POLÍTICA DE USO DE CONTROLES CRIPTOGRÁFICOS

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 la criptografía que protege la confidencialidad, autenticidad y/o integridad de la información 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.

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

-Token: Dispositivo físico utilizado para acceder a un recurso restringido electrónicamente.

-Criptografía: Se ocupa del estudio de los algoritmos, protocolos y sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican.

-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.
- 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

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 Tecnológicas 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

6.1. USO DE CONTROLES CRIPTOGRAFICOS

CONTROL	DIRECTRICES
Desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información	Emplear la herramienta de cifrado definida por la IUCMC en: • Unidades de disco duro de equipos portátiles de funcionarios con información sensible. • Claves de acceso a sistemas de información, datos y servicios (Token). • Información reservada y clasificada de la institución. • Correos electrónicos institucionales con información reservada y clasificada.
	Verificar que todo sistema de información que requiera realizar transmisión de información clasificada o reservada cuente con mecanismos de cifrado de datos.
	Utilizar controles criptográficos para la transmisión de información clasificada o reservada, fuera del ámbito institucional.
	Disponer de herramientas que permitan el cifrado de la información sobre los medios de almacenamiento de la institución.

6.2. GESTION DE LLAVES

CONTROL	DIRECTRICES
Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de	Comunicar por medio del subproceso de gestión de recursos tecnológicos, la solicitud para obtener de nuevo su información, en caso de que al ingresar al sistema realice más de tres intentos de inicio de sesión, dado que en estos casos el disco duro del equipo de cómputo portátil será cifrado.
	Desbloquear contraseña de los usuarios atendiendo requerimiento del olvido de contraseña a través del subproceso de gestión de recursos tecnológicos.

	Restablecer la información de los usuarios atendiendo requerimiento a través de la mesa de ayuda de tecnología en caso de que el disco duro sea cifrado por intento de acceso fallido.
	La asignación del tiempo de vida de las llaves criptográficas la realiza el usuario administrador de dominio del directorio activo, de acuerdo con el contexto y particularidades en el momento de la asignación. (Revisar para desagregar de acuerdo con oportunidad de mejora).

7. DISPOSICIONES FINALES

7.1. DIFUSIÓN

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.

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 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.

7.3. 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 relacionados con la política, según la operación vigente.