POLÍTICA DE DISPOSITIVOS MÓVILES

COPIA CONTROLADA

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

1. OBJETIVO GENERAL

Establecer las políticas y normas para asegurar el uso apropiado y eficaz de los dispositivos móviles institucionales o personales para proteger la confidencialidad, autenticidad y/o integridad de la información a la que accedan dentro de la Institución Universitaria Colegio Mayor del Cauca.

2. ALCANCE

Este documento aplica para todos los funcionarios, contratistas, y terceras personas que tengan acceso a las instalaciones de la Institución, sistemas de información y servicios de red.

3. TÉRMINOS Y DEFINICIONES

-**Integridad:** Propiedad de la información que pretende mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

-**Disponibilidad:** Propiedad de la información que pretende garantizar el acceso y uso de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

-**Dispositivo móvil:** Elementos de procesamiento de datos, conexión a internet y memoria de tamaño pequeño, ejemplo: celulares, tabletas y portátiles.

-**Confidencialidad:** Propiedad de la información que pretende garantizar que esta sólo es accedida por personas o sistemas autorizados.

-**Información:** Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

-**Dato:** Es una representación simbólica (numérica, alfabética, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.

-**SGSI:** Sistema de Gestión de Seguridad de la Información.

4. MARCO NORMATIVO

- Constitución política de Colombia
- Ley 80:1993 Estatuto general de contratación de la administración pública.
- Ley 87:1993 sobre Control Interno de los organismos del Estado.
- Ley 594:2000 Ley General de Archivo
- Ley 599:2000 Código penal colombiano.

COPIA CONTROLADA

- Ley 603:2000 Control de legalidad del Software
- Ley 734:2002 por la cual se expide el Código Disciplinario Único.
- Ley 1266:2008 Por la cual se dictan las disposiciones del Habeas Data y regulaciones del manejo de la información.
- CONPES 3701:2011Lineamientos de política para Ciberseguridad y Ciberdefensa.
- CONPES 3854:2016 Política Nacional de Ciberseguridad
- Ley 1581:2012 Por la cual se dictan disposiciones generales para la protección de datos personales y su decreto reglamentario 1377:27/06/2013.
- Manual para la Implementación de la Estrategia Gobierno en Línea.
- Herramienta MSPI de MINTIC
- Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión y seguridad digital.
- ISO/IEC 27000 Marco de gestión de seguridad de la información.
- NTC ISO 9001:2015 sobre la gestión de Sistemas de Calidad

COPIA CONTROLADA

5. MARCO DE REFERENCIA

La institución Universitaria Colegio Mayor del Cauca, reconoce la información como un activo relevante para el cumplimiento de la misión en el ámbito educativo, por lo tanto adopta la familia de la serie ISO/IEC 27000, que proporciona un marco de gestión de la seguridad de la información para cualquier organización, dando prioridad a la normas ISO/IEC 27001 "implementación del Sistema de Gestión de Seguridad de la Información SGSI", ISO/IEC 27002 "manual de buenas prácticas para la gestión de seguridad de la información" e ISO/IEC 27005 "Directrices para la Gestión de Riesgos en seguridad de la información", Herramienta Modelo de Seguridad y privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) y los documentos del Sistema Integrado de Calidad (SGI) de la Institución Universitaria Colegio Mayor del Cauca, disponible en: https://campus.unimayor.edu.co/CampusSGI/

6. DIRECTRICES

a. Seguridad para dispositivos móviles que accedan a información de la IUCMC.

CONTROL	DIRECTRICES
Desarrollar e implementar una política sobre el uso de dispositivos	La autorización para la aplicación y cumplimiento de la política de dispositivos móviles debe ser solicitada al subproceso de gestión de recursos tecnológicos por medio escrito o correo electrónico, en el caso de añadir un nuevo dispositivo móvil.
	La comunidad institucional debe aceptar las configuraciones de seguridad impuestas en los dispositivos móviles las cuales no podrán ser modificadas ni eliminadas mientras estos dispositivos tengan acceso a la información de la IUCMC.

	Configurar los dispositivos móviles con mecanismos de acceso como contraseñas con más de 8 caracteres, por lo menos una letra mayúscula y un número, a su vez huella digital o en el caso de un Smartphone patrón de seguridad de al menos 7 puntos de contacto.
	Establecer tiempos de bloqueo de pantalla menores a 10 minutos de actividad.
	Instalar y configurar un software antivirus dentro de los dispositivos móviles.
	Establecer opciones de borrado seguro y remoto de la información en los dispositivos móviles con el fin de eliminar información sensible perteneciente a la IUCMC.
	Realizar cifrado de los dispositivos móviles. Esto de acuerdo a la política de uso de controles criptográficos.

b. Seguridad para dispositivos móviles que sean propiedad de la IUCMC

CONTROL	DIRECTRICES
Desarrollar e implementar una política sobre el uso de dispositivos móviles.	No está permitido almacenar información personal en dispositivos móviles que sean entregados y asignado por la IUCMC.
	No es permitido que el usuario del dispositivo móvil reinstale el sistema operativo o instale uno nuevo del que este ha sido configurado por la IUCMC.
	No se permite que se realicen instalaciones de aplicaciones o softwares diferentes a las autorizadas por el subproceso de gestión de recursos tecnológicos.

c. Seguridad para personal que configura los dispositivos móviles.

CONTROL	DIRECTRICES
Desarrollar e implementar una política sobre el uso de dispositivos móviles.	Los encargados de la configuración deben respetar los lineamientos otorgados por la presente política de dispositivos móviles.
	Los dispositivos que no sean entregados por la IUCMC y que no se encuentren configurados con la presente política deben presentar la solicitud donde se menciona tanto la aceptación de las configuraciones de seguridad como el cumplimiento total de la política de dispositivos móviles.
	Se deben configurar los dispositivos móviles exclusivamente con cuentas institucionales para un mayor control de acceso a la información de la IUCMC.

COPIA CONTROLADA

7. DISPOSICIONES FINALES

a. DIFUSION

El personal autorizado por el subproceso 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 al año por personal competente y autorizado del subproceso Gestión de Recursos Tecnológicos y será el comité integral de planeación y gestión 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.

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
10-10-2022	Se actualizan denominaciones y códigos de documentos de la política, según la operación vigente.

COPIA CONTROLADA