POLÍTICA DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

Elaborado por:	Revisado por:	Aprobado por:
_____	_____	_____
Contratista Seguridad y privacidad de la información	Director Gestión de Recursos Tecnológicos	Rector(a)

1. OBJETIVOS

- Establecer la Política de Gestión de los Activos de Información de la Institución Universitaria Colegio Mayor del Cauca.
- Proponer directrices para mantener un inventario actualizado de los activos de información y garantizar que reciban un nivel adecuado de clasificado, etiquetado y protección.

2. ALCANCE

La política define un esquema de alto nivel sobre las normativas de seguridad y privacidad de la información basado en la norma ISO/IEC 27001:2013 para la Gestión de Activos de Información, es de carácter obligatorio para todo el personal de la Institución, sea cualquiera el área donde labore o el nivel de tareas que desempeñe. Esta política aplica también a los terceros que tengan alguna relación con la Institución Universitaria.

3. DEFINICIONES

Activo de información: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, hardware, software, sistemas de información, edificios, personas, imagen, etc.) que tenga valor para la Organización.

Confidencialidad: propiedad de que la información no esté disponible o revelada a personas no autorizadas, entidades o procesos. [ISO/IEC 27000: 2016].

Disponibilidad: propiedad de ser accesible y utilizable a la demanda por una entidad autorizada. [ISO/IEC 27000: 2016].

Integridad: propiedad de exactitud y completitud. [ISO/IEC 27000: 2016].

Política: intenciones y direcciones de una organización como se expresan formalmente por la Alta Dirección. [ISO/IEC 27000: 2016].

4. POLÍTICAS Y NORMAS DE SEGURIDAD DE LA INFORMACIÓN – ACTIVOS DE LA INFORMACIÓN

La institución debe realizar un inventario de sus activos de información, y posteriormente, debe clasificarlos de acuerdo con los niveles de clasificación como confidencialidad,

disponibilidad, integridad y ubicación, para lo cual es necesario realizar una asignación de responsabilidades de los activos de información.
Se debe identificar, documentar y actualizar cualquier modificación de la información y los Activos consignados en el inventario. Este debe ser revisado con una periodicidad no mayor a un (1) año. Es responsabilidad de cada Líder de Proceso realizar y mantener actualizado el inventario de activos de la información en compañía del Líder de Seguridad de la Información.

Los niveles de confidencialidad según los cuales se deben clasificar los activos de información son:

- **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. [Ley 1712: 2014].

- **Información púbica clasificada:** Es aquella información que estando en poder o custodia de un objeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la [Ley 1712: 2014].

- **Información pública reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a interés públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la [Ley 1712: 2014].

Únicamente el funcionario responsable de la información puede asignar o cambiar su nivel de clasificación.
Se debe desarrollar procedimientos para el etiquetado y manejo de la información, de acuerdo con el esquema de clasificación definido en el presente documento. Estos procedimientos deben contemplar toda la información en formato físico y digital.

Se debe realizar el registro en el documento Activos de información, respetando la clasificación de la norma ISO 27001 además del responsable del activo y proceso al cual pertenece.

5. DOCUMENTOS DE REFERENCIA

- Ley 1712 de 2014
- ISO 27001

6. CONSIDERACIONES GENERALES

No aplica.

7. DISPOSICIONES FINALES

a. 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 de seguridad de la información.

b. ACTUALIZACIÓN

Para garantizar la vigencia, mejora continua y actualización de esta política, deberá ser revisada por lo menos una vez por año por personal competente y autorizado del proceso Gestión de Recursos Tecnológicos y será el comité integral de Planeación y gestión quien avale 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.

c. SANCIONES

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.

8. CONTROL DE CAMBIOS

FECHA DE CAMBIO	CAMBIO REALIZADO
2 de diciembre de 2019	Se realizó actualización del alcance de política y adición del numeral 7. Disposiciones finales.

21 de septiembre del 2021	Se actualizó apartado de sanciones.
14 de junio del 2022	Se realizó revisión de la política en todos sus aspectos con el equipo de seguridad de la información donde se considera que actualmente no requiere modificación relevante a la fecha evaluada. Se realizó actualización de cargo de asesor TIC a Director de Gestión de Recursos Tecnológicos. Se actualizó el código de la política según nueva TRD. Se actualizó el nombre del proceso según el nuevo mapa de procesos.
13 de octubre de 2022	Se actualiza la política según revisión realizada por el proceso de Gestión de Recursos Tecnológicos