POLITICA DE ARCHIVO Gestión de Información y Administración del Documento Electrónico			
Proceso: Gestión Documental			
Código	Versión	Emisión	Página
201.03.03.02.D3	01	22 de octubre de 2014	1 de 1

INTRODUCCIÓN

Las políticas y los estándares establecidos para la gestión documental institucional en este documento, son lineamientos y referentes marco para la administración y conservación de los activos informáticos, los documentos y los archivos de la Institución Universitaria Colegio Mayor del Cauca.

Con la definición de las políticas para la gestión de la información, la administración documental y la gestión archivística, se establece al interior de la institución una cultura de la calidad, operando de forma confiable y controlada, estructurando los requerimientos y patrones técnicos de organización archivística y aplicación de tecnologías a la gestión de documentos, involucrando todo el recurso humano comprometido en la gestión institucional de la información y el uso de los recursos informáticos.

En la institución universitaria Colegio Mayor del Cauca los documentos, los archivos y la información son de carácter público y por lo tanto cumplen con los objetivos esenciales de organización, clasificación, conservación y consulta en las diferentes fases del ciclo vital de los documentos, bajo el concepto de archivo total.

La gestión documental en la institución se basa en los principios archivísticos de procedencia y orden original de los documentos, se estructura en las tres fases reguladas por las tablas de retención documental y se soporta en la estructura orgánica-funcional de la entidad. La primera fase o primer ciclo vital de los documentos ocurre en los archivos de gestión, fase en la que los documentos se administran y conservan temporalmente en las oficinas por concepto de trámite o gestión. La segunda fase semi-activa, se cumple al ser transferidos los documentos de los archivos de gestión al archivo central para su descripción, conservación y consulta, y una tercera fase de conservación total en el archivo histórico después de agotados los tiempos de retención en el archivo central.

Finalidad de la Política:

Con el establecimiento de las políticas para la gestión documental institucional, se da enfoque y soporte a la producción, administración, procesamiento y recuperación de los documentos y la información, se garantiza el acceso, la publicación y divulgación de documentos auténticos, íntegros, usables y conformes, características que los hacen utilizables efectivamente en la gestión institucional y en la toma de decisiones, como garantía en la prestación del servicio que oferta el Colegio Mayor del Cauca.

Alcance:

Las políticas para la gestión documental en el Colegio Mayor del Cauca aplican para todo el Programa de Gestión Documental (PGD Institucional) desde la producción o recepción de los documentos, el direccionamiento, trámite, almacenamiento, consulta, conservación o disposición final según las Tablas de Retención Documental, contextualizando la información y los documentos como un activo estratégico para el cumplimiento misional.

1. POLÍTICA DE SEGURIDAD INSTITUCIONAL

La información y los documentos contenidos en los recursos informáticos, serán clasificados, trasmitidos, almacenados y custodiados de forma segura y controlada como soporte a los procesos institucionales misionales y de apoyo. El proceso institucional de gestión de recursos tecnológicos y de la comunicación (TIC) propondrá y controlará el cumplimiento de normas y políticas de seguridad informática que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de la información automatizada en general.

Todos los usuarios deben autenticarse con los mecanismos de control de acceso lógico: identificador de usuario y contraseña, siendo su responsabilidad la confidencialidad de los mismos, antes de tener acceso a los recursos de infraestructura tecnológica del Colegio Mayor del Cauca. No está permitido a los usuarios proporcionar información a personal externo sobre los mecanismos de control de acceso a los recursos e infraestructura tecnológica de la institución, salvo el caso de autorización expresa de la dirección.

Todo servidor o funcionario nuevo de la institución Universitaria Colegio Mayor del Cauca debe contar con la inducción sobre las políticas y estándares de seguridad informática, donde se dan a conocer las obligaciones y sanciones en que se puede incurrir en caso de incumplimiento.

2. POLÍTICA DE INTEGRIDAD Y AUTENTICIDAD DOCUMENTAL

El proceso de gestión documental en la institución es un proceso planeado, estructurado, administrado, documentado y revisado de manera integral a la función archivística y la administración pública. La integridad se define para la IUCMC como la propiedad del documento que indica que está completo, sin alteración con copiado autentico. La autenticidad se materializa en que puede probarse que el documento es lo que afirma ser, que ha sido creado por la persona que se afirma lo creó, en la fecha y sin modificación. Los recursos informáticos serán objeto de administración, custodia, respaldo, protección, mantenimiento preventivo y actualización permanente, implementando una visión organizacional eficaz y actualizada en la administración de la información y los documentos.

3. POLÍTICA DE CONFIABILIDAD

Los usuarios informáticos en la IUCMC, cumplirán las normas relacionadas con la seguridad informática, contarán con permisos de acceso a los sistemas de información y cumplirán con los principios de integridad, confidencialidad y autenticidad de la información. La confiabilidad del documento radica en que su contenido es una representación completa y precisa de la actuación, las actividades, los desarrollos y los resultados institucionales.

4. POLÍTICA PARA LA IMPLEMENTACIÓN DE LAS TABLAS DE RETENCIÓN DOCUMENTAL DIGITAL

La Tabla de Retención Documental Digital como instrumento archivístico que permite la clasificación, normalización y estandarización en la producción de los documentos, es aprobada, implementada y de obligatoria aplicación y consulta para la gestión documental en la IUCMC, institucionalizando el ciclo vital de los documentos, dando inicio al proceso de organización y automatización de documentos y archivos en soporte digital.

Objetivo de la Política: Establecer los requisitos para mantener la integridad archivística, técnica y estructural de los documentos institucionales electrónicos, en el sistema de gestión documental institucional.

Alcance de la Política: Aplica para todos los documentos institucionales en soporte digital, vinculados a los procesos y procedimientos del sistema de gestión, hasta su integración a un archivo de conservación o custodia y/o eliminación por tiempo de retención.

Normatividad Relacionada: Ley general de archivos 594 de 2000, Articulo 21. Gestión de documentos: todas las entidades públicas deben elaborar programas de gestión documental, contemplando el uso de nuevas tecnologías y soportes en cuya aplicación debe observarse los principios y procesos archivísticos.

Artículo 19. Las entidades del Estado podrán incorporar tecnologías en la administración y conservación de sus archivos: electrónico, informático, óptico o telemático, siempre y cuando cumplan con los siguientes requisitos: 1. Organización archivística de los documentos. 2. Realización de estudios técnicos para una adecuada decisión teniendo en cuenta la conservación, las condiciones ambientales, operacionales, de seguridad, perdurabilidad y acceso a la información contenida en estos soportes, así como el funcionamiento razonable del sistema.

Dcto 3816 de Dbre 31 de 2003: Creación de la comisión intersectorial de políticas y de gestión de la información para la optimización del uso de medios tecnológicos en la administración pública.

Decreto 2609 y 2578 de 2012, normatividad para archivos y documentos electrónicos.

5. POLITICA DE PROTECCIÓN DE LA INFORMACIÓN Y DE LOS BIENES INFORMATICOS

Los usuarios y servidores de IUCMC, deben preservar y proteger los registros y la información procesada en la infraestructura tecnológica, de igual forma protegerán la información almacenada o transmitida ya sea dentro de la red interna institucional a otras dependencias, sedes alternas o redes externas.

Todos los archivos de computadores que sean proporcionados por personal externo o interno (programas, software, bases de datos, documentos y hojas de cálculo) que tengan que ser descomprimidos, los usuarios deben verificar que estén libres de virus, utilizando el software antivirus autorizado en la institución antes de ejecutarse.

Todo incidente u ocurrencia de accidente de seguridad informática debe ser reportado oficialmente a la oficina de TIC.

Queda prohibido falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

6. POLÍTICA DE CONTROL DE VIRUS Y SOFTWARE MALICIOSO

Para prevenir infecciones de virus informático, los usuarios de la IUCMC, no deben hacer uso de software que no haya sido proporcionado y validado por la oficina de TICS. En el caso de sospecha de infección de virus, debe dejar de usar inmediatamente el equipo y notificar la sospecha a la oficina de TIC.

Se efectuarán controles para la generación y restauración de copias de respaldo o back-up como salvaguarda de información crítica de los procesos institucionales significativos, la realización de copias de respaldo o seguridad se harán periódicamente en los equipos administrativos y servidores. Las copias de seguridad deben rotularse para ser almacenadas, se utilizará el software OwnCloud en la opción de back-up. Opción datos: la rotulación contenida, fecha de copia, asunto, código según TRD digital y se entregará a la oficina de TIC para almacenamiento y custodia.

Cuando un funcionario no autorizado o visitante requiera entrar a las salas donde se encuentran los servidores, debe solicitar autorización mediante comunicación interna a la oficina de TIC.

Cuando se va a realizar mantenimiento en alguno de los equipos, se debe dar aviso con anticipación al usuario informático o servidor público.

7. POLÍTICA DE CONTROL DE ACCESO FÍSICO

Se deberá reportar y registrar al momento de la entrada, en el área de recepción, los equipos de cómputo, de comunicaciones, medio de almacenamiento y herramientas que no sean propiedad de la institución.

8. POLÍTICA DE PROTECCIÓN DE EQUIPOS

Los usuarios de IUCMC, no deben mover o reinstalar, reubicar los equipos, ni retirar sellos de los mismos sin autorización.

Es responsabilidad de los usuarios almacenar su información únicamente en la partición del disco duro diferente, destinada para archivos de programas y sistemas operativos (C: /

Es prohibido que el usuario o funcionario distinto al personal autorizado abra o destape los equipos, asimismo cuando se requiera realizar cambios de ubicación en lugares físicos de trabajo o locativos, debe ser notificado con 3 días de anticipación a la oficina de TIC.

El préstamo de portátiles o laptops tendrá que solicitarse en la oficina de TIC.

Todos los usuarios de los sistemas de información, serán registrados en la base de datos para la autorización de uso de dispositivos de almacenamiento externo (memorias USB, discos portátiles, unidades CD, DVD, así mismo para el manejo y traslado de información o realización de back-up.

Todo el personal o usuario informático nuevo de la institución deberá ser notificado a la oficina de TIC para asignarle derechos correspondientes, equipo, creación de usuario para la red y anulación en caso de retiro.

Controles de acceso lógico: Administración y uso de contraseñas /usuarios / equipos /

Controles para otorgar, modificar y retirar usuarios: Creación cuentas de usuario

Solicitud creación cuentas de usuarios

Seguimiento a back-up

Protección y ubicación de equipos: Pérdida de equipos

Uso de dispositivos extraíbles

Internet

9. POLÍTICA DE ADMINISTRACIÓN DE LA RED

Los usuarios informáticos de la IUCMC, no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de archivos (ftp) u otro tipo de protocolo para transferencia de información, empleando la infraestructura de la red de la institución sin autorización de la oficina de TICS.

10. POLÍTICA DE SEGURIDAD DE LA RED

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada, en la cual los usuarios o funcionarios realicen exploración de los recursos informáticos en la red de la IUCMC, así como de las aplicaciones que sobre dicha red operan, con fines a detectar y explotar una posible vulnerabilidad.

11. POLITICA DE ADQUISICIÓN DE SOFTWARE

Los usuarios o funcionarios que requieran instalación de software deben justificar su uso, indicando el equipo donde se instalará y el período de tiempo que será usado.

Se considera una falta grave que los usuarios instalen cualquier tipo de programa en sus computadores, servidores, estación de trabajo u otros equipos conectados a la red del colegio mayor que no esté autorizado por la oficina de TIC. Se debe mantener por parte de la oficina de TICS el inventario actualizado de equipos, programas y licencias instaladas.

12. POLÍTICA DE LICENCIAMIENTO DE SOFTWARE

Se prohíbe en la IUCMC, instalar software y programas no autorizados y sin licenciamiento en la red de la IUCMC.

13. POLÍTICA DE USO DEL CORREO ELECTRÓNICO

Los usuarios informáticos de la Institución Universitaria Colegio Mayor del Cauca, deben tratar los mensajes y los archivos adjuntos como información de propiedad de la institución.

No se deben utilizar cuentas de correo electrónico asignadas a otros usuarios, ni recibir mensajes en cuentas de otros, si fuera necesario leer el correo de alguien más (mientras se encuentra por fuera o de vacaciones) el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externo al Colegio Mayor del Cauca, a menos que cuente con una autorización de la oficina de TIC.

Los usuarios informáticos de la Institución Universitaria Colegio Mayor del Cauca, podrán enviar información reservada o confidencial vía correo electrónico siempre y cuando vaya de manera encriptada y destinada exclusivamente a personas autorizadas y en ejercicio de funciones y responsabilidades institucionales.

14. POLÍTICA DE AUTENTICIDAD DE LA INFORMACIÓN

Se cumplirán en la institución los procedimientos de archivo y gestión documental en la administración de los procesos. Se divulgarán solo documentos controlados, versionados, en formato estable y firmado digital. Se establecerán los roles y responsabilidades en la gestión documental, quiénes firman los documentos, quiénes están autorizados para modificar, suprimir o adicionar información institucional.

Elaboró:

Grupo de Trabajo Tic y gestión documental (Mildred Caicedo, John Jairo Perafan, Edgar Gutiérrez, Ana victoria Ospina Reina).