o en el caso de situaciones críticas como incendios o inundaciones.

- *Flexibilidad*: los diferentes grupos de usuarios pueden necesitar otros metadatos y estas necesidades pueden cambiar a medida que pasa el tiempo, por lo que el diseño del sistema debe ser lo más flexible posible.
- *Sistemas de almacenamiento distribuido*: en una universidad grande puede ser más práctico tener una serie de pequeños sistemas de correo electrónico que un sistema muy grande. En este caso, es importante garantizar el control completo, porque puede ser un requisito buscar en todo el sistema.
- *Tiempos de respuesta y fiabilidad*: ya que los usuarios tendrán que utilizar el sistema de almacenamiento como parte de su día a día de trabajo, los tiempos de respuesta cortos y la máxima fiabilidad son una exigencia. Dos cosas son importantes aquí. En primer lugar el usuario debe ser capaz de guardar un mensaje de correo electrónico en el sistema de almacenamiento rápida y fácilmente. En segundo lugar, la información ya almacenada en el sistema debe ser de fácil acceso y fácil de encontrar.
- *Instalación, mantenimiento, formación y soporte:* cuando la estrategia requiere métodos nuevos y cambios en las aplicaciones y redes, los usuarios finales necesitarán formación. Los informáticos deberían hacer lo posible para que las interfaces sean amigables y los procedimientos lo más sencillos posible. A partir de ahí, el propio servicio de informática, junto con el archivero, deberán formar y dar soporte en el uso correcto del correo electrónico.

Los usuarios finales

Todos los requisitos que se hayan propuesto deben llevarse a la práctica por lo que la implicación del usuario final es determinante. Es él quien decide si va a llevar a cabo las recomendaciones que se le plantean. Es el último eslabón de la cadena y quien al final hace posible que la universidad pueda mantener una correcta política de preservación del correo electrónico.

Básicamente el usuario final tiene la responsabilidad de generar correos electrónicos de forma correcta, clasificarlos y ordenarlos siguiendo los esquemas desarrollados al efecto; así como de capturar aquéllos que forman parte de sus procedimientos y eliminar los que no forman parte de los mismos. Como en el caso de la documentación en soporte papel, las oficinas tienen la responsabilidad de organizar y conservar los mensajes por ellas generados.

Para llevar a cabo su labor, es necesario que se hayan dado los pasos previos: que exista una política institucional sobre la gestión del correo electrónico, que ésta se incluya dentro de una gestión integral de los documentos dentro de la Universidad, y que se haya organizado de forma coherente un sistema para su conservación. Sólo si se cumplen estos requisitos previos, el usuario final podrá saber cómo actuar en cada momento, siguiendo procedimientos claros y definidos.

ANEXO I

RECOMENDACIONES PRÁCTICAS PARA LA GESTIÓN DEL CORREO ELECTRÓNICO

¿Qué es un mensaje de correo electrónico y para qué sirve el correo electrónico?

Un mensaje de correo electrónico es un simple mensaje electrónico, elaborado usando una aplicación de correo electrónico. Generalmente, el mensaje tiene la siguiente estructura: encabezado o cabecera, con información sobre el emisor y el receptor; cuerpo, con el contenido del mensaje y la firma; y, en ocasiones, documentos adjuntos.

El sistema de correo electrónico de la Universidad es un servicio que ofrece la Universidad a sus miembros, a quienes proporciona una cuenta de correo individual. Es una tecnología corporativa, ya que cada universidad elige un software o aplicación para el correo electrónico: Microsoft Outlook, Eudora, Thunderbird, etc.

Por tanto, el correo electrónico es una herramienta que permite el intercambio de mensajes.

El servidor de correo electrónico no es un espacio de archivo.

¿Quién debe utilizar la cuenta de correo institucional?

El acceso debe ser permitido solamente las personas autorizadas, por lo que el usuario debe responsabilizarse y no facilitar las claves a otras personas.

El correo institucional sólo será utilizado por personas autorizadas

¿Qué uso puedo hacer del correo institucional?

Se debe hacer un uso puramente profesional. En caso de que la Universidad permita el uso personal, éste debe estar dentro de los límites legales y de corrección. Se debe abstener de hacer un uso ilegal, comercial o simplemente no autorizado, que pueda crear conflictos en la Universidad.

La persona que envía el mensaje debe estar correctamente identificada. Del mismo modo, deben quedar claramente separadas las opiniones personales de las institucionales. Se podría incluir una nota de exoneración en los mensajes enviados al exterior.

Se debe ser especialmente cauteloso con la legislación sobre la protección de datos y la propiedad intelectual, teniendo en cuenta quiénes pueden tener acceso a la información contenida en los mensajes. El correo electrónico no ofrece ninguna garantía de confidencialidad. Hay cierta información que no debería ser enviada por correo electrónico o distribuida sin la debida autorización.

El correo institucional solo debe ser utilizado dentro de los límites legales

¿Todos los mensajes de correos electrónicos son documentos de archivo?

No todos los mensajes de correos enviados o recibidos por personal de la Universidad son documentos de archivo.

Los mensajes de correo electrónico son considerados documentos de archivo cuando son enviados o recibidos como resultado de una función administrativa, docente o investigadora, esto es, cuando evidencian una actividad propia de la Universidad. Por tanto, estos mensajes deben ser gestionados como el resto de documentos administrativos de la Universidad, de acuerdo con las directrices del Sistema de gestión documental de la propia Universidad.

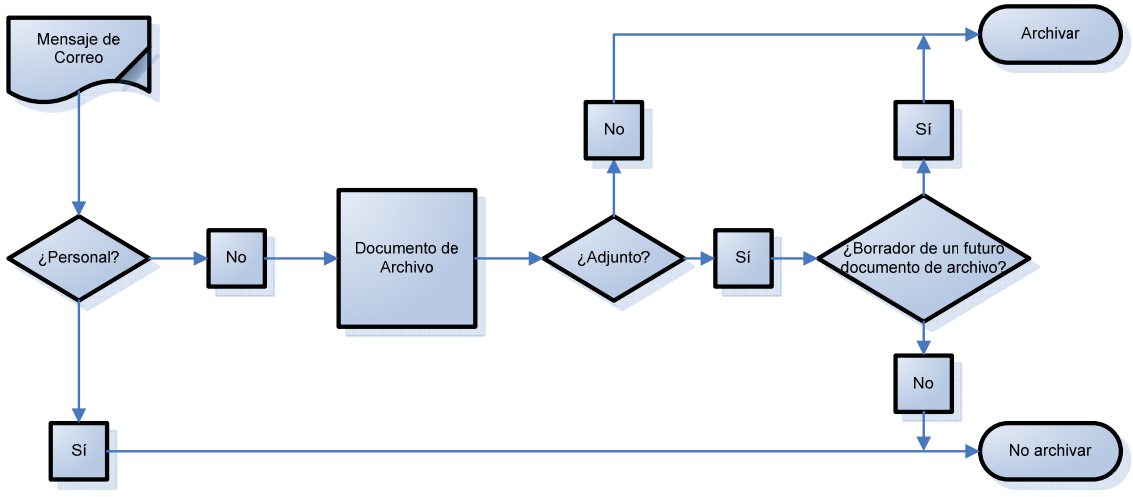
Los mensajes son documentos de archivo cuando son testimonio de una actividad propia de la Universidad

¿Cómo determinar si un mensaje es un documento de archivo?

Para determinar si un mensaje de correo electrónico es un documento de archivo, hay que responder afirmativamente a las siguientes preguntas:

- ¿Está el mensaje relacionado con mis funciones o actividades propias?
- ¿Forma parte de un expediente abierto?
- ¿Contiene información útil para mi trabajo?

El siguiente esquema puede ayudar a determinar el carácter de documento de un mensaje:



Así, son ejemplos de mensajes electrónicos considerados documentos de archivo:

- políticas o directrices
- informes, memorias
- correspondencia relacionada con actividades administrativas

- cualquier documento que inicia, tramita, autoriza o completa una actividad administrativa.

No se consideran documentos de archivo:

- mensajes personales
- spam
- información no solicitada (información de cursos, artículos, etc.)

El primer paso es identificar los mensajes que son documentos de archivo

¿Quién tiene la responsabilidad en la gestión del correo electrónico?

Al igual que ocurre con los documentos en papel, el remitente tiene la responsabilidad de gestionar y conservar los mensajes que crea y envía, como evidencia de una actuación determinada.

El destinatario, por su parte, tiene la responsabilidad de gestionar y conservar aquellos mensajes que forman parte de un expediente. En el caso de mensajes colectivos, será la unidad administrativa que conserve el expediente completo, la que conservará obligatoriamente el mensaje de correo.

La unidad administrativa productora es la responsable de incorporar los mensajes a los expedientes

¿Cómo crear mensajes de correo electrónico?

Para una eficaz gestión de los mensajes de correo electrónico, es importante crear mensajes unívocos. Para ello, se recomienda:

En la cabecera del mensaje:

- Identificar claramente el destinatario principal, esto es, quien debe actuar o decidir sobre el mensaje, y los destinatarios secundarios (CC), que reciben el mensaje sólo con fines informativos.
- Evitar el uso de destinatarios secundarios ocultos (CCO, BCC), ya que un documento administrativo debería incluir el listado de aquéllos a los que se les ha enviado.
- Sin embargo, si se envía un mensaje a una larga lista de destinatarios que no conocen sus direcciones de correo entre sí, es mejor opción utilizar una lista de distribución para que esta información no se incluya en el mensaje.
- Utilizar siempre la dirección de correo completa de los destinatarios.
- Identificar de forma clara y concisa el asunto del mensaje. En cada mensaje, hacer referencia a un único asunto.
- Utilizar prefijos en el asunto del mensaje que ayude al receptor a conocer el alcance del mismo.
- Identificar la urgencia o importancia del mensaje.
- En caso necesario, activar la opción de notificación de recepción.

- Cuando se responde a un mensaje, utilizar la opción "responder", en vez de insertar el texto. No modificar el texto original en la respuesta. Algunas aplicaciones podrían no reflejar la diferencia.

En el cuerpo del mensaje:

- Texto:
  - Escribir mensajes breves.
  - Explicar de forma clara y unívoca el objetivo del mensaje y la acción que se requiere. Especificar si el mensaje necesita respuesta.
  - No utilizar lenguaje coloquial ni excesivamente formal, sino un lenguaje claro y conciso[29].
  - En trámites habituales utilizar una plantilla formalizada de documento. Incluir en este caso, el código de clasificación de la serie o la referencia del expediente.
  - No incluir en el texto información o referencias personales.
  - Informar si se incluye documentación aneja.
  - Evitar formatos y gráficos en el cuerpo del mensaje. Es posible que el receptor no pueda visualizarlos.
  - Avisar de errores en la recepción.
  - No incluir campos que se actualicen automáticamente.
- Pie de firma:
  - Utilizar el pie de firma institucional, si existe, y en todo caso, identificar el remitente: Nombre y apellidos; puesto de trabajo; Universidad y servicio al que pertenece; teléfono; fax; correo electrónico.
  - Añadir advertencias o recomendaciones: sobre la confidencialidad del mensaje, para imprimir sólo los correos necesarios, etc.
- Documentos adjuntos:
  - Se debe evitar enviar documentos adjuntos siempre que se pueda incluir la información en el cuerpo del mensaje.
  - Si el documento adjunto se puede consultar en una página web, intranet o servidor común, es mejor proporcionar el enlace dentro del cuerpo del mensaje.
  - Aunque en los mensajes de correo se puede adjuntar documentos en cualquier formato, se recomienda utilizar formatos abiertos y estándares, así como tamaños adecuados. Es importante asegurarse de que la persona que lo recibe puede leerlo.

La identificación y el asunto en los mensajes de correo facilitan su archivo en el expediente correspondiente

[29] Las normas de cortesía que recoge Nicole Periat en su artículo *Politique de gestion du courrier electronique: des mesures à prendre.* http://www.ebsi.umontreal.ca/cursus/vol3no1/periat.htm son muy completas.

¿Cómo organizar los mensajes de correo electrónico?

Al igual que el resto de documentos administrativos, los mensajes de correo deben ser gestionados en un plazo de pocos días. Para ello, se recomienda:

- Incorporar la gestión de los mensajes de correo, tanto los de la bandeja de entrada como los de salida, al trabajo diario.
- Una vez recibido o enviado un mensaje, determinar su valor y en consecuencia, su destino:
  - Si el mensaje no está relacionado con una actividad o función propia de la Universidad, eliminar una vez leído o enviado.
  - Si es un borrador de un documento, conservar hasta recibir o enviar el documento definitivo.
  - Si es un mensaje que recibimos como información, sin valor administrativo, conservar mientras sea útil.
  - Si es un mensaje que se imprime y se archiva en el expediente en papel, eliminar una vez impreso.
  - Los mensajes enviados a varias personas, sólo serán conservados por el remitente y por el destinatario principal.
  - El remitente debe conservar el mensaje original enviado, la lista de los destinatarios y todas las respuestas.
  - En los mensajes con documentos adjuntos, si el mensaje de correo es sólo un documento de trámite para avisar del envío, se puede eliminar. Por el contrario, si tiene información contextual importante debe conservarse.
  - En el caso de mensajes envío-respuesta, conservar el último que incluya la cadena de mensajes anteriores.

Una vez realizada la acción correspondiente al mensaje de correo, se debe decidir su eliminación o conservación, temporal o permanente

¿Cómo clasificar y archivar los mensajes de correo electrónico?

Al igual que el resto de documentos administrativos, los mensajes electrónicos deben seguir los criterios de clasificación y archivo establecidos por el Sistema de Gestión Documental de la Universidad.

Los correos deberían sen capturados directamente en un Sistema de Gestión de documentos para garantizar su autenticidad e integridad. Cuando esto no es posible, se deben aplicar otras soluciones técnicas y organizativas que nos den las máximas garantías.

En primer lugar habrá que clasificar y archivar los mensajes a conservar, para incorporarlos al expediente correspondiente, ya sea en papel o electrónico. Estas operaciones deberían realizarse lo más cerca posible del momento de su creación o recepción.

Es recomendable que la clasificación pueda automatizarse dentro de la aplicación de correo, para facilitar y fomentar su uso. Probablemente será necesario un desarrollo informático[30]. Una vez clasificados, se aplicarán los mismos criterios de selección y evaluación que al expediente del que forman parte.

Se recomienda:

- En el caso de expedientes formados mayoritariamente por documentos en papel, imprimir el mensaje electrónico con todos los datos del encabezado y archivarlo en el expediente en papel. Sin embargo se deberá conservar el mensaje electrónico, ya que será éste el que tenga valor como evidencia.
- Los mensajes pueden archivarse temporalmente en la aplicación del correo electrónico, de manera que estén disponibles para su utilización. Para ello se creará una estructura de carpetas y subcarpetas de acuerdo con el cuadro de clasificación de la Universidad, y similar a la existente en el disco duro.
- Además de las carpetas para los documentos administrativos, se recomienda crear una carpeta denominada "Personal" para incluir todos los mensajes de carácter personal y una carpeta denominada "Información" para incluir aquellos mensajes exclusivamente informativos y publicitarios. Ambas carpetas sólo se conservaran temporalmente. De esta forma se simplificarán las tareas de gestión y clasificación.
- Para conservar a largo plazo, o para que los mensajes y sus documentos adjuntos sean accesibles a otras personas del servicio, los mensajes de correo electrónico se archivarán en el servidor o archivo digital correspondiente, manteniendo la estructura de carpetas según el cuadro de clasificación. De esta forma, se garantiza la unidad del expediente.
- Cuando los mensajes incluyen documentos adjuntos, habrá que considerar si debemos conservar el mensaje, el adjunto, o ambos. En el último caso, estos documentos se archivarán separadamente, ya que pueden tener diferentes necesidades de conservación en función de su formato y podrán ser identificados y reutilizados más fácilmente. Se almacenarán en la carpeta del servidor correspondiente al expediente en cuestión, manteniendo la conexión con el mensaje mediante metadatos.
- Sobre esta estructura de carpetas clasificadas podrán aplicarse los distintos plazos de conservación para cada una de las series.
- Los mensajes pueden almacenarse en el formato de la aplicación de correo electrónico, ya que se mantienen así sus funcionalidades (respuesta, reenvío…), lo que facilita su reutilización. Sin embargo, para su conservación a largo plazo, será necesario migrar a un formato abierto o estándar, como .txt, .pdf o preferentemente .xml. Este último es sin duda la mejor opción, ya que nos permite crear objetos digitales, formados por el fichero XML, el fichero de transmisión, el fichero de registro y los metadatos añadidos[31]. Se recomienda establecer una política de migraciones que tenga en cuenta no sólo la conservación, sino la posterior recuperación y accesibilidad a los correos electrónicos.

[30] Como ejemplo véase la solución adoptada en el Archivo Municipal de Antwerp. Boudrez, F. *Filing and archiving e-mail.*
[31] Véase por ejemplo el Proyecto Testbed y otras soluciones en: Pennock, M. *Curating e-mails*, p. 48.

Los mensajes de correo se archivarán junto con el expediente del que forman parte

¿Qué debo hacer en caso de ausencia prolongada de mi puesto de trabajo?

Se deberá tener cierta previsión para que la cuenta de correo no se vea saturada y pueda llegar a bloquearse. Por ejemplo se recomienda darse de baja de las listas de difusión durante el periodo de ausencia prolongada, eliminar aquéllos mensajes que no deban conservarse y almacenar aquéllos que tengan un valor archivístico.

En ausencias prolongadas se debe prevenir el bloqueo del correo electrónico por saturación

¿Qué debo hacer cuando cambio de puesto de trabajo?

En caso de cambiar de puesto de trabajo o dejar la Universidad, es importante que todos los correos electrónicos creados o recibidos en el transcurso de sus funciones estén disponibles para la persona que vaya a sustituirla. Es responsabilidad del usuario final garantizar la conservación de todos aquéllos mensajes que puedan ser evidencia de las actividades de la Universidad, para su posterior utilización cuando sea necesario.

Si se abandona la Universidad, se debe garantizar la conservación y acceso de los mensajes considerados de archivo

ANEXO II: BIBLIOGRAFÍA

Artículos, recursos en línea y monografías:

BANÚS GIMÉNEZ, Teresa y CORTÉS LONGARES, Marta: El Correu Electrònic: un Problema a Resoldre. En Lligall, n.25 (2003).

BOUDREZ, Filip. *Filing and archiving e-mail* [en línea]. Antwerp, 2006 http://www.expertisecentrumdavid.be/docs/filingArchiving_email.pdf [Consulta: 2 marzo, 2010].

Digital Preservation Testbed. *From digital volatility to digital permanence* [en línea]*:Preserving email.*The Hague, April 2003. http://www.digitaleduurzaamheid.nl/bibliotheek/docs/volatility-permanence-email-en.pdf [Consulta: 2 marzo, 2010].

Electronic mail [en línea].*: Guidelines for Developing Policy & Establishing Procedures forE-mail. A Component of an Agency Records Management Program.* Office of the Secretary of State, *Division of Archives & Records Management*. http://www.nationalarchives.gov.uk/documents/managing_emails.pdf [Consulta: 2 marzo, 2010].

GAMERO CASADO, Eduardo y MARTÍNEZ GUTIÉRREZ, Rubén: Legislación de Administración Electrónica y de Protección de Datos. Tecnos, 2008.

HEDSTROM, Margaret y WALLACE, David: *And the Last Shall Be First: Recordkeeping Policies and the NII*. En *Journal of the American Society of Information Science*, vol.50 núm.4, 1999.

International Council on Archives: *Electronic Records: a Workbook for Archivists* [en línea]. http://www.ica.org/en/node/30273 . [Consulta: 2 marzo, 2010].

LUKESH, Susan: *E-mail and potencial loss to future archives and scholarship or the dog that didn't bark* [en línea] http://hofprints.hofstra.edu/13/01/Lukesh%2C_Susan_S._(1999)_E-mail_and_Potential_Loss_to_Future_Archives_and_Scholarship_or_The_Dog_that_Didn%27t_Bark._FirstMonday_4(9).htm. [Consulta: 2 de marzo, 2010]

McGill University Archives. *Recordkeeping and Email Best Practices* [en línea]. *http://www.archives.mcgill.ca/dp/assets/pdf_dp_email_best_practices_rev.pdf.* [Consulta: 2 marzo, 2010].

National Archives of Australia: *Managing Electronic Messages as Records* [en línea]. http://pandora.nla.gov.au/pan/22371/20011105-0000/www.naa.gov.au/recordkeeping/er/elec_messages/summary.html. [Consulta: 2 marzo, 2010].

North Carolina State University: *University E-mail Retention* [en línea]. (Policies, Regulations and Rules, REG08.00.9, 2004) http://www.ncsu.edu/policies/informationtechnology/REG08.00.9.php. [Consulta: 2 marzo, 2010].

ONU: *Gestión de correos electrónicos como expedientes* [en línea]. http://www.un.org/spanish/archives/unrecordsmgmt/manageemailrecs.shtml.[Consulta: 2 marzo, 2010].

PERIAT, Nicole: *Politique de gestion du courrier electronique: des mesures à prendre* [en línea]. http://www.ebsi.umontreal.ca/cursus/vol3no1/periat.htm .[Consulta: 2 marzo, 2010].

PADI (Preserving Access to Digital Information) [en línea]: e-mail. http://www.nla.gov.au/padi/topics/47.html. [Consulta: 2 marzo, 2010].

PENNOCK, Maureen. *"Curating E-Mails* [en línea]*: A life-cycle approach to the management and preservation of e-mail messages" DCC Digital Curation Manual*, S.Ross, M.Day (eds.), (July 2006), Retrieved <from http://www.dcc.ac.uk/resource/curation-manual/chapters/curating-e-mails. [Consulta: 2 marzo, 2010].

SCHMIDT, LISA M**.** *Preserving the H-Net Academic Electronic Mail Lists* [en línea]. (SAA Campus Case Studies – CASE 11, 2009). http://www.archivists.org/publications/epubs/CampusCaseStudies/casestudies/Case11-Schmidt.pdf . [Consulta: 2 marzo, 2010].

SERRA SERRA, Jordi: Los Documentos Electrónicos: Qué Son y Cómo se Tratan. Editorial TREA, 2008.

SERRA SERRA, Jordi. Gestión y preservación de la documentación electrónica [en línea]: Material docente. Pamplona, 15 y 16 de octubre de 2009. http://eprints.rclis.org/17064 . [Consulta: 2 marzo, 2010].

University of Aberdeen. *Guidelines for the Management of University E-Mail* [en línea] *(Sept 2005)* http://www.abdn.ac.uk/central/records-management/e-mail.shtml. [Consulta: 2 marzo, 2010].

University of Bath. *Computing Services E-mail Policy* [en línea] *(Feb 2003)* http://www.bath.ac.uk/bucs/policies/e-mail.shtml. [Consulta: 2 marzo, 2010].

University of Edinburgh (UoE). *Managing Your Emails* [en línea] (V.10-2007) http://www.recordsmanagement.ed.ac.uk/InfoStaff/RMstaff/ManagingEmail/ManagingEmail.htm. [Consulta: 2 marzo, 2010].

University of Wales, Aberystwyth. *Policy on the use of E-mail* [en línea] *(March 2004)* http://www.aber.ac.uk/infopolicies/e-mail-policy.shtml. [Consulta: 2 marzo, 2010].

WALLACE, David A. *Recordkeeping and Electronic Mail Policy* [en línea]*: The State of Thought and the State of the Practice*. Draft of the paper prepared for the Annual Meeting of the Society of American Archivists, Orlando, Florida, September 3, 1998. http://www.mybestdocs.com/dwallace.html. [Consulta: 2 marzo, 2010].

Normas ISO

- ISO 15801:2004 Información almacenada electrónicamente. Recomendaciones para la veracidad y admisibilidad de documentos.
- ISO/TR 18491:2005 Long-term preservation of electronic document-based information.
- ISO 19005:2005 Document management- Electronic document file format for long-term preservation.
- UNE-ISO 23081 (1 y 2): 2008 Información y documentación. Procesos de gestión de documentos. Metadatos para la gestión de documentos.
- ISO/TR 26122: 2008 Information and documentation. Work process analysis for records.
- ISO/IEC 26300: 2006 Open Document format for office applications (Open Document) v.1.0.