POLÍTICA DE COPIAS DE RESPALDO (BACKUPS)

COPIA CONTROLADA

Elaborado por:	Revisado por:	Aprobado por:
_____	_____	_____
Contratista Recursos Tecnológicos	Director Recursos Tecnológicos	Rector(a)

1. OBJETIVO

Garantizar el respaldo en forma segura de toda la información digital institucional que dentro del desarrollo de las funciones se considere documental, importante y crítica, generada en cada una de las dependencias y/o procesos de la Institución Universitaria Colegio Mayor del Cauca.

2. ALCANCE

Esta Política aplica para todo el personal administrativo, docente y contratistas de la Institución Universitaria Colegio Mayor del Cauca, que tienen a cargo procesos y actividades que generen información digital institucional importante y crítica. Comprende desde la clasificación de los archivos por parte de cada uno de los usuarios, hasta el almacenamiento y preservación de las copias de seguridad para cumplir con la disponibilidad, confidencialidad e integridad de la información.

COPIA CONTROLADA

3. DEFINICIONES

Información Documental: Son todos aquellos archivos digitales institucionales, creados por cada uno de los usuarios en sus respectivas dependencias.

Información Importante y Crítica: Son todos aquellos archivos digitales académicos/administrativos generados en la Institución.

Backup: Es una copia de seguridad a mayor o menor escala. Puede ser una versión reciente de la información contenida en todos los equipos de nuestra Institución, o puede tratarse de servidores completos con ingentes cantidades de datos.

Google Drive: Es un software para compartir y sincronizar archivos utilizando una cuenta de @unimayor.edu.co y es el que actualmente está siendo utilizado en la IUCMC.

Tablas De Retención Documental - TRD: Es el Instrumento que permite establecer cuáles son los documentos de una entidad, su necesidad e importancia en términos de tiempo de conservación y preservación y qué debe hacerse con ellos una vez finalice su vigencia o utilidad.

4. POLÍTICA

Todo activo de información que sea de interés para los procesos y/o subprocesos identificados en el Sistema Aseguramiento Interno de la Calidad (SAIC) de la Institución Universitaria Colegio Mayor del Cauca, deberá ser respaldada con copias de seguridad, en la periodicidad que establezca el proceso Gestión de Recursos Tecnológicos junto con el usuario final y de conformidad con las responsabilidades enunciadas en el numeral 5 de la presente política.

La IUCMC maneja los correos institucionales con la plataforma Google, entonces se aprovecha la herramienta Google Drive que permite realizar almacenamiento en la nube y copias de respaldo de la información, además de poder acceder a los archivos desde cualquier dispositivo móvil, tableta o computadora utilizando la cuenta de correo institucional.

La cuota de almacenamiento en la plataforma de Google tiene un límite, por lo tanto, se han caracterizado los usuarios por grupos y se le ha asignado una cuota de almacenamiento a cada grupo, esta caracterización se muestra en la tabla 1, de esta manera se garantiza que los usuarios siempre tengan espacio de almacenamiento.

COPIA CONTROLADA

Tabla 1: Cuotas de almacenamiento en Google Drive por grupo de usuarios

Grupo de usuarios	Cuota de almacenamiento por cuenta(GB)
Administrativos	Variable
Administrativos especiales	200
Procesos Campus	8000
Docentes Planta	150
Docentes TC	100
Docentes Cátedra	50
Estudiantes	30

Egresados	20
Contratistas	100

5. RESPONSABILIDADES

5.1. De los usuarios:

- **Crear una carpeta según TRD:** En el equipo asignado al usuario debe existir una carpeta ubicada en una partición diferente a la del sistema operativo y nombrada según la Tablas de Retención Documental - TRD - de cada dependencia, en dicha carpeta deben reposar todos los archivos y carpetas que se requiere respaldar mediante copia de seguridad.

COPIA CONTROLADA

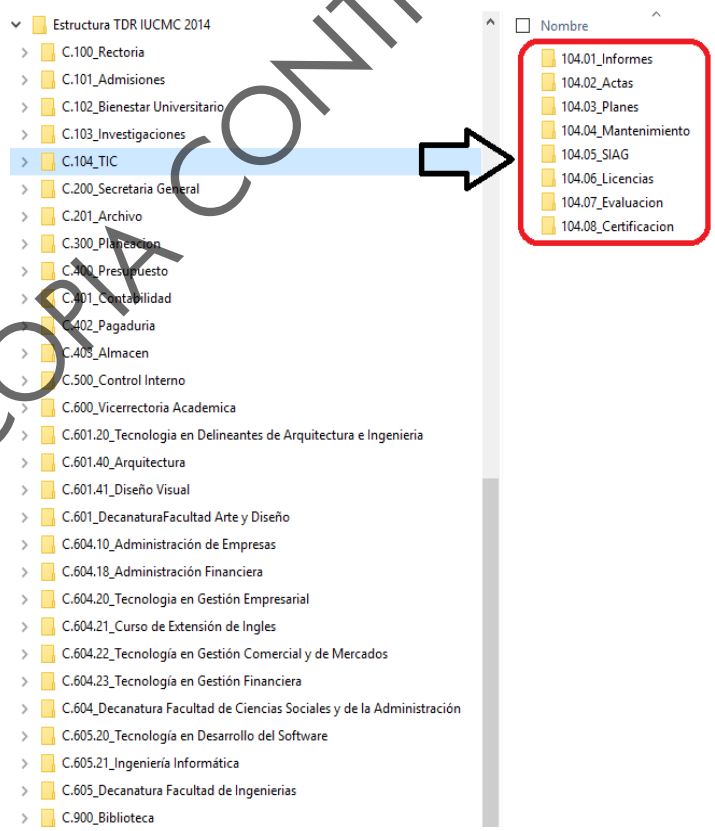

Figura 1: Estructura mínima de directorios según TRD general.

- **Conservar una copia de respaldo de la Información Institucional:** Toda la información institucional que se genere en cada una de las estaciones de trabajo debe estar alojada en la carpeta destinada para el proceso de copia de seguridad de la información y es responsabilidad del usuario garantizar que así sea. En el caso que el usuario almacene información en ubicaciones distintas a las establecidas para el proceso de respaldo y copia de seguridad de la información es responsabilidad directa del usuario si llegase a presentar una pérdida de información institucional.

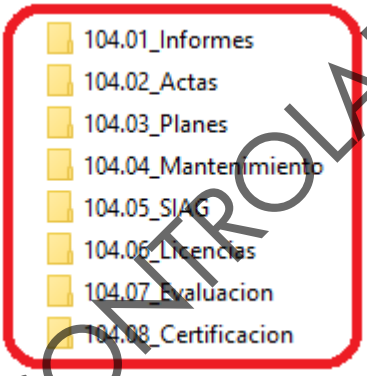

Figura 2: Ejemplo directorios de acuerdo a las TRD correspondientes al proceso de Gestión de Recursos Tecnológicos

COPIA CONTROLADA

- Verificar que la aplicación Google Drive esté activa en su computadora, de ésta manera se garantiza que haya respaldo de la información, de lo contrario el proceso no se llevará a cabo.
- Realizar el reporte inmediato ante cualquier anomalía en el aplicativo, si se detecta la no ejecución de la aplicación o cualquier otra anomalía, el usuario debe informar inmediatamente al proceso de *Gestión de Recursos Tecnológicos* en las extensiones 2244 y/o 2209 y a los correos electrónicos: tic@unimayor.edu.co, tdigital@unimayor.edu.co, seguridaddigital@unimayor.edu.co .
- No realizar copias de seguridad de datos personales, la información de carácter personal del usuario (imágenes, archivos, videos, música, etc) no deben estar en la carpeta designada para copia de seguridad. Para la IUCMC y el proceso de Gestión de Recursos Tecnológicos es menester respaldar y realizar copias de seguridad de la información estrictamente institucional.

5.2. Del proceso de Gestión de Recursos Tecnológicos:

- Suministrar a los usuarios las herramientas o recursos y capacitación necesarias para realizar las copias de seguridad.
- Realizar la instalación y configuración del Software en cada uno de los computadores de la institución.
- Mantener el software en correcto funcionamiento.
- Realizar y llevar registro de la revisión semestral de las copias de seguridad.
- Realizar visitas de verificación de buen uso del software y cumplimiento de la presente política.
- El asesor del proceso o su delegado deberá gestionar las medidas de protección lógica y física adecuadas.
- Si es requerido se realizará el soporte de sincronización automática Google Drive en modalidad de teletrabajo o trabajo en casa asistido por medios tecnológicos.

5.3. Administrador (Responsable) de las Bases de Datos:

- Realizar periódicamente copia de seguridad de la(s) base(s) de datos, asociada(s) a los sistemas de información institucional.
- Realizar pruebas de restauración de los backups con la periodicidad establecida dentro de su plan de mantenimiento, de manera aleatoria para garantizar que sean leídas y restauradas correctamente.
- Almacenar por lo menos en dos sitios físicos/virtuales diferentes las copias de seguridad de las bases de datos relevantes, con el fin de garantizar la continuidad de los procesos críticos.

COPIA CONTROLADA

6. DOCUMENTOS DE REFERENCIA

- MIPG
- ISO 27001
- MSPI- Modelo de Seguridad y Privacidad de la Información.
- Ley 1221 de 2008 y decreto 884 del 2012.
- Circular No. 0041 de 2020 Mintrabajo

7. DISPOSICIONES FINALES

7.1. DIFUSIÓN

El personal autorizado por el proceso Gestión de Recursos Tecnológicos realizará la socialización y/o difusión de esta Política a la comunidad universitaria y grupos de interés, de acuerdo a las directrices del documento 104.01.02.D.13 Plan de Sensibilización Seguridad y Privacidad de la Información.

7.2. ACTUALIZACIÓN

Para garantizar la vigencia, mejora continua y actualización de esta Política, deberá ser revisada por lo menos una vez al año por personal competente y autorizado del proceso Gestión de Recursos Tecnológicos y será el Comité Institucional de Gestión y Desempeño quien apruebe las mejoras a implementar.
Durante la actualización se deberá tener en cuenta la normatividad vigente, lineamientos institucionales y resultado de auditorías de seguridad y privacidad de la información.

7.3. SANCIONES

Ante el incumplimiento de esta Política se aplicará la normativa vigente en la Institución Universitaria Colegio Mayor del Cauca, además de las normas emitidas a nivel Nacional y Regional a través del proceso Gestión y Desarrollo del Talento Humano.

COPIA CONTROLADA

8. ANEXOS

Anexo A: Manual de procedimiento: Configuración de Google Drive para realizar copias de seguridad.

9. CONTROL DE CAMBIOS

FECHA DE CAMBIO	CAMBIOS REALIZADOS
03-06-2021	Se actualizó código de la política según nueva TRD.
26-10-2022	Se actualizó la herramienta software para realizar Backups, se actualizó las responsabilidades del usuario final, se anexó el manual de procedimientos para la instalación y configuración de la herramienta de Backups.