COMITÉ ADMINISTRATIVO
ACTA 276

RESOLUCIÓN CAD- 010
12 de julio de 2007

Por la cual se adopta el Manual de Políticas de Almacenamiento de la Información Digital

El Comité Administrativo de la Corporación Universitaria Lasallista, organismo permanente para los asuntos administrativos, económicos y financieros y,

CONSIDERANDO:

Que de acuerdo con la definición acogida por la UNESCO[1], el patrimonio digital consiste en recursos únicos que son fruto del saber o la expresión de los seres humanos. Comprende recursos de carácter cultural, educativo, científico o administrativo e información técnica, jurídica, médica y de otras clases, que se generan directamente en formato digital o se convierten a éste a partir de material análogo ya existente.

Que dada la importancia y el valor que reviste el patrimonio digital de la Corporación, éste debe considerarse como un material digno de protección y conservación como garantía y respaldo de las acciones institucionales.

Que la Corporación requiere establecer y dar a conocer las directrices y recomendaciones para asegurar el adecuado almacenamiento y manejo de los archivos digitales de la Institución.

Por lo anterior,

RESUELVE:

Artículo 1. Aprobar para la Corporación Universitaria Lasallista el Manual de Políticas de la Información Digital, en los siguientes términos:

[1] ORGANIZACIÓN DE LAS NACIONES UNIDAS PARA LA EDUCACIÓN, LA CIENCIA Y LA CULTURA. Directrices para la preservación del patrimonio digital. Preparado por la Biblioteca Nacional de Australia.(Online) s.l.p: UNESCO, (Citado 12 junio 2007). Disponible url http//www.**unesco**.org/es. Marzo de 2003.

1. REFERENTES

1.1 INFORMACIÓN DIGITAL

El concepto de información digital se aplica para todo contenido que está representado mediante ceros y unos dentro de una computadora. La información digital no sólo son textos electrónicos, también se incluyen las imágenes, el audio y el video, los cuales, al igual que los textos, tienen diferentes formatos, codificaciones y representaciones en el mundo electrónico. Documentos de texto, imágenes, videos, animaciones, sonidos, etc., son convertidos a formato digital y almacenados en archivos que se distinguen unos de otros mediante el empleo de etiquetas pegadas al nombre que distinguen su naturaleza (doc, txt, jpg, gif, wav, etc.).

La información digital que tiene que ver con imágenes, videos y textos “html” (es decir, que contienen enlaces a páginas de Internet) es mucho más voluminosa que los simples textos, o las hojas electrónicas.

1.2 DIGITALIZACIÓN (GESTIÓN DE MANEJO DE LA INFORMACIÓN)

Técnica que permite la reproducción de información que se encuentra de manera analógica (papel, video, sonido, cine, microfilm y otros) en otra, que sólo puede ser leída o interpretada por computador.

Como registro, almacenamiento digital, o respaldo de registros, se entiende cualquier información relativa al trabajo de la corporación.

La gestión de archivos-registros se apoya fundamentalmente en tres tipos tradicionales de registros[2]:

- Registros personales: cualquier información personal creada o mantenida en una estación de trabajo, de interés para aquella persona que la tiene y la consulta.

- Registros transitorios: son aquellos documentos que elaboran una o varias personas de manera temporal mientras confeccionan un documento oficial en su versión definitiva. Por ejemplo, son registros transitorios los memos y las

[2] GARCÍA PÉREZ, Alexeis. La gestión de documentos electrónicos como respuesta a las nuevas condiciones del entorno de información. (Online). Ciudad de la Habana: Universidad de la habana. 2001 (citado en 15 junio 2007) Disponible URL http://prints.rclies.org/archive/000001983

versiones preliminares de un proyecto. Algunos registros transitorios se convierten finalmente en oficiales.

- Registros oficiales: documentos finales de una decisión oficial dentro de la institución o de esta hacia el exterior, como por ejemplo la versión final de un proyecto, mensajes decisivos de correo electrónico y otros documentos que constituyen registros oficiales.

Dentro de los aspectos técnicos que se contemplan en el proceso del manejo digital se ofrecen ventajas tales como: la velocidad y facilidad de consulta de archivos en red, capacidad de mejorar imágenes de documentos en mal estado, versatilidad en el manejo de diferentes tipos de documentación, disminución del espacio físico que se utiliza para almacenar archivos análogos y disponibilidad de la información por varios usuarios en tiempo real.

En este mismo sentido podemos constatar algunas desventajas del proceso de digitalización. La primera de ellas se refiere a la conservación, ya que los medios de almacenamiento digital no han sido diseñados para perdurar indefinidamente en el tiempo. Una segunda desventaja es la dificultad que se puede presentar ante los cambios en los formatos de almacenamiento que pueden impedir consultas futuras. Adicionalmente, si no se mantienen unas condiciones ambientales controladas tales como humedad y temperatura, no podrá garantizarse la permanencia del respaldo de la información.

1.3 PRESERVACIÓN DIGITAL

Los registros análogos y digitales que son almacenados en cualquier institución o corporación son la memoria viva de la organización, es por eso que se debe considerar el favorecimiento de la longevidad de la información digital.

Al aplicar sistemas de respaldo digital como los computacionales (archivo y respaldo de documentación), se debe ser conciente de los problemas de la obsolescencia tecnológica. Entendida ésta como la degradación de la información digital debido al envejecimiento de los soportes informáticos y físicos, que ocasionan la pérdida de datos o de información[3].

[3] BIA,Alejandro y SÁNCHEZ, Manuel. Desarrollo de una política de preservación digital: tecnología, planificación y perseverancia. (Online) Alicante: Biblioteca Virtual Miguel de Cervantes, Universidad de Alicante. 2003 (citado en 15 junio 2007)Disponible URL http://cervantesvirtual.com/

1.4 ANTECEDENTES LEGALES

- Con la promulgación de la Ley General de Archivos 594 de 14 de Julio de 2000, se establece la responsabilidad de la administración pública y de los funcionarios de archivo con la conservación de los documentos tanto en soporte de papel como los producidos con el uso de tecnologías de avanzada. Para ello es necesario partir de las evaluaciones técnicas sobre su conservación física, condiciones ambientales y operacionales, seguridad, perdurabilidad y reproducción de la información. Por otro lado, se deberán garantizar los espacios y las instalaciones necesarias para el correcto funcionamiento de los archivos, teniendo en cuenta las especificaciones técnicas requeridas en los casos de construcción, adecuación de espacios, adquisición o arriendo.

- En el artículo 9 del Acuerdo 060 de 2001 (Archivo General de la Nación), sobre conservación documental, se establece que “las entidades son responsables por la adecuada conservación de su documentación, para ello deben incluir en sus programas de gestión documental y en sus manuales de procedimientos, pautas que aseguren la integridad de los documentos desde el momento de su producción. Así, se requieren adoptar las normas relativas a la permanencia y la durabilidad de los soportes, tales como la NTC 4436 para papel y la NTC 2676 aplicable a los soportes digitales. La manipulación, las prácticas de migración de la información y la producción de backups, serán adaptadas para asegurar la reproducción y recuperación hasta tanto se estandaricen los sistemas de almacenamiento y formatos de grabación de la información”.

2. POLÍTICAS GENERALES PARA LA CONSERVACIÓN Y ALMACENAMIENTO DE LA INFORMACIÓN DIGITAL

Está sección busca consolidar políticas generales para la conservación y almacenamiento de la información digital a fin de que ésta se mantenga actualizada y respaldada permitiendo su accesibilidad, tal como sucede con los documentos en papel.

El respaldo de la información digital permite resguardar los archivos ante posibles eventos considerados como críticos: virus informáticos, fallos de electricidad, deficiencias de hardware y software, caídas de red, violación de la información, pérdidas por error humano, y sucesos catastróficos como: incendios, inundaciones, terrorismo, entre otros. Y aunque no se pueda prevenir cada una de

estos eventos, la Corporación sí puede prepararse para minimizar las consecuencias que éstas le puedan ocasionar al patrimonio digital de la entidad.

Política 1: acceso a la información.

Todo el personal que trabaja en la Corporación debe tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En el caso de personas ajenas a la Institución sólo el Jefe de Sistemas debe autorizar el acceso indispensable de acuerdo con los procesos en que participan las personas, previa justificación. (Cfr: Formato Asignación de Permisos de Acceso a Servidor de Archivos. En: Procesos en Athos\ServArchivos\FORMATOS PROCESOS\Formatos Sistemas).

Política 2: seguridad de la información.

Todo el personal de la Corporación es responsable de la información que maneje y deberá cumplir con las políticas establecidas en este documento y aquellas directrices que emanen de su directivas a fin de proteger la información y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

Todo el personal académico y administrativo de la entidad tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneja, especialmente si la información es de carácter institucional.

Política 3: seguridad para los servicios informáticos.

Los servicios informáticos que presta la Corporación, tales como: correo electrónico (Word Client), grupos de charla (ComAgent), deben ser usados únicamente para el desarrollo de las funciones laborales.

La Corporación se reserva el derecho de acceder y develar todos los mensajes enviados por medio del sistema de correo electrónico para cualquier propósito.

Política 4: seguridad en recursos informáticos

Para mantener la seguridad en las estaciones de trabajo, que es el principal recurso informático, es necesario cumplir como mínimo con lo siguiente:

Administración de usuarios: Establece cómo deben ser utilizadas las claves de

ingreso a los recursos informáticos. Define parámetros sobre la longitud mínima de las contraseñas, los tipos de caracteres que la componen y la frecuencia con la que los usuarios deben cambiarla, entre otras.

Perfil de Usuario: Para la utilización de los recursos informáticos la División de Sistemas aplicará los perfiles de usuario definidos por la Corporación de tal manera que permita asignar los privilegios que correspondan a las funciones de los diferentes usuarios.

Política 5: accesos restringidos

Las contraseñas de acceso a los recursos informáticos, que sean asignados al personal académico o administrativo de la Corporación son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona, por lo tanto, son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.

Política 6: seguridad en comunicaciones

Las direcciones internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la entidad, deberán ser consideradas y tratadas como información confidencial.

Política 7: almacenamiento y respaldo

La información digital soportada por la infraestructura tecnológica de la Corporación deberá ser almacenada y respaldada de acuerdo con las políticas generales y políticas del usuario, de tal forma que se garantice su disponibilidad.

El almacenamiento de la información deberá respaldarse interna y externamente a la Institución, para garantizar el patrimonio digital de la Corporación.

Los usuarios son directamente responsables de un buen uso en la gestión y manejo de la información digital en cada una de las estaciones de trabajo.

Política 8: contingencia

La administración de la Corporación deberá diseñar y poner en marcha un plan de contingencia que permita asegurar el respaldo de la información digital ante eventos catastróficos.

Política 9: seguridad física

La Corporación deberá contar con los mecanismos de control necesario para resguardar la información de la Corporación. Se limitará el acceso a áreas consideradas críticas.

Los centros de cómputo o áreas que la entidad considere críticas, deben ser lugares de acceso restringido y cualquier persona que ingrese a ellas deberá registrar el motivo del ingreso y estar acompañada permanentemente por el personal responsable del lugar.

3. CONSIDERACIONES TÉCNICAS PARA EL ALMACENAMIENTO DE LA INFORMACIÓN DIGITAL EN LA CORPORACIÓN UNIVERSITARIA LASALLISTA.

El almacenamiento digital en la Institución puede realizarse de diferentes maneras:

3.1 DISCO DURO DE LA ESTACIÓN DE TRABAJO.

En este caso, con la mayor capacidad de almacenamiento de los computadores, parece ser ilimitado el número de archivos que podemos guardar en nuestras estaciones de trabajo. Sin embargo, la *información institucional* no debe ser almacenada allí, por los riesgos o dificultades de las cuales se encuentran inmersos los sistemas de Información; estos pueden ser, entre otros:

- Es información a la que difícilmente pueden tener acceso otros empleados de la Corporación ya que no se encontraría en la red. En el momento que un empleado requiera de dicha información se requeriría de diferentes canales de comunicación para llevar la información a su destinatario, lo cual implicaría: enviar documentos voluminosos a través del correo electrónico (limitado), utilizar dispositivos de almacenamiento digital (USB, CDs, etc.), perder tiempo en el traslado de los documentos, entre otros.
- En caso de daños en el hardware, como por ejemplo el disco duro u otro que se presente en el computador, producto de apagones, sobre picos de tensión eléctrica, o la vida útil del equipo, se volvería irrecuperable la información.
- La información tiende a volverse descontroladamente redundante (duplicada). Se tienen varias copias del mismo documento en diferentes equipos, no todas ellas sincronizadas e importantes.

- La información institucional es mucho más vulnerable a un acceso no permitido.
- Es más fácil que una estación de trabajo sea vulnerable a virus informáticos que un servidor.
- El usuario accidentalmente puede borrar la información y no hay cómo recuperarla.
- No es fácil volver a versiones anteriores de un documento que se estaba trabajando como transitorio o temporal.
- Las estaciones de trabajo tienen mayor riesgo de robo, con la consecuente pérdida de los documentos guardados allí.

3.2 SERVIDOR DE ARCHIVOS.

Este es el medio que debe ser utilizado preferentemente para almacenar la información digital corporativa de uso cotidiano, por la facilidad que brinda la plataforma tecnológica de la Corporación Universitaria Lasallista y que consiste en lo siguiente:

- En los servidores de dominio de las áreas administrativa y académica de la Corporación (es decir, aquellos que validan usuario y contraseña de las estaciones de trabajo que se conectan a las redes), se establecen unas particiones especiales de sus discos duros que se dedican exclusivamente al almacenamiento de los archivos de las diferentes unidades. Actualmente estos servidores se llaman: ATHOS para la red administrativa y SOPHOS para la red académica.

  En una de las particiones en el servidor administrativo ATHOS se asigna unas carpetas con acceso restringido a los directores de unidad (por ejemplo: decano de facultad, jefe de programa) y las personas que ellos designen. Cada director podrá definir las sub-carpetas que desee dentro de su carpeta.

- Otra partición, en ambos servidores, tiene acceso totalmente público y sin ningún tipo de restricción para todo el personal que se pueda conectar a la red administrativa y académica. En adelante se llamarán papeleras de cada unidad, éstas facilitan el poder compartir información (archivos, documentos, etc.) entre los empleados que requieran de información oportuna por algún proceso o compañero que contenga información transitoria o definitiva para uso exclusivo de la Corporación, una de sus ventajas es el no tener que utilizar el correo electrónico para tal fin, pues éste presenta dificultades de almacenamiento y de tiempo de entrega, pero una de las desventajas es que la información que se encuentre en ellas está disponible para toda la comunidad

administrativa y académica, por tanto no podría haber confidencialidad. La información contenida en las papeleras será borrada por un funcionario de las división de Sistemas todos los viernes antes de las 17:00 horas, o según otra regularidad que para este efecto se defina . De esta información no se realizará backup.

La disponibilidad de la información almacenada en los servidores de archivos es permanente. Los servidores permanecen encendidos todos los días las 24 horas del día y únicamente cesa la posibilidad de acceso a ellos cuando hay alguna caída de los servicios, como por ejemplo, un daño en un servidor, la desconexión de una estación de trabajo a la red, la reiniciación de un servidor por aplicación de un parche de seguridad, el mantenimiento preventivo y correctivo tanto en hardware como en software, entre otros.

3.2.1 ACCESO A LOS DOCUMENTOS ALMACENADOS EN LAS CARPETAS RESTRINGIDAS DE LOS SERVIDORES DE ARCHIVOS.

Con el fin de garantizar el adecuado manejo y conservación de los documentos almacenados en las carpetas restringidas de las unidades, sólo se permitirá el acceso al jefe de cada unidad. Éste a su vez puede solicitar el otorgamiento de accesos a otras personas (auxiliares, secretarias, etc.) diligenciando el formato “Asignación de Permisos de Acceso a Servidor de Archivos”.

En el caso de los docentes, cada carpeta restringida es totalmente individual, no se pueden delegar privilegios a otros empleados o profesores de la Corporación. Cuando se retira un profesor, su carpeta es eliminada del Servidor de Archivos.

Mientras un usuario no sea autorizado por un jefe de unidad no tendrá acceso a las carpetas restringidas. Por lo tanto, es necesario ser muy cuidadoso con el uso de las claves de ingreso a la red, para evitar violaciones a la confidencialidad de la información.

3.2.2 RESPALDOS DE LA INFORMACIÓN.

La información almacenada en las carpetas restringidas se protege diariamente en cintas. Manteniéndose el siguiente esquema de protección:

- La protección diaria de lunes a viernes.
- La protección semanal (viernes o último día hábil de cada semana) del último mes corrido.

- La protección mensual (último día hábil de cada mes) del último año corrido. La protección del último mes debe tener una copia adicional guardada fuera de la Corporación.
- Una protección anual (último día hábil de cada año). Se dispone de información anual desde el 21 de diciembre de 2005.

La protección de la información realizada en el último mes así como el último año, es guardada en un tape fuera de la sede de la Corporación.

3.2.3 VOLUMEN DE ALMACENAMIENTO.

Se debe mantener control sobre el volumen de datos almacenado en el servidor de archivos. Para verificar el tamaño que ocupa una carpeta el usuario se debe realizar la siguiente operación en el orden descrito:

- Abrir el Explorador de Windows.
- Dar clic derecho sobre la carpeta.
- Clic izquierdo sobre propiedades. Aparece el tamaño en bytes, megabytes (MB) o gigabytes (GB). Tener en cuenta que: 1 MB= 1024 bytes; 1 GB = 1024 MB.

Cada unidad, incluyendo los docentes de planta, no deben exceder un tamaño de almacenamiento de 700 MB. Si éste es excedido, el servidor no dejará almacenar más información allí. La División de Sistemas revisará de manera permanente que ninguna carpeta exceda los 700 MB, en cuyo caso notificará al respectivo responsable de la carpeta. Para mejorar la capacidad que cada usuario tiene en el servidor de archivos, se recomienda:

- Eliminar la información que ya no es necesaria.
- Compactar algunas carpetas o archivos. Para ello se puede utilizar el WinZip que está instalado en los equipos de las secretarias y algunas unidades de la Corporación o el mismo que usa windows.
- Solicitar una protección en medios especiales (cintas, CDs-RW, etc.) de la información que no necesita estar permanentemente.

3.3 OTROS MEDIOS.

La información digital puede ser almacenada en otros medios tales como:

- Disquetes, con capacidad de almacenamiento de 1.44 MB, los cuales están cayendo en desuso que se evidencia en los equipos nuevos, los cuales no incluyen lectora de este medio.
- CDs, con capacidad de almacenamiento de hasta 700 MB. Para su grabación, requieren que el equipo tenga una unidad con capacidad de lectura / grabación (RW) y su respectivo software de grabación. En la Corporación hay un número limitado de máquinas con esta facilidad, por lo tanto, la unidad que requiera este tipo de grabación, puede solicitar ayuda a la División de sistemas.
- Memorias USB. Son dispositivos con capacidades de almacenamiento de 512 MB, 1024 MB, 2 GB, etc. Es un medio de almacenamiento digital temporal con facilidad para trabajar y respaldar información. Requiere un puerto USB en el equipo.
- Cintas (“Tapes”). Con capacidad de almacenamiento mayor a 12 GB. Se utilizan para proteger bases de datos, conjuntos de carpetas almacenadas en el servidor, etc. Se pueden utilizar para proteger información histórica que solamente se necesite consultar eventualmente, para ahorrar espacio en los servidores. Se deben grabar a través de un dispositivo especial (Tape Backup).
- Discos duros externos. Son medios físicos de almacenamiento de información de alto volumen, que van desde los 20 GB hasta 250 GB y en aumento. Por ser externo permite intercambiar información entre diferentes computadores u otros medios de almacenamiento.

4. POLÍTICAS A DESARROLLAR POR EL USUARIO PARA EL ALMACENAMIENTO DE INFORMACIÓN DIGITAL

Las siguientes políticas están diseñadas para todo el personal académico y administrativo de la Corporación que maneja información digital institucional. Es importante señalar que dentro de las políticas generales para la conservación de la información digital se establece la responsabilidad de todos los usuarios para cuidar y proteger el patrimonio digital de la Corporación.

Para simplificar los términos, de ahora en adelante al servidor de archivos lo denominaremos como ATHOS y el equipo de cómputo asignado a la unidad se llamará estación de trabajo.

Las políticas que deben asumir todos los usuarios de información digital en la Corporación son:

Política 1: documentos institucionales.

ATHOS es el recurso físico que está disponible para almacenar solamente los documentos institucionales que se generen en cada puesto de trabajo. Por ningún motivo se debe almacenar información personal, como: documentos de texto, hojas de calculo, imágenes, fotos, música, videos, ente otros.

Política 2: respaldo y acceso a la información en ATHOS.

- En ATHOS solamente se deben tener almacenados los documentos que correspondan a archivo activo o archivo permanente que necesiten ser consultados constantemente.
- La información correspondiente a archivo inactivo debe llevarse a un medio de acceso menos frecuente. Puede ser a un CD, a una cinta de protección semestral, anual, etc. Coordinar con la División de Sistemas para acordar la información que se necesita proteger y el medio a utilizar.
- Un archivo debe estar solamente en la carpeta restringida de la unidad responsable del mismo. Las demás unidades que lo requieran deben usarlo solamente como temporal, mientras está en estudio y luego eliminarlo una vez producida la versión definitiva.
- Las versiones definitivas deben ser convertidas al formato PDF con el fin de que estos archivos sirvan de consulta por los demás funcionarios y no puedan ser modificados sin autorización de la persona responsable del control de la información o del documento.

Nota: Debe solicitarse a la División de Sistemas que le instalen la versión libre del software PDF995

Política 3: actualización de documentos y/o de archivos.

En ATHOS sólo debe estar la última versión actualizada de un archivo o documento. Las versiones de prueba (documento borrador) pueden conservarse en el disco duro de la estación de trabajo.

Como recomendación los documentos han de trabajarse sobre una versión de prueba y cada cierto tiempo se actualizará conservando los cambios. Analizar cuidadosamente si es necesario guardar diferentes versiones de prueba de un archivo.

Política 4: utilización de las papeleras.

La información almacenada en las papeleras de cada unidad (Papeleras en "Athos") debe ser únicamente de carácter transitorio. No se garantiza ninguna confidencialidad durante el tiempo que permanezca allí, ya que puede ser leída, modificada o eliminada por cualquier usuario que tenga acceso a la red administrativa. Estas se borran por un funcionario de las división de Sistemas todos los viernes antes de las 17:00 horas, o según otra regularidad que se le defina y no se les realiza backup.

Política 5: respaldo de correo electrónico entrante.

El personal académico y administrativo de la Institución tiene un límite de 30 MB en el buzón de correo de dominio @lasallista.edu.co, que se considera un tamaño suficiente para hacer una buena gestión y uso de la información de correo electrónico. A los buzones de correo de los estudiantes que soliciten una cuenta en la Corporación se les asignará una capacidad de 10MB. También se determina un límite de 10MB al tamaño de los correos entrantes y salientes.

En caso de que se requiera conservar los correos, se debe realizar el siguiente procedimiento:

- Copiar el texto de correo en Word (o un editor de texto que tenga la estación de trabajo), con pegado especial / texto sin formato.
- Guardar el archivo en Word almacenado en una subcarpeta (dentro de la carpeta de la respectiva dependencia que puede ser nombrada como RespaldoCorreoElectrónicoEntrante) de ATHOS en la que sea fácilmente localizable.
- Archivar junto al correo los archivos anexos que sean de interés. Se recomienda guardarlos como archivos comprimidos con WinZip, auto-ejecutables (es decir, que se puedan abrir en cualquier equipo, aunque no se tenga WinZip instalado en él).

Política 6: manejo de correo electrónico saliente externo.

Al enviar un correo electrónico que contenga archivos anexos, debe tenerse en cuenta que muchos servidores de correo externo establecen límites sobre el volumen del archivo a recibir. Asimismo, la capacidad disponible del buzón del destinatario del correo puede convertirse en un obstáculo para que pueda recibirlo, por lo tanto se sugiere compactar el archivo anexo por medio del formato PDF.

Si se desea respaldar la información enviada, es recomendable seguir los pasos sugeridos en la política 5, acto seguido debe retirarse el mensaje enviado con el fin de liberar el espacio asignado en el buzón de correo.

Actualmente el servidor de correo de la Corporación no permite el envío ni el recibo de archivos con numerosas extensiones, tales como .zip, .gif ni .tiff, etc., ya que este tipo de archivos son frecuentemente utilizados para la transmisión de virus informáticos y no se cuenta con un antivirus de correo. Esta política puede variar si se establece otra plataforma de correo.

Cuando se está enviando o recibiendo información de personas confiables, se recomienda establecer una convención para modificar la extensión del archivo antes de anexarlo y advertirlo en el texto del mensaje, para que se restablezca una vez recibido el correo.

Política 7: manejo de correo electrónico saliente interno.

Al enviar un correo electrónico interno que contenga archivos anexos, es necesario hacer uso de las papeleras asignadas a las unidades, siempre y cuando el documento no sea de información confidencial. También se puede utilizar el ComAgent para envíos de archivos internos y como canal de información o divulgación directa y oportuna. Esto ahorra utilización de espacio en los buzones de correo y tráfico en la red de Internet.

Para personal de una misma unidad, se debe utilizar las carpetas restringidas. Puede definirse un esquema de carpetas con privilegios controlados de acceso en el que, por ejemplo, una secretaria tenga solamente una sub-carpeta de la dependencia y se lleven allí todos los documentos de correspondencia, borradores de documentos, etc.

Política 8: manejo de fotografías.

Cuando se utilicen o manejen imágenes o fotografías deben salvarse preferiblemente en el formato ".jpg" (comprimidas con pérdida de calidad) para su almacenamiento permanente. Este formato permite la reducción del tamaño del archivo. En el caso de las imágenes con formatos de alta resolución, se deberán almacenarse en CD´s o DVD´s, para evitar ocupar espacio en el servidor.

Las fotografías que se realicen institucionalmente se almacenarán en la carpeta de ATHOS destinada para este tipo de archivos (Fotografías en

"Athos\ServArchivos"). La capacidad máxima de almacenamiento en el servidor no podrá exceder los 700 MB de tamaño.

Si una unidad desea almacenar fotografías de interés institucional deberá remitirse a la unidad de comunicaciones para que ella se encargue de su almacenamiento, ya que esta unidad tiene el permiso de acceso a la carpeta de fotografías.

Política 9: manejo de multimedia.

Para el almacenamiento de archivos multimedia con fines académicos o institucionales (videos, sonido y presentaciones en herramientas como Flash player, entre otros) se deben guardar en medios masivos, como CD, USB, DVD, entre otros. En ningún momento se deberá emplear el servidor de archivos ATHOS para su respaldo.

Política 10: manejo de presentaciones y diapositivas.

Las presentaciones y diapositivas institucionales realizadas por las diferentes unidades en herramientas como Power Point no deben exceder en su cantidad y tamaño más allá de los 100 MB para ser guardadas en ATHOS. Si se llegara a sobrepasar esta capacidad se debe aplicar la política 9.

Artículo 2. La presente Resolución surte sus efectos a partir de la fecha de su expedición.

Dada en Caldas, a los 12 días del mes de julio de 2007.

(Original firmado) (Original firmado)

César Augusto Fernández Posada
Rector

Marta Lucía Martínez Trujillo
Secretaria General