

POLÍTICA DE TELETRABAJO

COPIA CONTROLADA

Elaborado por:

Revisado por:

Aprobado por:

Contratista Seguridad de la
Información

Director Gestión de
Recursos Tecnológicos

Rector(a)

POLÍTICA CONTROL DE ACCESO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
Proceso: Gestión de Recursos Tecnológicos			
Código	Versión	Emisión	Página
100.05.05.D.47	02	10-10-2022	2 De 5

1. OBJETIVO GENERAL

Establecer las políticas y normas para asegurar la continuidad del trabajo que realiza el personal institucional garantizando la confidencialidad, disponibilidad, 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.

-**Teletrabajo:** Forma legal acordada entre el empleador y su empleado para realizar sus labores en un lugar físico diferente al de las instalaciones de la entidad.

-**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

POLÍTICA CONTROL DE ACCESO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
Proceso: Gestión de Recursos Tecnológicos			
Código	Versión	Emisión	Página
100.05.05.D.47	02	10-10-2022	3 De 5

- 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 3701:2011 Lineamientos 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
- Ley N° 2088 del 12 de mayo del 2021 Por la cual se regula el teletrabajo en casa y otras disposiciones.

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

6.1. AUTORIZACIÓN PARA TELETRABAJO

La autorización para teletrabajo de cualquier miembro de la Institución Universitaria Colegio Mayor del Cauca debe ser provista por el jefe inmediato una vez sea analizada por las altas directivas. Dentro de los términos para entregar la autorización se tendrá en cuenta los siguientes datos:

- Nombre del empleado.
- Ocupación del empleado.
- Justificación por la cual se requiere el teletrabajo.
- Fecha de inicio del teletrabajo.

POLÍTICA CONTROL DE ACCESO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
Proceso: Gestión de Recursos Tecnológicos			
Código	Versión	Emisión	Página
100.05.05.D.47	02	10-10-2022	4 De 5

- Fecha final del teletrabajo.
- Horario establecido de teletrabajo para el empleado.
- Aplicaciones a ser usadas por el empleado (Opcional).

Una vez las altas directivas aprueben la autorización de teletrabajo para el empleado, esta será enviada al jefe inmediato del subproceso de Gestión de Recursos Tecnológicos para que se otorguen las configuraciones necesarias de acuerdo a la institución.

6.2. EQUIPO PARA TELETRABAJO

Al ser otorgada la autorización de teletrabajo del empleado al jefe inmediato del subproceso de gestión de recursos tecnológicos se debe validar el equipo remoto que será utilizado por el empleado. Este equipo de cómputo puede ser:

- Equipo de cómputo asignado por la Institución Universitaria Colegio Mayor del Cauca con las configuraciones realizadas por el área TIC.
- Cliente VPN que será configurado por el área TIC.
- Escritorio virtual que permite al empleado acceder remotamente mediante credenciales a un escenario simulado que asemeja la interacción física de un sistema computacional.

Esta selección del equipo remoto a utilizar por el empleado o su configuración dependerá de los recursos con los que se cuente en el momento y de las tareas a ejecutar.

6.3. CONEXIÓN

Independientemente del equipo de cómputo o la configuración establecida, se deberá tener en cuenta las políticas de seguridad de la información de la IUCMC. A su vez, se establecen consideraciones importantes dentro de los cuales el empleado debe hacer mayor realce:

- No establecer conexiones dentro de lugares públicos, por ejemplo, aeropuertos, cafés, bares, restaurantes, centros comerciales, entre otros.
- Cumplir con las recomendaciones del área TIC y la autorización de las altas directivas.
- Se debe respetar los requerimientos de seguridad establecidos por el área de tecnología como lo es: restricciones a sitios, configuración del equipo, divulgación de información y demás.
- No será permitido que las sesiones establecidas con la IUCMC sean utilizadas por terceros, es decir, las conexiones a la institución solo serán válidas por el empleado autorizado para teletrabajo.
- Reportar anomalías que se presenten en el periodo del teletrabajo.

7. DISPOSICIONES FINALES

POLÍTICA CONTROL DE ACCESO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
Proceso: Gestión de Recursos Tecnológicos			
Código	Versión	Emisión	Página
100.05.05.D.47	02	10-10-2022	5 De 5

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.