POLÍTICA CONTROL DE ACCESO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Elaborado por:	Revisado por:	Aprobado por:
PU Seguridad Digital	Director Gestión de Recursos Tecnológicos	Rector(a)

1. OBJETIVO GENERAL

Establecer las políticas y normas para garantizar un adecuado control de acceso a físico y lógico de la Institución Universitaria Colegio Mayor del Cauca.

1.1. OBJETIVOS ESPECÍFICOS

- Identificar la información relacionada con los activos.
- Definir los perfiles de usuarios comunes (estándar) para los puestos de trabajo comunes.
- Definir los niveles de acceso de acuerdo a la clasificación de activos asegurando la Confidencialidad, Integridad y Disponibilidad de la información.
- Identificar los requerimientos de seguridad y privacidad de la información según el Anexo A de la Norma ISO 27001:2013 y requisitos de la herramienta MSPI (Modelo de Seguridad y Privacidad de la Información).

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

Se tomarán los mismos términos y condiciones dados dentro del documento 104.01.02.D.20 Plan de Seguridad y Privacidad de la Información. Disponible en la url: https://campus.unimayor.edu.co/CampusSGI opción: Campus Unimayor SAIC/Gestión de Recursos Tecnológicos/Seguridad de la Información/Documentos y https://unimayor.edu.co/web/transparencia?layout=edit&id=2855

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 Tecnologías de la Información y las Comunicaciones (MINTIC) y los documentos del Sistema de Gestión Integrado (SGI) de la Institución Universitaria Colegio Mayor del Cauca, disponible en: https://campus.unimayor.edu.co/CampusSGI opción Campus Unimayor SAIC.

6. CONTROL DE ACCESO

6.1. REGLAS PARA EL CONTROL DE ACCESO

Para prevenir el acceso no autorizado a la información, físico y lógico, la Institución Universitaria Colegio Mayor del Cauca (IUCMC) ha definido políticas y procedimientos

que garanticen el ingreso adecuado a la red, sistemas de información, bases de datos, sistemas operativos, áreas restringidas y elementos que permitan el acceso a información relevante.

El acceso a los sistemas de información se rige por el principio de mínimos privilegios: Todos los programas y usuarios del sistema deben operar utilizando el menor conjunto de privilegios necesarios para realizar la labor. Los derechos de acceso deben adquirirse sólo por permiso explícito; por omisión deberían ser "sin acceso".[1]

Los controles (reglas) están documentados dentro de los procedimientos y manuales de seguridad y privacidad de la información; publicados y disponibles en el Sistema de Gestión Integrado; https://campus.unimayor.edu.co/CampusSGI opción Campus Unimayor SAIC.

Las directrices descritas en este documento son complementarias el Sistema Integral de Calidad para aseguramiento de la información, como activo indispensable para la consecución de los objetivos y estrategias de la IUCMC.

6.2. POLÍTICA DE CONTROL DE ACCESO

La institución Universitaria Colegio Mayor del Cauca establece medidas de control de acceso físico y acceso lógico a nivel de red, sistema operativo, sistemas de información y servicios de TI. Estas medidas son de conocimiento de todo el personal de la Institución y limitan el acceso a los activos de información de acuerdo con lo indicado por el rol o perfil del cargo establecido.

6.3. ACCESO A REDES Y SERVICIOS EN RED

El acceso a redes desde y hacia afuera de la Institución se debe realizar a través de credenciales de acceso cumpliendo con los lineamientos de GESTION DE CONTRASEÑAS. (Numeral 6.9)

El Administrador de redes y servidores deberá generar un procedimiento para la activación y desactivación de permisos de acceso a las redes para administrar:

- El acceso a los servicios de red internos y externos.
- Las redes (VLANS) y servicios de red a los cuales se permite el acceso.

[1] Tomado de: https://pepeirlinux.wordpress.com/2012/06/06/los-principios-de-diseno-de-las-medidas-de-seguridad/

- Acceso a servidores.

Las conexiones deben ser restringidas al horario normal de oficina, a menos que exista un requerimiento operativo de horas extra. En caso de permitir acceso por fuera de este horario, debe documentar y discriminar a funcionarios o contratistas con permiso, sus motivos y evidencia de la autorización expedida por el líder de proceso y validación líder del proceso de gestión recursos tecnológicos.

El Administrador de redes y servidores es responsable de restringir el acceso a páginas relacionadas con contenido para adultos, pornografía, drogas, alcohol, webproxys, web transfer, descargas de música, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en la Institución y páginas que no sean de uso corporativo mediante el uso de un servidor proxy, firewall o la estrategia que mejor se ajuste a los recursos y protección de los activos de información.

El acceso a los sitios web anteriormente mencionados será permitido únicamente por solicitud (escrita o por correo electrónico) del líder de proceso, según la necesidad del cargo una vez el Técnico Administrativo de redes (persona encargada de redes) y el encargado del Sistema de Gestión de Seguridad de la Información validen que el sitio sea confiable y no comprometa la seguridad de las redes.

Se deben mantener instalados y habilitados únicamente los servicios y puertos que sean utilizados por los sistemas de información y software de la institución. El acceso lógico a estos servicios debe ser controlado mediante la apropiada configuración del firewall.

6.3.1. AUTENTICACIÓN DE USUARIOS PARA CONEXIONES EXTERNAS

El acceso remoto a conexiones externas se realiza previa autorización y coordinación con el administrador de Redes y funcionarios de la IUCMC, haciendo uso de programas de acceso remoto y las credenciales personales descritas en el numeral 6.8, únicamente se realiza durante los días y jornada laboral y con supervisión de personal del proceso Gestión de Recursos Tecnológicos.

6.3.2. IDENTIFICACIÓN DE EQUIPOS EN LA RED

El proceso de Gestión de Recursos Tecnológicos es el responsable por la administración de los equipos conectados a la red cableada Institucional, mediante la configuración de DHCP para asignación automática de direcciones IP asociada a la dirección MAC (de las siglas en ingles Media Access Control) única de cada equipo.

6.3.3. ACCESO REMOTO

El responsable de la red de datos Institucional deberá mantener restringido el acceso a sistemas y servicios internos desde fuera de la red, aplicando las medidas de seguridad necesarios para proteger la información y evitar posibles intrusiones.

Para realizar soporte técnico remoto, los usuarios responsables de cada equipo de cómputo institucional deberán permitir el acceso y control remoto al proceso de Gestión de Recursos Tecnológicos, teniendo la precaución de no dejar a la vista información sensible y supervisar el equipo mientras dura la sesión de acceso remoto.

Será responsabilidad del proceso de Gestión de Recursos tecnológicos difundir e informar a los funcionarios con acceso remoto a sistemas y servicios, las políticas y procedimientos de seguridad a tener en cuenta dentro de las actividades a desarrollar, si es el caso deberá comunicar las responsabilidades para AUTENTICACIÓN DE USUARIOS PARA CONEXIONES EXTERNAS (numeral 6.3.1.)

Será responsabilidad de los funcionarios con acceso remoto autorizado, el cumplimiento de las medidas de seguridad y privacidad.

6.3.4. ACCESO DE TERCEROS

Los terceros como: proveedores, consultores, empresas de soporte, entre otros, deberán cumplir con la política de seguridad y privacidad de la información de la IUCMC.

El proceso Gestión de Recursos Tecnológicos proporcionará credenciales de autenticación temporal a terceros para permitir el acceso remoto o interno a sistemas de información y/o servicios de red, una vez termine el uso se deberán eliminar dichas credenciales.

Incluir en TODOS los contratos cláusulas de seguridad y confidencialidad de la información.

6.3.5. SEPARACIÓN DE REDES

Para garantizar la seguridad en las redes de datos el proceso Gestión de Recursos Tecnológicos deberá administrar a través de firewall o UTM (Unified Threat Management) el acceso a la Red Institucional, la segmentación se debe realizar en los equipos de enrutamiento configurando listas de control de acceso y VLANs, teniendo en cuenta la siguiente clasificación:

- Administrativos
- Servidores
- Biblioteca
- Wifi:

  - ✓ Administrativos
  - ✓ Docentes
  - ✓ Estudiantes
  - ✓ Invitados
  - ✓ Aulas Móviles
  - ✓ CEU
  - ✓ IT
  - ✓ DSI
  - ✓ Sala de juntas
  - ✓ Rectoría
  - ✓ Usabilidad
  - ✓ FI
- Financiera
- Salas de computo
- Cámaras
- Laboratorios
- DMZ
- VPN

6.3.6. CONTROL DE CONEXIÓN DE LAS REDES

El proceso Gestión de Recursos Tecnológicos de la IUCMC responsable por la red institucional, administrará el acceso a los servicios tanto internos como externos.

La conexión de portátiles, equipos de cómputo de escritorio, todo en uno y portátiles conectados a puntos cableado, se hará mediante protocolos y validación de parámetros de red previa autorización del responsable de redes de la IUCMC.

Con el fin de garantizar que los usuarios no comprometan la seguridad de la información, administrará las siguientes redes Wifi, asignando parámetros de seguridad y contraseña para su uso.

- Administrativos
- Docentes
- Estudiantes
- Invitados
- Aulas Móviles
- CEU
- IT
- DSI

- Sala de juntas
- Rectoría
- FI
- Usabilidad

6.3.7. CONTROL DE ENRUTAMIENTO DE RED

El proceso Gestión de Recursos Tecnológicos suministrará el servicio de internet a través de sus ISPs (Proveedor de Servicios de Internet), respetando los protocolos y aspectos técnicos contractuales y enrutamiento de la red de datos, deberá realizarse mediante VLANs o separación de redes, según los criterios del numeral 6.35, a través de configuración de políticas de acceso en la plataforma UTM (por las siglas en inglés de Administración unificada de Amenazas - Unified Threat Management-) y requisitos del numeral 6.6 (Control de acceso a sistemas o servicios informáticos).

6.3.8. SEGURIDAD EN LOS SERVICIOS DE RED

El proceso Gestión de Recursos Tecnológicos deberá:

- Mantener instalados y habilitados UNICAMENTE los servicios y puertos necesarios por los sistemas de información y software licenciado.
- Administrar el acceso lógico a los servicios y sistemas permitiendo el ingreso al personal autorizado haciendo uso de sus credenciales personales.
- Los niveles de rendimiento y seguridad deben ser definidos e incluidos en los acuerdos de nivel de servicio, tanto internos como externos; además de definir el medio por el cual se realizará la verificación de cumplimiento.

6.4. ACCESO A INTERNET

La IUCMC tendrá un ISP (por su sigla en inglés: Internet service provider) principal y un ISP secundario que hará las veces de canal alterno o de respaldo para garantizar continuidad de servicios evitando suspensión o alteración en la misión Institucional. El acceso y uso de internet estará regulado por el manual de mejores prácticas.

6.4.1. LIMITACIÓN DE TIEMPO DE CONEXIÓN

Para evitar acceso no autorizado el tiempo de conexión a internet estará limitado a la jornada laboral así: Red cableada, de lunes a sábado entre las 6:15 hasta las 23:30, red Wifi, de lunes a sábado entre la 6:50 hasta las 22:15

Por lo anterior, se suspenderá el acceso a internet el día Domingo; se exceptúa la conexión de los servidores (y/o activos con información sensible).

6.5. ACCESO FÍSICO

El acceso físico a las sedes de la IUCMC estará administrado por una empresa experta en seguridad, cualquier alteración o ingreso no autorizado será su responsabilidad. La comunidad IUCMC deberá tener en posesión su respectivo carnet de identificación para el ingreso y/o adquisición de alguno de los servicios con los que cuenta la entidad.

6.5.1. ACCESO A LAS INSTALACIONES

Está permitido el acceso a las instalaciones o sedes de la Institución, excepto a las áreas o procesos que manipulen activos de información identificados como sensible, en cuyo caso se deberá gestionar permiso por personal responsable del área, proceso y/o activo.

Para acceso a las instalaciones en horarios no laborales o ingreso de personal externo para adelantar trabajos o servicios contratados se deberá solicitar permiso por escrito en Secretaria General, detallando: nombres completos, número de identificación, nombre de la empresa contratada, fecha y hora de entrada y de salida.

6.5.1.1. ÁREAS SEGURAS

Se consideran áreas seguras y con acceso restringido las zonas destinadas a almacenamiento o procesamiento de información, donde se ubiquen equipos e infraestructura tecnológica y de comunicaciones.

La IUCMC identifica las siguientes áreas seguras:

- Gestión Financiera y contable
- Gestión Jurídica
- Gestión de Recursos Tecnológicos
- Oficina Sistema de información
- Gestión Documental
- Centros de datos
- Decanaturas
- Centros de Cableado y/o Subestaciones de energía.

Los Centros de datos, y/o áreas de procesamiento de datos sensibles se deberán proteger con sistemas de control de acceso para administrar el ingreso de personal autorizado además de llevar un registro de altas y baja.

6.5.1.2. INFORMACIÓN SOBRE ÁREAS SEGURAS

La información sobre las áreas seguras y de manera especial los servidores, solo será conocida por quienes tienen necesidad de manipularla por la labor que desempeña según lo dispuesto en el manual de funciones.

6.5.2. ACCESO FÍSICO A ARCHIVADORES Y DOCUMENTACIÓN

De manera general debe restringirse el acceso físico a zonas de oficinas (o áreas) que hagan uso de equipos de cómputo con información Institucional, equipos de comunicaciones y/o almacenen documentos físicos en archivadores, de manera que solo ingrese personal autorizado.

Es potestad de los líderes de proceso otorgar permiso para el acceso a la información que este bajo su responsabilidad.

Los archivadores deberán estar con llave y estas deberán guardarse en un lugar seguro.

6.5.3. UBICACIÓN EQUIPOS DE CÓMPUTO

Se deberá cumplir las directrices del manual de mejores prácticas, numeral 6.2.4 Escritorio Limpio Y Pantalla Limpia; de manera especial:

- Ubicar los equipos de cómputo institucionales de manera que impida el acceso innecesario a las áreas de trabajo y reducir el riesgo que personal ajeno pueda visualizar la información cargada en pantalla.
- Se deberá tener en cuenta los procedimientos del Sistema de Gestión de Seguridad y Salud en el trabajo, respetando zonas de evacuación.

6.6. CONTROL DE ACCESO A SISTEMAS O SERVICIOS INFORMÁTICOS

El proceso de Gestión de Recursos Tecnológicos debe asegurar el bloqueo al acceso de páginas de contenido para adultos, redes sociales, hacking, descargas (FTP), mensajería instantánea y cualquier página que represente riesgo potencial para la Entidad mediante el uso de servidor proxy, firewall o el software que mejor se ajuste a la necesidad. Excepciones de acceso, serán aprobados por el jefe inmediato, según la necesidad del cargo y verificación previa de que las páginas solicitadas no contengan código malicioso con la aprobación del responsable de seguridad de la información.

La concesión de acceso a sistemas de información con privilegios administrativos se dará mediante la red cableada (Ethernet); exclusivamente a equipos institucionales cuyo ingreso y responsable esté formalizado de acuerdo al documento: 403.03.03.01.P.01 procedimiento administración de almacén general, Se prohíbe el acceso a sistemas de información y servicios críticos con privilegios administrativos por red WIFI.

6.6.1. GESTIÓN DE ACCESO A USUARIOS

Los responsables o propietarios de los activos de información deberán revisar periódicamente los derechos de acceso otorgados o en curso de todos los usuarios de los sistemas o plataformas a su cargo.

La autorización de acceso a sistemas o plataformas será otorgada de acuerdo a las funciones asignadas para el desarrollo de la labor.

El acceso a sistemas de información y/o servicios de red debe realizarse de acuerdo a los numerales, 6.6. Control de acceso a sistemas o servicios informáticos y 6.8. Gestión de contraseñas.

6.6.2. PERFILES DE USUARIO

La asignación de perfiles o roles en los sistemas de información de la Entidad y acceso a servicios de TI, se deberá documentar en cada sistema o servicio de acuerdo a lo indicado los derechos de acceso en cada perfil y las funciones que pueden realizar, el dueño de sistema es el responsable de la asignación de permisos y roles.

Las autorizaciones de acceso privilegiado deben tramitarse por el líder de proceso o jefe inmediato cuando se requiera, haciendo uso de correo institucional o sistema de incidencias y posterior solicitud de este último al líder del proceso Gestión de recursos Tecnológicos, quien aprobará el acceso y direccionará la petición a quien corresponda, garantizando la posible afectación de disponibilidad, integridad o confidencialidad de la información de la IUCMC.

6.6.3. ADMINISTRACIÓN DE PRIVILEGIOS

El acceso a los sistemas de información, servicios de red e información en cualquier formato está determinado por el principio de mínimo privilegio; se otorgarán casos por caso según la necesidad para el cumplimiento de las funciones asignadas a docentes, terceros, funcionarios, temporales y contratistas.

El acceso a la información contempla permisos específicos para leer, escribir, modificar, borrar o ejecutar; utilidades para manipular o hacer uso de información institucional. El acceso administrativo a servidores y equipos de red, será exclusivo de personal autorizado del proceso Gestión de Recursos Tecnológicos.

6.6.4. REVISIÓN PERIÓDICA DE ACCESO A SISTEMAS O SERVICIOS DE RED

Se deberá realizar revisión de manera regular mínimo cada semestre, para validar las conexiones permitidas con la finalidad de asegurar que sean las que deben estar vigentes.
Previa iniciación de semestres el sistema Campus reportes de la IUCMC será utilizado como fuente de información para realizar un reporte del personal con contrato vigente, este será suministrado al personal autorizado del proceso Gestión de Recursos Tecnológicos quien ejecutará la suspensión de las cuentas y/o accesos a los diferentes sistemas de información.

6.6.5. CAMBIO DE ESTADO DE ACCESO

Todos los cambios de acceso deben ir acompañados de una justificación válida relacionada y alineada al análisis de seguridad.
Cuando ya no se requiera el acceso a los servicios informáticos, será necesario que el líder de proceso notifique mediante un correo electrónico o por escrito al responsable del proceso Gestión de Recursos Tecnológicos para restringir el acceso a los servicios tecnológicos.
Si existe un incidente de seguridad como acceso indebido a la red, cambio o finalización de empleo, será necesario una modificación a los permisos actuales, o en efecto, suspensión total a la conexión.

6.7. INICIO SEGURO

A fin de proveer un mayor grado de seguridad en los accesos, en servicios de red, sistemas de información y sistemas operativos se deberá ingresar mediante inicio seguro de sesión, nombre de usuario y contraseña (ver numeral 6.8. Gestión de contraseñas), además deberá contemplar las siguientes condiciones:

- No suministrar mensajes de ayuda, durante el tiempo de autenticación
- Omitir datos visibles durante el cargue de inicio.
- Limitar el número de intentos fallidos de acceso.
- No transmitir datos de contraseña para autenticación en texto claro.
- No mostrar los caracteres digitados de la contraseña.
- Evitar que el sistema guarde la contraseña digitada.

6.8. GESTIÓN DE CONTRASEÑAS

La asignación de la contraseña (credenciales de acceso) para acceso a sistemas, servicios de red (incluidas plataformas) o equipos de cómputo (personal administrativo, docente, contratistas) se realizará de forma individual, por lo tanto, el uso de

contraseñas compartidas está prohibido. En caso de compartir las credenciales de acceso, el usuario autorizado será el ÚNICO responsable de acciones que otras personas hagan con su contraseña.
Los usuarios son responsables de todas las actividades realizadas con su identificación de usuario y contraseña.
Las credenciales de acceso a sistemas de información inicialmente suministrada por un administrador de sistema son válidas solamente para la primera conexión del usuario, quien debe cambiarla una vez realice el primer ingreso al sistema.
Es responsabilidad de los usuarios salvaguardar sus credenciales de acceso (usuario y contraseña), por ningún motivo deberán estar visibles en cualquier medio impreso o escrito en el área de trabajo.
Los responsables de los sistemas deberán implementar métodos de recuperación de contraseña.
Los usuarios deberán Informar oportunamente al personal responsable de los sistemas o redes sobre cualquier inconveniente con los accesos de usuario.

Los usuarios deberán cumplir con los siguientes parámetros para construir y uso de las contraseñas:

- Debe estar compuesta al menos con doce (12) caracteres. Deberá incluir caracteres alfabéticos en mayúscula y minúscula, numéricos y símbolos o caracteres especiales. No deberá incluir la "ñ" ni letras con tilde para evitar errores.
- La contraseña podrá ser cambiada por el dueño de la cuenta.
- El usuario no deberá generar contraseñas que incluyan datos personales, familiares o de mascotas, que sean fáciles de averiguar.
- Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, tendrá la obligación de cambiarla inmediatamente.
- Los sistemas de información deberán configurarse con límite de intentos consecutivos infructuosos para ingreso de credenciales de acceso, que deberá ser como máximo tres (3). Superado el tope se suspende el acceso del usuario hasta que el administrador de la base de datos active el usuario nuevamente.
- Las contraseñas no deben ser parte o estar incorporadas dentro de los sistemas, de esta manera se garantizará que las contraseñas se puedan cambiar cuando se requieran.
- Los intentos fallidos a nivel de acceso en red en algunos casos se les tiene programada cuarentena de IP o bloqueo del acceso indefinido.

- Cuando un usuario bloquee su cuenta debido a la superación del número máximo de intentos, debe reportarlo al líder del proceso Gestión de Recursos Tecnológicos o profesional del área de desarrollo de sistemas de Información, indicando a que sistema de información o servicio, para que se le active la cuenta y restaure su contraseña.
- Los sistemas, equipos de red o cualquier activo de información Institucional con contraseña y/o usuario proporcionado por el fabricante (contraseñas por defecto) deberán ser cambiados antes de ponerse en producción.

6.9. USO DE UTILITARIOS DEL SISTEMA

Los utilitarios o programas básicos (como 7zip, desfragmentador, reproductores, reproductores multimedia, etc.) instalados en los equipos de cómputo y servidores de la Institución deberán ser licenciado o versión libre.

El proceso Gestión de Recursos Tecnológicos será el responsable por la instalación de los programas utilitarios necesarios en cada uno de los equipos de cómputo de la IUCMC.

El personal responsable de realizar mantenimiento de equipos de cómputo deberá restringir mediante contraseña el ingreso al BIOS y deshabilitar la opción de booteo por unidades extraíbles.

7. PROTECCIÓN DE PUERTOS USB.

Los puertos USB de equipos de cómputo de escritorio y portátiles estarán habilitados y el uso es responsabilidad exclusiva de los usuarios finales.

7.1. GESTIÓN DE MEDIOS REMOVIBLES

Los medios removibles (memorias USB, discos externos) NO son alternativa de respaldo de información permanente, siendo responsabilidad de los usuarios mantener la información en los servidores, servicios en la nube o equipos destinados para tal fin.

Los medios removibles autorizados por el proceso Gestión de Recursos tecnologías para almacenar información Institucional, deben ser escaneados cada vez que sea conectado a un equipo de la red institucional.

Los medios removibles autorizados con datos que puedan comprometer la confidencialidad e integridad de los mismos, deberán usar técnicas criptográficas para su protección.

8. TIEMPO DE INACTIVIDAD DE LA SESIÓN – EQUIPOS DESATENDIDOS

Los equipos de cómputo del personal administrativo, docentes y contratistas deberán ser configurados para que después de 10 minutos entre en inactividad sin cerrar las sesiones de aplicación, mostrando en pantalla inicio de sesión solicitud contraseña para desbloquear el sistema.

El usuario deberá bloquear su sesión, cuando abandone temporalmente el puesto de trabajo y deberá asegurarse de apagar los equipos de cómputo al finalizar la jornada laboral.

8.1. ACCESO A SISTEMAS SENSIBLES

El proceso Gestión de Recursos Tecnológicos deberá establecer controles estrictos para el acceso sistemas y activos físicos sensibles (servidores, firewalls) con el fin de salvaguardarlos de accesos no autorizados.

Deberá implementarse controles biométricos en los centros de datos y procesamiento de información.

8.2. COMPUTACIÓN Y COMUNICACIONES MÓVILES

El personal administrativo que haga uso de equipos de cómputo portátiles deberá cumplir con la política y demás directrices de seguridad de la información aprobada y publicada por la IUCMC.

Todo el personal de la comunidad universitaria es responsable por el uso o almacenamiento de información en los equipos móviles personales (celulares, Tablet o portátiles).

8.2.1. TRABAJO REMOTO

Cuando los funcionarios requieran acceder a servicios de red desde fuera de la institución deberán realizar la solicitud por escrito o correo electrónico, al líder del proceso Gestión de Recursos Tecnológicos; indicando los servicios de red o sistemas de información requeridos y tiempo de conexión.

Se deberán cumplir los controles de acceso remoto numeral 6.3.3, además, el responsable de la red institucional deberá proveer controles necesarios para garantizar la seguridad de la información.

8.3. ACCESO A EQUIPOS TI

Los equipos de cómputo del proceso Gestión de Recursos tecnológicos tendrán privilegios de administrador y deberán cumplir los controles de inicio seguro, numeral

6.7, gestión de contraseñas, numeral 6.8 y demás controles que apliquen para el cumplimiento de la política de seguridad y privacidad de la información.
Los servidores, firewall, routers, switches y equipos considerados como sensibles deberán estar aislados en salas de servidores y comunicaciones (centro de datos), deberán cumplir con las condiciones ambientales necesarias, planes de contingencia y acceso restringido sólo para personal autorizado del proceso gestión de Recursos Tecnológicos; es responsabilidad de este último mantener actualizada la información del centro de datos e informar a quién corresponda, de cambios en las condiciones de seguridad.

8.4. RETIRO DE ACTIVOS

La reparación o retiro de activos o componentes hardware de oficinas está prohibido, salvo autorización y requerimiento expreso de personal del proceso Gestión de Recursos Tecnológicos o terceros autorizados y supervisados por esta dependencia.
El retiro de activos de las sedes de la Institución se deberá hacer tramitando el formato: 104.07.R.17 orden de entrada y salida de elementos tecnológicos.

En caso de pérdida o daño total del dispositivo retirado, el funcionario público deberá dar aviso al personal de Gestión de Recursos Tecnológicos y Gestión jurídica, quien deberá realizar los trámites legales pertinentes.

9. DISPOSICIONES FINALES

9.1 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 de seguridad de la información.

9.2 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 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.

9.3 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.

10.CONTROL DE CAMBIOS

FECHA DE CAMBIO	CAMBIO REALIZADO
2 de diciembre de 2019	Se realizó actualización de documento alineado con los resultados obtenidos del diagnóstico MSPI (Modelo de Seguridad y Privacidad de la Información) emitido por MINTIC (Ministerio de Tecnologías de Información y las Tecnologías). Plan de tratamiento de riesgos, además se hizo modificación de título.
21 de septiembre del 2021	Se actualizó separación de redes y conexión a las mismas. Se actualizó apartado de sanciones.
23 de junio del 2022	Se actualizó separación de redes y conexión de las mismas, tiempo de inactividad y número de caracteres en contraseña. Se realizó actualización de cargo de asesor TIC a Director de Gestión de Recursos Tecnológicos. Se actualiza nombre del proceso, según nuevo mapa de procesos. Ahora corresponde al macro proceso de apoyo. Se actualiza código de la política según nueva TRD.
13 de octubre de 2022	Se actualiza la política según revisión realizado desde el proceso de Gestión de Recursos Tecnológicos.

21 de junio del 2023	Se actualizó apartado 6.3.5 Separación de redes. Se actualizó apartado 6.3.6 Control de conexión de redes. Se actualizó apartado 6.8 Gestión de contraseñas. Se actualizó apartado 8.4 Retiro de activos.
9 de febrero de 2024	Se actualiza código según TRD aprobadas por el Consejo Departamental de Archivos.