- **Política de Planeación Institucional**

  El Colegio Mayor del Cauca para cada periodo rectoral incluye y planifica los ejes temáticos identificando líneas estratégicas, misionales y de apoyo, para las cuales se establecen planes, programas y proyectos encaminados al cumplimiento de la misión y visión institucional, y que permita visualizar las metas alcanzables durante la vigencia del Plan de Desarrollo Institucional aprobado.

- **Política de Gestión Presupuestal y Eficiencia del Gasto Público**

  El Colegio Mayor del Cauca, incorpora en su gestión prácticas administrativas que permiten la optimización del uso de los recursos públicos y la generación de resultados eficientes. La actividad contractual y financiera se soporta en la planeación de las actividades a desarrollar en cumplimiento de los procesos estratégicos, misionales y de apoyo, encaminados al cumplimento de las metas establecidas por la Institución en su Plan de Desarrollo. La institución atiende sus procesos misionales y administrativos valiéndose de las NICSP y de las mejores prácticas contractuales y financieras, racionalizando con ello los gastos de funcionamiento e inversión, cumpliendo con ser una Institución fiscalmente responsable.

- **Política de Talento Humano**

  El Colegio Mayor del Cauca se compromete a adelantar procesos de selección, inducción y evaluación acorde con la normatividad vigente; adoptar anualmente para sus servidores públicos un Plan de Capacitación y Formación que propenda por el mejoramiento continuo y un Programa de Bienestar Social Laboral fundamentado en los principios y valores institucionales.

- **Política de Integridad**

Con el propósito de garantizar ante los grupos de valor el actuar honesto, ético y profesional, el Colegio Mayor del Cauca hará partícipes a sus Directivos, Administrativos, Docentes y Contratistas en la construcción, implementación, evaluación y divulgación del Código de Integridad institucional, logrando con ello su interiorización.

- **Política de Transparencia, acceso a la información pública y lucha contra la corrupción**

  El Colegio Mayor del Cauca se compromete a generar estrategias sobre: Lineamientos de Transparencia Activa, lineamientos de Transparencia Pasiva, Elaboración de los instrumentos de gestión de la información y Monitoreo del Acceso a la Información Pública, brindando acceso a la información, a los trámites y servicios para una atención oportuna y efectiva, dando cumplimiento a lo dispuesto en la Ley 1712 de 2014.

- **Política de Fortalecimiento organizacional y simplificación de procesos**

  El Colegio Mayor del Cauca se compromete con la identificación, racionalización, simplificación y automatización de trámites, procesos, y procedimientos, así como el uso adecuado de los recursos, garantizando respuestas oportunas, innovadoras, flexibles a las necesidades y requerimientos del entorno y la comunidad.

- **Política de Servicio al Ciudadano**

  El Colegio Mayor del Cauca establece los procedimientos y protocolos para la atención a los grupos de valor identificados, desde la recepción, así como la gestión y trámite de las peticiones, quejas, reclamos, sugerencias, denuncias y felicitaciones recibidos a través de los diferentes medios de atención (presencial, telefónico y digital).

- **Política de Participación Ciudadana en la Gestión Pública**

  El Colegio Mayor del Cauca establece los mecanismos de participación ciudadana para los grupos de valor identificados, y los medios de comunicación que la entidad coloca a su disposición para acceder a la información y facilitar la participación en la toma de decisiones de la Institución.

- **Política de Racionalización de Trámites**

  El Colegio Mayor del Cauca se compromete a revisar, actualizar y racionalizar sus trámites y procesos administrativos, con el fin de generar celeridad, eficacia y transparencia en las relaciones con sus partes interesadas y la comunidad en general.

- **Política de Gestión Documental**

  El Colegio Mayor del Cauca realiza apropiación de la metodología general que permite la implementación de los ocho procesos de la Gestión Documental: planeación, producción, trámite, organización, transferencia, disposición final, preservación a largo plazo y valoración documental, como el marco conceptual, jurídico y técnico, para la implementación y desarrollo del Programa de Gestión Documental PGD, al interior de la institución.

- **Política de Gobierno Digital**

  El Colegio Mayor del Cauca se compromete a avanzar en la implementación de la estrategia de Gobierno en Digital, designando al interior de la Entidad la responsabilidad en su desarrollo y el seguimiento y verificación del cumplimiento de cada uno de los componentes de la estrategia, promoviendo la utilización de los medios electrónicos.

- **Política de Seguridad Digital**

  El Colegio Mayor del Cauca, entiende y conoce la existencia de riesgos en seguridad de la información que pueden afectar el desarrollo de la misión institucional. En consecuencia, se compromete a realizar las tareas necesarias para mantener la confidencialidad, integridad y disponibilidad de los activos de la información, mediante una gestión de riesgos, asignación de responsabilidades en seguridad y la participación activa de las partes interesadas, cumpliendo con la normatividad vigente y para lograr la mejora continua.

- **Política de Defensa Jurídica**

  La política de prevención del daño antijurídico y defensa judicial del Colegio Mayor del Cauca busca identificar las causas de los daños antijurídicos que se presentan en la Institución y que como consecuencia podrían generar posibles demandas, las cuales pueden dar como resultado fallos en contra. La política de prevención del daño antijurídicobusca establecer estrategias al interior de la Institución para identificar los riesgos y costos de los procesos judiciales.

- **Política de Control Interno**

  El Colegio Mayor del Cauca, se compromete a aplicar el Sistema de Control Interno tal como lo establece la Dimensión 7 del Modelo Integrado de Planeación Gestión y a velar por su cumplimiento por parte de todos los servidores públicos para que desarrollen estrategias que conduzcan a una administración eficiente, eficaz, imparcial, íntegra y transparente, por medio de la autorregulación, la autogestión, el autocontrol y el mejoramiento continuo para el cumplimiento de los fines del Estado, y propiciando el control estratégico, el control de gestión y el control de evaluación.

- **Política de Seguimiento y Evaluación del Desempeño Institucional**

  El Colegio Mayor del Cauca realizará seguimiento y evaluación del desempeño institucional con el fin de recopilar, analizar y divulgar la información asociada con la ejecución del Plan de Desarrollo Institucional mediante el monitoreo y seguimiento a los riesgos identificados, al cumplimiento de planes, programas y proyectos, el manejo eficaz y eficiente de los recursos y la satisfacción de los grupos de valor, generando la cultura del mejoramiento continuo de cada uno de sus procesos para garantizar el logro de los resultados previstos en la gestión institucional.

- **Política de Gestión del Conocimiento e Innovación**

  Con el propósito de fortalecer la capacidad y el desempeño institucional el Colegio Mayor del Cauca, establece planes, programas y proyectos que se interrelacionan en los ejes de generación y producción, herramientas para uso y apropiación, analítica institucional y cultura de compartir y difundir, con el fin de lograr lo establecido en las metas institucionales.

- **Política de Mejora Normativa**

  La producción normativa es entendida como el proceso por medio del cual la administración establece reglas mediante instrumentos jurídicos dotados de legalidad, los cuales inciden en las diferentes esferas de la población y garantizan el entendimiento entre la sociedad y la administración.

  Uno de los beneficios de adoptar la política de mejora normativa es el fortalecimiento de la legitimidad del accionar de la administración al garantizar la protección de

derechos y así contribuir al amparo del Estado Social de Derecho.

Para la materialización de la Política de Mejora Normativa es necesario establecer unos lineamientos para efectuar el diagnostico, definición de herramientas y posterior construcción del plan de acción, por ello algunas de las actividades a tener en cuenta son:

- ✓ Adelantar inventario con los diferentes procesos con el objetivo de eliminar normas obsoletas, racionalizar o suprimir si es el caso.
- ✓ Hacer seguimiento al cumplimiento de los estándares y herramientas definidas por la política para la mejora de la producción normativa.
- ✓ En mediano y largo plazo evaluar la percepción de los grupos de valor en la mejora normativa implementada.

- **Política de Gestión Estadística**

El Colegio Mayor del Cauca se compromete a generar y disponer la información estadística, así como la de sus registros administrativos, de acuerdo con los lineamientos establecidos por MIPG, para mejorar la efectividad de su gestión y planeación basada en evidencias; garantizando una continua disponibilidad de información de calidad a lo largo del ciclo de su gestión, fomentando la participación de sus grupos de valor y de interés identificados, para la construcción participativa de soluciones a sus necesidades y expectativas, y generando una herramienta de control que permita la transparencia en las actuaciones como institución de educación superior pública.

- **Política Ambiental**

El Colegio Mayor del Cauca, está comprometido con el cuidado y protección del medio ambiente, mediante el mejoramiento continuo de su gestión ambiental, el desarrollo de acciones de prevención de la contaminación y de control de los aspectos ambientales significativos asociados a las actividades realizadas en la Institución. El Colegio Mayor del Cauca promoverá el respeto por los recursos naturales, el uso racional de los recursos, manejo de residuos y dará cumplimiento de los requisitos legales ambientales y otros suscritos por la institución.

- **Política Ambiental Cero Papel**

El Colegio Mayor del Cauca, Institución Universitaria, asume su compromiso con la

sociedad reconociendo su deber como entidad educativa del estado y se propone aportar a la mejora continua del medio ambiente en sus sedes. El Colegio Mayor del Cauca busca promover un entorno ambientalmente sano para el desarrollo de su misión, mitigando las problemáticas ambientales que se presentan en sus espacios, velando por la eficiencia administrativa y los lineamientos exigidos por la Política Cero Papel, incorporando el uso de las herramientas tecnológicas en la gestión documental y el uso racional del papel, articulando las actividades del plan ambiental en sus procesos, previniendo la contaminación y cumpliendo con los requisitos legales ambientales aplicables vigentes.

- Política de Control de acceso

El 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.

- Política de Desarrollo Seguro

El Colegio Mayor del Cauca establece controles para garantizar que la seguridad y privacidad de la información sea un requisito para el desarrollo de nuevos sistemas o la mejora de existentes. En caso de que el desarrollo sea llevado a cabo por el personal de la Institución, debe incluirse los requisitos de seguridad de la información en los nuevos sistemas de información o la mejora de los actuales.

Estos requisitos deben ser identificados mediante herramientas como: obtención de requisitos de cumplimiento a partir de políticas y reglamentación, modelado de amenazas, revisiones de incidentes o umbrales de vulnerabilidades. Esta identificación debe ser documentada y revisada por las partes interesadas.

En caso de que estos desarrollos sean producidos por terceros, debe seguirse un proceso formal de adquisición, que incluya los requisitos de seguridad de la información de la Institución. Se deben realizar pruebas periódicas a los sistemas de información de la entidad, para lo cual se debe tener bien definidos ambientes de pruebas seguros; en caso de que el desarrollo sea hecho externamente a la Institución, debe exigirse este

ambiente de pruebas al proveedor en los contratos, estos ambientes deberán permitir ser auditados por personal autorizado de la Institución. De igual manera, el nivel de protección de la información que se encuentra en un ambiente de prueba no puede ser menor que el utilizado en procesos de desarrollo.

Debe evitarse que los datos de producción sean utilizados para el desarrollo; en caso de ser necesarios, estos datos deben permanecer en estos ambientes y deberán estar bajo monitoreo permanente. El proceso Gestión de Recursos Tecnológicos debe implementar los controles necesarios para asegurar que las migraciones entre ambientes de desarrollo, pruebas y producción sean aprobadas de acuerdo al procedimiento de control de cambios. El Profesional Universitario de Desarrollo de Sistemas de Información, debe certificar que cualquier tipo de desarrollo que vaya a ser pasado a producción cumple con los requerimientos de seguridad establecidos antes de realizar este proceso.

Esta validación se realiza con metodologías o instructivos establecidos o creados por el equipo de desarrollo de sistemas de Información para tal fin, documentando todas las pruebas realizadas. Es responsabilidad del Profesional Universitario de Desarrollo de Sistemas de Información que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén adecuadamente actualizados y parchados. Todo desarrollo, que haya sido creado internamente o adquirido por terceros, debe contar con un proceso de soporte. En caso de ser creado de manera interna, el (los) desarrollador(es) deben proporcionar un nivel adecuado de soporte, capacitación y documentación; en caso de ser adquirido por terceros o de manera externa, debe exigirse durante la contratación que se cuente con un proceso de soporte, capacitación y documentación para los incidentes que puedan presentar las aplicaciones.

Todas las aplicaciones (sistemas), desarrollos internos o externos, deben asegurar que:

- Tengan una opción de cerrar sesión o desconexión, que permite terminar completamente con la sesión, disponible en todas las páginas protegidas por autenticación o control de acceso lógico.
- Los formularios de ingreso de datos deben validar aspectos como tipos de datos, longitud, rangos válidos, listas de caracteres aceptados, caracteres considerados peligrosos, etc.

• No se debe divulgar información sensible de la aplicación mediante los mensajes de error mostrados al usuario.
• Validar los datos de autenticación y cumplir con las mejores prácticas relacionadas con control de acceso lógico, adquisición, desarrollo y mantenimiento de sistemas.
• Antes de la puesta en producción, todas las características que no sean estrictamente esenciales deben ser removidas de la aplicación.
• Las conexiones a la base de datos son cerradas desde las aplicaciones tan pronto no sean requeridas.
• No se debe poder ejecutar comandos en el sistema operativo del servidor que las aloja.
• Debe prevenirse revelar la estructura de directorios de los sistemas de información de la Institución.
• Los valores para conexión a base de datos no deben estar insertados en el código sino en archivos independientes que permanecen por fuera del control de cambios, y que, de ser posible, se encuentren cifrados.
• Generar copias de respaldo, realizar pruebas y tener actualizados los procedimientos para cargue en caso de ser necesario.
• Cumplir con el Instructivo desarrollo de sistemas de información.

- **Política de Seguridad para proveedores**

El personal externo que tenga acceso a la información de la institución deberá considerar que dicha información por defecto, tiene carácter público confidencial (véase la Política de Gestión de Activos). La única información que se puede considerar como no confidencial es aquella que esté dispuesta en los canales de difusión pública. Para acceder a los sistemas de información de la Institución, se necesita un acceso adecuado, como se indica en la política de control de acceso. Se incorporará a cada tercerouna identificación segura y única para su autenticación. En el caso que, por asuntos únicamente relacionados a lo laboral, el empleado de la empresa proveedora entre en posesión de información confidencial en algún tipo de soporte, debe entenderse que esa posesión es de forma temporal, con obligación de secreto y sin que ello le confiera algún derecho de posesión, titularidad o copia sobre dicha información.
El empleado de la empresa proveedora se compromete a devolver los soportes mencionados inmediatamente después de la finalización de la tarea que dio origen al

uso temporal de los mismos, y, en cualquier caso, al cabo del término de la contratación que tenga con la Institución. Los recursos que se ponen a disposición del personal externo están disponibles exclusivamente para cumplir las obligaciones y propósito de los contratos que se firmen con ellos. Por tanto, se prohíbe:

- El uso de estos recursos para actividades no relacionadas con el objeto del servicio.
- La búsqueda o explotación de vulnerabilidades en cualquier aplicación o equipos.
- Introducir en los sistemas de información o la red interna contenidos obscenos, inmorales, amenazadores u ofensivos.
- Introducir voluntariamente cualquier tipo de malware, dispositivo lógico, físico o cualquier tipo de secuencia de instrucciones que pueda causar daño o alteración en los recursos informáticos.
- Intentar obtener accesos o permisos diferentes a los que les hayan sido asignados.
- Intentar acceder a áreas restringidas de los sistemas de información sin la respectiva autorización. Cada usuario externo, por el hecho de serlo, asume ciertas responsabilidades, como son:
  - ✓ Cumplir con la política de confidencialidad y demás políticas relacionadas con seguridad y privacidad de la información.
  - ✓ El usuario será responsable de todas las acciones registradas en los sistemas informáticos de la institución realizadas con su identificador asignado.
  - ✓ Los usuarios externos deberán acatar los controles para contraseñas que se indican en la política de control de acceso.
  - ✓ Los usuarios externos no deben revelar bajo ninguna circunstancia su identificador y/o contraseña a otra persona, ni mantenerla por escrito a la vista o alcance de terceros.
- Si un usuario tiene sospechas de que su acceso está siendo utilizado por otra persona, debe cambiar inmediatamente su contraseña y reportar el incidente al proceso de Gestión de Recursos Tecnológicos o líder de Seguridad de la Información de la Institución.

- **Política de Seguridad institucional**

La información y los documentos contenidos en los recursos informáticos, serán clasificados, trasmitidos, almacenados y custodiados de forma segura y controlada

como soporte a los procesos institucionales misionales y de apoyo. El proceso institucional de Gestión de Recursos Tecnológicos propondrá y controlará el cumplimiento de normas y políticas de seguridad informática que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de la información automatizada en general. Todos los usuarios deben autenticarse con los mecanismos de control de acceso lógico: identificador de usuario y contraseña, siendo su responsabilidad la confidencialidad de los mismos, antes de tener acceso a los recursos de infraestructura tecnológica del Colegio Mayor del Cauca. No está permitido a los usuarios proporcionar información a personal externo sobre los mecanismos de control de acceso a los recursos e infraestructura tecnológica de la institución, salvo el caso de autorización expresa de la dirección. Todo servidor o funcionario nuevo del Colegio Mayor del Cauca debe contar con la inducción sobre las políticas y estándares de seguridad informática, donde se dan a conocer las obligaciones y sanciones en que se puede incurrir en caso de incumplimiento.

- **Política de Integridad y autenticidad documental**

  El proceso de gestión documental en la institución es un proceso planeado, estructurado, administrado, documentado y revisado de manera integral a la función archivística y la administración pública. La integridad se define para la IUCMC como la propiedad del documento que indica que está completo, sin alteración con copiado autentico. La autenticidad se materializa en que puede probarse que el documento es lo que afirma ser, que ha sido creado por la persona que se afirma lo creó, en la fecha y sin modificación. Los recursos informáticos serán objeto de administración, custodia, respaldo, protección, mantenimiento preventivo y actualización permanente, implementando una visión organizacional eficaz y actualizada en la administración de la información y los documentos.

- **Política de Confiabilidad**

  Los usuarios informáticos en la IUCMC, cumplirán las normas relacionadas con la seguridad informática, contarán con permisos de acceso a los sistemas de información y cumplirán con los principios de integridad, confidencialidad y autenticidad de la información. La confiabilidad del documento radica en que su contenido es una

representación completa yprecisa de la actuación, las actividades, los desarrollos y los resultados institucionales.

- **Política para la Implementación de las tablas de retención documental digital**

  La Tabla de Retención Documental Digital como instrumento archivístico que permite la clasificación, normalización y estandarización en la producción de los documentos, es aprobada, implementada y de obligatoria aplicación y consulta para la gestión documentalen la IUCMC, institucionalizando el ciclo vital de los documentos, dando inicio al proceso de organización y automatización de documentos y archivos en soporte digital.

- **Política de Protección de la información y de los bienes informáticos**

  Los usuarios y servidores de la IUCMC, deben preservar y proteger los registros y la información procesada en la infraestructura tecnológica, de igual forma protegerán la información almacenada o transmitida ya sea dentro de la red interna institucional a otras dependencias, sedes alternas o redes externas. Todos los archivos de computadores que sean proporcionados por personal externo o interno (programas, software, bases de datos, documentos y hojas de cálculo) que tengan que ser descomprimidos, los usuarios deben verificar que estén libres de virus, utilizando el software antivirus autorizado en la institución antes de ejecutarse. Todo incidente u ocurrencia de accidente de seguridad informática debe ser reportado oficialmente a la oficina de TIC. Queda prohibido falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

- **Política de Control de virus y software malicioso**

  Para prevenir infecciones de virus informático, los usuarios de la IUCMC, no deben hacer uso de software que no haya sido proporcionado y validado por la oficina de Gestión de Recursos Tecnológicos. En el caso de sospecha de infección de virus, debe dejar de usar inmediatamente el equipo y notificar la sospecha a la oficina de Gestión de Recursos Tecnológicos. Se efectuarán controles para la generación y restauración de copias de respaldo o back-up como salvaguarda de información crítica de los procesos institucionales significativos, la realización de copias de respaldo o seguridad se harán

periódicamente en los equipos administrativos y servidores. Las copias de seguridad deben rotularse para ser almacenadas, se utilizará el software OwnCloud en la opción de back-up. Opción datos: la rotulación contenida, fecha de copia, asunto, código según TRD digital y se entregará a la oficina de Gestión de Recursos Tecnológicos para almacenamiento y custodia. Cuando un funcionario no autorizado o visitante requiera entrar a las salas donde se encuentran los servidores, debe solicitar autorización mediante comunicación interna a la oficina de Gestión de Recursos Tecnológicos. Cuando se va a realizar mantenimiento en alguno de los equipos, se debe dar aviso con anticipación al usuario informático o servidor público.

- Política de Control de acceso físico

Se deberá reportar y registrar al momento de la entrada, en el área de recepción, los equipos de cómputo, de comunicaciones, medio de almacenamiento y herramientas que no sean propiedad de la institución.

- Política de protección de equipos

Los usuarios de la IUCMC, no deben mover o reinstalar, reubicar los equipos, ni retirar sellos de los mismos sin autorización. Es responsabilidad de los usuarios almacenar su información únicamente en la partición del disco duro diferente, destinada para archivos de programas y sistemas operativos /c: / Es prohibido que el usuario o funcionario distinto al personal autorizado abra o destape los equipos, asimismo cuando se requiera realizar cambios de ubicación en lugares físicos de trabajo o locativos, debe ser notificado con 3 días de anticipación a la oficina de Gestión de Recursos Tecnológicos.

El préstamo de portátiles o laptops tendrá que solicitarse en la oficina de Gestión de Recursos Tecnológicos.

Todos los usuarios de los sistemas de información, serán registrados en la base de datos para la autorización de uso de dispositivos de almacenamiento externo (memorias USB, discos portátiles, unidades CD, DVD, así mismo para el manejo y traslado de información o realización de Backups. Todo el personal o usuario informático nuevo de la institución deberá ser notificado a la oficina de Gestión de Recursos Tecnológicos para asignarle derechos correspondientes, equipo, creación de usuario para la red y anulación en caso

de retiro. Controles de acceso lógico: Administración y uso de contraseñas /usuarios/ equipos/Controles para otorgar, modificar y retirar usuarios: Creación cuentas de usuario, solicitud creación cuentas de usuario, seguimiento a Backups, protección y ubicación de equipos, pérdida de equipos, uso de dispositivos extraíbles e Internet.

- **Política de Administración de la red**

  Los usuarios informáticos de la IUCMC, no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de archivos (ftp) u otro tipo de protocolo para transferencia de información, empleando la infraestructura de la red de la institución sin autorización de la oficina de Gestión de Recursos Tecnológicos.

- **Política de Seguridad de la red**

  Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada, en la cual los usuarios o funcionarios realicen exploración de los recursos informáticos en la red de la IUCMC, así como de las aplicaciones que sobre dicha red operan, con fines a detectar y explotar una posible vulnerabilidad.

- **Política de Adquisición de software**

  Los usuarios o funcionarios que requieran instalación de software deben justificar su uso, indicando el equipo donde se instalará y el período de tiempo que será usado. Se considera una falta grave que los usuarios instalen cualquier tipo de programa en sus computadores, servidores, estación de trabajo u otros equipos conectados a la red del colegio Mayor del Cauca que no esté autorizado por la oficina de Gestión de Recursos Tecnológicos. Se debe mantener por parte de la oficina de Gestión de Recursos Tecnológicos el inventario actualizado de equipos, programas y licencias instaladas.

- **Política de Licenciamiento de software**

  Se prohíbe en la IUCMC, instalar software y programas no autorizados y sin licenciamiento en la red de la IUCMC.

- **Política de Uso del correo electrónico y/o Sistemas de Información**

Los usuarios informáticos del Colegio Mayor del Cauca, deben tratar los mensajes y los archivos adjuntos como información de propiedad de la institución. No se deben utilizar cuentas de correo electrónico asignadas a otros usuarios, ni recibir mensajes en cuentas de otros, si fuera necesario leer el correo de alguien más (mientras se encuentra por fuera o de vacaciones) el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externo al Colegio Mayor del Cauca, a menos que cuente con una autorización de la oficina de Gestión de Recursos Tecnológicos. Los usuarios informáticos de la Institución Universitaria Colegio Mayor del Cauca, podrán enviar información reservada o confidencial vía correo electrónico siempre y cuando vaya de manera encriptada y destinada exclusivamente a personas autorizadas y en ejercicio de funciones y responsabilidades institucionales.

Se prohíbe el envío de documentos que contengan firmas escaneadas o digitalizadas a través del correo electrónico institucional y/o sistemas de información. Esta medida tiene como objetivo proteger la autenticidad, integridad y validez de los documentos y evitar posibles fraudes o malentendidos en las comunicaciones oficiales de la institución.

Los documentos que requieran ser firmados deben ser procesados siguiendo procedimientos oficiales y no deben ser enviados ni recibidos por correo electrónico en formato electrónico con firmas digitalizadas, salvo en los casos siguientes:

- **Autorización explícita:** Cuando se haya recibido una autorización previa por parte del área legal o de cumplimiento normativo de la institución para el envío de documentos con firmas digitalizadas o escaneados.
- **Requisitos legales o contractuales:** Cuando el uso de firmas digitalizadas sea requerido por ley o un acuerdo contractual específico, y dicho envío haya sido aprobado previamente por la persona o área correspondiente.

- **Política de Autenticidad de la información**

Se cumplirán en la institución los procedimientos de archivo y gestión documental en la administración de los procesos. Se divulgarán solo documentos controlados, versionados, en formato estable y firmado digital. Se establecerán los roles y responsabilidades en la gestión documental, quiénes firman los documentos, quiénes están autorizados para modificar, suprimir o adicionar información institucional.

- **Política de Tratamiento y protección de datos personales**

Garantizar el adecuado Tratamiento de los datos personales que se recolecten, almacenen, clasifiquen, usen, publiquen, circulen y suprimen en el ejercicio de las funciones misionales del Colegio Mayor del Cauca, dando así cumplimiento a lo contemplado en la Constitución Política de Colombia, Ley 1581 de 2012, Decreto 1377 de 2013 y 886 de 2014, y las demás normatividades aplicables.

La Política de Tratamiento y Protección de Datos Personales, se implementará a todas las Bases de Datos y/o archivos que contengan datos personales y que sean objeto de tratamiento el Colegio Mayor del Cauca, quien para efectos del cumplimiento de la presente política.

TRATAMIENTO Y FINALIDAD. El tratamiento que realizará el Colegio Mayor del Cauca con la información personal será la siguiente:

- ✓ Recolectar, almacenar, usar, circular o suprimir información de aspirante, estudiante (activo e inactivo), egresado, familiar o tutor de estudiante, docente, funcionario, exfuncionario, contratista con funciones administrativas, familiar de trabajador, practicante, aspirante a proveedor, proveedor, periodista, investigador, asistente a evento, usuario de servicios, monitor académico, visitante, usuarios externo y todos aquellos inmersos en la prestación del servicio público de educación superior.
- ✓ Alimentar las bases de datos institucionales por medio de sus correspondientes sistemas de información.
- ✓ Caracterizar usuarios y grupos de interés. - Recepción, seguimiento y respuesta a las peticiones, quejas, reclamos, felicitaciones o denuncias presentados a la Institución. Conocer y consultar la información del Titular
- ✓ Establecer contacto con los aspirantes a programas académicos para el proceso de admisión. - Llevar a cabo el proceso de admisión y publicación de listas de admitidos. Recolectar datos personales en campañas de comunicación y mercadeo para la promoción de los programas tecnológicos, profesionales, de postgrado y extensión.
- ✓ Entregar información de datos personales a entes de control, según lineamientos gubernamentales y/o entes de control.

- ✓ Realizar contacto telefónico o por medio de canales electrónicos con estudiantes para promoción, seguimiento e información en general sobre actividades académicas.
- ✓ Realizar el proceso de matrícula financiera y académica de los estudiantes admitidos, activos y reingresos.
- ✓ Registrar y analizar solicitudes de trasferencias u homologaciones académicas internasy externas.
- ✓ Administrar el Sistema de Información Académico y de Gestión (SIAG), para la actualización de datos personales, creación y/o actualización de usuarios, parametrización del sistema y generación de reportes.
- ✓ Realizar la captura y divulgación en la página web institucional y redes sociales, de archivos digitales (fotos y vídeos), en los diferentes eventos y actividades realizadas por la Institución.
- ✓Llevar a cabo procesos de contratación y convenios (evaluación, selección y seguimiento).
- ✓ Realizar préstamo de medios educativos (ayudas audiovisuales, espacios físicos, material bibliográfico).
- ✓ Registrar y controlar académicamente los procesos académicos (pagos, registro y publicación de notas, adiciones y cancelaciones a matrícula académica, entre otros), de los programas regulares y el programa de educación para el trabajo y desarrollo humano del programa inglés.
- ✓ Promocionar y dar uso a los servicios de bienestar universitario en las siguientes áreas: físico-deportiva, artística, lúdica, psico-afectiva, médica y social de la Institución.
- ✓ Planear y ejecutar actividades protocolarias para eventos, conferencias, grados, diplomados, seminarios, cursos, entre otros.
- ✓ Realizar el seguimiento a egresados del programa de educación para el trabajo y desarrollo humano del programa inglés, programas tecnológicos, profesionales y de postgrado. Además del ofrecimiento de los programas académicos y educación continuada.
- ✓ Planear y desarrollar proyectos y programas de los subprocesos proyección social, internacionalización y egresados. - Inscribir, seleccionar y otorgar auxilios

educativos a estudiantes de la Institución, previo cumplimiento a requisitos.

- ✓ Diligenciar encuestas de satisfacción del cliente.
- ✓ Almacenar la información contable durante los tiempos establecidos por la normatividad colombiana vigente.
- ✓ Funciones investigativas (semilleros, etc.)
- ✓ Respaldar y resguardar la información laboral y pensional de los ex-funcionarios de la Institución, con el fin de dar cumplimiento a los requerimientos normativos de las entidades competentes. - Planear y ejecutar actividades del subproceso de internacionalización, para el tema de convocatorias de movilidad académica, gestión de convenios (municipales, nacionales e internacionales) y relacionamiento externo.
- ✓ Realizar transferencia internacional de datos personales a instituciones educativas internacionalespara gestión de movilidad académica saliente y entrante.
- ✓ Planear y ejecutar el proceso de titulación de la Institución Universitaria Colegio Mayor del Cauca (verificación de requisitos, elaboración de actas de grado y ceremonia).
- ✓ Controlar el acceso y salida del personal administrativo por medio de la identificación biométrica.
- ✓ Entregar reportes estadísticos a entes gubernamentales
- ✓ Gestionar cuentas de correo institucional
- ✓ Respaldar y resguardar la información académica de los egresados de la Institución, con el fin de dar cumplimiento a los requerimientos normativos de las entidades competentes.
- ✓ Realizar el Registro Nacional de Bases de Datos para dar cumplimiento a los requerimientos de la Superintendencia de Industria y Comercio.
- ✓ Recepcionar y tramitar permisos, licencias e incapacidades laborales

TRATAMIENTO DE DATOS PERSONALES DE NIÑOS, NIÑAS Y ADOLESCENTES.

El Colegio Mayor del Cauca, quien obra en calidad de Responsable del Tratamiento de datos personales de niños, niñas y adolescentes, se acoge a la normatividad colombiana citada en la presente Política y los demás lineamientos que se citan a continuación: El Artículo No. 3 del Código de la Infancia y de la adolescencia

- ✓ Sujetos titulares de derechos: clasifica por rangos de edades la pertenencia a las etapas de niñez y adolescencia, entre los 0 y los 12 se entiende que se es niño o niña, mientrasque entre los 12 y 18 años de edad se es adolescente.
  El Artículo No. 8 del Código de la Infancia y de la adolescencia
- ✓ Interés superior de los niños, niñas y adolescentes: menciona la obligación de todas las personas a garantizar a los niños, niñas y adolescentes la satisfacción integral y simultánea de todos los derechos humanos, que son universales, prevalentes e interdependientes. En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

a) Queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública (ibídem).

b) Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás. El Gobierno Nacional reglamentará la materia, dentro de los seis (6) meses siguientes a la promulgación de Ley 1581 de 2012 (ibídem).

Según los lineamientos normativos establecidos para el tratamiento de datos personales de niños, niñas y adolescentes el Colegio Mayor del Cauca solicita la autorización (oral o escrita), del adulto responsable y/o su representante legal, no obstante, el menor conserva su derecho a ser escuchado y su opinión será valorada teniendo en cuenta el nivel de comprensión y la capacidad de entendimiento sobre el asunto a tratar.

- **Políticas de Uso de salas de sistemas y laboratorios**

Se hace necesario establecer las políticas que garanticen el uso adecuado de las salas de sistemas y laboratorios de la Unimayor por parte de la comunidad académica, para lo cual se recomienda definir las normas que reglamenten los derechos y deberes de los usuarios, la prestación del servicio, reservas, prohibiciones, sanciones, mantenimiento, funciones encargado de la sala y socialización.

Se debe adoptar las políticas para el manejo y utilización de las salas de sistemas y laboratorios, como apoyo al proceso de enseñanza-aprendizaje, según se describe a continuación:

DEFINICIÓN:

Se considera como Sala de Sistemas aquellos espacios físicos, adecuadas y dotados con hardware, software (licenciado), redes de datos y eléctricas con que cuenta la institución como apoyo a los procesos de enseñanza - aprendizaje, disponibles al servicio de la comunidad académica y administrativa.

USUARIOS:

La Institución Universitaria Colegio Mayor del Cauca define como usuarios delas salas de sistemas y laboratorios a:

- ✓ Estudiantes de programas tecnológicos.
- ✓ Estudiantes de programas profesionales.
- ✓ Estudiantes de postgrados.
- ✓ Estudiantes del Programa de Educación para el Trabajo y el Desarrollo Humano delidioma inglés.
- ✓ Estudiantes de Educación Continua Egresados. Personal Administrativo. PersonalDocente. Contratista.
- ✓ Personal Externo enmarcado en convenios interinstitucionales

PRESTACIÓN DEL SERVICIO:

Las salas de sistemas y laboratorios de Unimayor estarándisponibles para el servicio de los usuarios, previa reserva de los espacios.

- Cuando no se encuentren en uso de las clases, estarán disponibles a los usuarios para el desarrollo de sus actividades individuales, respetando los horarios y normas establecidas para el uso de éstas. Para la prestación del servicio se deben tener en cuenta los siguientescasos:

  - Para el desarrollo de las actividades académicas individuales en horarios diferentes a los establecidos se debe presentar el carné vigente que lo acredita.
  - Como usuario de la institución debe realizar la solicitud de ingreso a la sala ante

el responsable de la sala o laboratorio.

- Si la sala se encuentra reservada y no está siendo utilizada, se permitirá a los usuarios el ingreso, previa solicitud ante el responsable de la sala.
- El docente que tiene asignada la sala para el desarrollo de su clase, cuenta con la potestad de autorizar, restringir o denegar el ingreso de usuarios ajenos a su componente de módulo.

DERECHOS Y DEBERES DE USUARIOS:

Los usuarios de las salas de sistemas y laboratoriostienen derecho a:

a. Recibir el soporte técnico por el personal del subproceso de Gestión de Recursos Tecnológicos.

b. Recibir un trato respetuoso y cortés por parte de los funcionarios encargados de lassalas de sistemas y laboratorios.

c. Contar con las condiciones adecuadas que le permita el desarrollo pleno de sus actividades.

d. Hacer uso de las salas de sistemas y laboratorios para el desarrollo de sus actividadesacadémicas.

e. Conocer la programación del uso de salas de sistemas y laboratorios.

Los usuarios de salas de sistemas y laboratorios deben cumplir los siguientes deberes:

a. Conocer y dar cumplimiento a la política de uso de las salas de sistemas y laboratorios.

b. Realizar la solicitud correspondiente ante el área o funcionario encargado de las salas, cuando requieran utilizar el (los) equipo(s) o dispositivo(s) con que cuentan las salas de sistemas y laboratorios.

c. Manejar un trato respetuoso y cordial con los demás usuarios y encargados de las salas de sistemas y laboratorios.

d. Presentar el carné vigente que lo acredite como usuario de la institución.

e. Cuidar los recursos software y hardware que se encuentran disponibles en las salas de sistemas y laboratorios.

f. Cuidar de los recursos como mesas, sillas, porta teclados, tableros, cámaras y equipos de respaldo (UPS), que hacen parte de la infraestructura de las salas de sistemas y laboratorios.

g. El usuario debe entregar el carné como garantía del préstamo cuando requiera haceruso de los equipos y dispositivos de las salas, una vez terminadas sus actividades debe hacer entrega al encargado (garantizando el perfecto funcionamiento de éstos) y reclamar su carné.

h. El uso de las salas de sistemas y laboratorios es para fines académicos.

i. En caso de presentarse un problema se debe reportar inmediatamente al responsable de la sala de sistemas y laboratorios.

j. Guardar silencio en las salas de sistemas y laboratorios, se recomienda mantener la configuración del celular en modo silencio, para no incomodar a los demás usuarios que seencuentren en ella.

RESERVAS:

Las reservas de las salas de sistemas y laboratorios de la UNIMAYOR, para el desarrollo de las clases durante el semestre son asignadas por los secretarios académicos de las facultades y la coordinación del programa de inglés, a través de la aplicación web Meeting Room Booking System (MRBS).

Una vez realizada la respectiva reserva estará disponible para su consulta a través de la página web de la institución. Para la cancelación de una reserva de las salas de sistemas, sedeberá enviar un correo informativo con anticipación, a la cuenta de correo según corresponda, con el fin de eliminarla del cronograma y disponer del espacio.

PROHIBICIONES:

A continuación, se mencionan las acciones que se prohíben a los usuariosque accedan al uso de los servicios de las salas de sistemas y laboratorios:

a) Permitir el ingreso de personal ajeno a UNIMAYOR a las salas de sistemas y laboratorios,sin previa autorización de la autoridad competente.
b) Consumir alimentos y/o bebidas dentro de las salas sistemas y laboratorios.
c) Consumir sustancias psicoactivas o fumar dentro de las salas de sistemas y laboratorios.
d) El plagio de software, descarga, instalación y uso de aplicaciones, programas, bases de datos, códigos o archivos multimedia que infrinjan la ley de derechos de autor.

e) Usar los equipos de cómputo y los servicios de la red, para fines de ocio, como juegos, envío y recepción de material pornográfico, uso de redes sociales.
f) Usar los equipos para consultar o intercambiar material ofensivo, difamatorio o cualquier información que vulnere la dignidad de las personas.
g) Eliminar, modificar o alterar el software que se encuentre instalado en los equipos de cómputo.
h) Modificar la configuración de los equipos respecto a la imagen institucional y cuentas de usuario.
i) Tomar prestados algunos elementos, como teclados, ratones, tabletas, audífonos, entre otros, sin previa autorización del responsable de la sala de sistemas o laboratorio.
j) Mover, destapar, desconectar o alterar el orden de los equipos con que cuentan las salas de sistemas y laboratorios.

SANCIONES:

El Colegio Mayor del Cauca estipula que si se presentan daños parciales o totales, pérdida o robo de los equipos de cómputo, recursos tecnológicos, inmobiliarios y medios audiovisuales con los que cuentan las salas de sistemas y laboratorios de la institución se procederá a la aplicación de las sanciones pertinentes según lo establecido en la reglamentación institucional vigente.

MANTENIMIENTO:

A los equipos de las salas y laboratorios de sistemas se deberá realizar mantenimiento preventivo/correctivo según el cronograma definido por el subproceso.

ACTIVIDADES DEL RESPONSABLE DE LA SALAS DE SISTEMAS Y LABORATORIOS:

- Llevar un registro detallado de los recursos tecnológicos (controles de Video Beam, parlantes, Tabletas Digitales, Cables HDMI y VGA) que se utilizan frecuentemente para el desarrollo de las actividades académicas en las salas y laboratorios de sistemas.
- Preparar los equipos y verificar el buen funcionamiento de los mismos para el desarrollo de las prácticas o investigaciones por parte de los usuarios.
- Asesorar a los usuarios en el uso adecuado de los computadores y los recursos de los

que dispone la sala de sistemas y laboratorios.

- Velar por el buen uso del hardware y software de las salas de sistemas y laboratorios.

- Supervisar que los equipos queden bien apagados y las sillas organizadas al terminar su turno de trabajo.

- Verificar permanentemente el estado del antivirus de los equipos de cómputo de las salas y laboratorios con el objetivo de garantizar que se encuentren actualizados, previniendo que se infecten de software malicioso o virus.

- Verificar el diligenciamiento del formato disponible para el de uso y préstamo de salas desistemas y laboratorios los cuales permiten generar las estadísticas del uso de las mismas.

- **Política de Seguridad de la Información**

El Colegio Mayor del Cauca, entiende y conoce la existencia de riesgos en seguridad y privacidad de la información que pueden afectar el desarrollo de la misión institucional. Por ello, se compromete a realizar las tareas necesarias para mantener la confidencialidad, integridad y disponibilidad de los activos de la información, mediante una gestión de riesgos, asignación de responsabilidades en seguridad y la participación activa de las partes interesadas, cumpliendo con la normatividad vigente y para lograr la mejora continua.

Los objetivos de Seguridad y privacidad de la Información son:

- Proteger los activos de la información en términos de su confidencialidad, integridad y disponibilidad que permiten la prestación de los servicios del Colegio Mayor del Cauca.

- Atender y solucionar los incidentes de seguridad y privacidad de la información reportada en la Institución Universitaria.

- Sensibilizar al personal de la Institución en seguridad y privacidad de la información, buscando el compromiso en el cumplimiento de políticas de seguridad de la información, reporte de incidentes de seguridad a través de los canales autorizados y participación periódica en la gestión de riesgos.

Esta política será revisada periódicamente por el Líder de Seguridad de la Información y la Alta Dirección, igualmente cuando se identifiquen cambios en los procesos y/o tecnología o se presente alguna condición que afecte la seguridad de la información de

la institución, esto como parte de lograr la mejora continua. En caso de realizarse cambios, la política será comunicada a las partes interesadas a través de los canales aprobados por la Alta Dirección de la institución.

- **Política 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 físicoy digital. Se debe realizar el registro en el documento Activos de información, respetandola clasificación de la norma ISO 27001 además del responsable del activo y proceso al cual pertenece.

- **Política Copias de respaldo**

Todo activo de información que sea de interés para los procesos y/o subprocesos identificados en el Sistema de Aseguramiento interno de la calidad del Colegio Mayor del Cauca, deberá ser respaldada con copias de seguridad, enla periodicidad que establezca el proceso Gestión de Recursos Tecnológicos junto con el dueño del proceso y de conformidad con las siguientes responsabilidades:

RESPONSABILIDADES de los usuarios:

- ✓ Conservar una copia de seguridad de todos sus archivos, en la partición de disco duro diferente a la utilizada por el sistema operativo.
- ✓ Mantener siempre en su computadora activo y actualizado el sistema OwnCloud.
- ✓ No realizar copias de seguridad de datos personales dentro del aplicativo (fotos, música,videos, ejecutables de programas, instaladores, etc.), la información de los archivos debe ser única y exclusivamente de uso institucional.
- ✓ La periodicidad de los backups por parte de los usuarios debe ser diaria.
- ✓ La identificación y ubicación de la información deberá ser acorde a la establecida en las TRD- Tablas de Retención Documental aprobadas y generadas por el proceso de Gestión Documental.
- ✓ Realizar el reporte inmediato ante cualquier anomalía en el aplicativo, al proceso Gestión de Recursos Tecnológicos.
- ✓ En modalidad de teletrabajo o trabajo en casa: Realizar sincronización automáticamente en Google Drive de una carpeta denominada UNIMAYOR. 5.2. Del subproceso de Gestión de Recursos Tecnológicos.
- ✓ Suministrar a los usuarios las herramientas o recursos y capacitación necesarias para realizar las copias de seguridad.
- ✓ Realizar la instalación y configuración del Software en cada uno de los computadores de la institución.

- ✓ Mantener el software en correcto funcionamiento.
- ✓ Realizar y llevar registro de la revisión semestral de las copias de seguridad.
- ✓ Realizar visitas de verificación de buen uso del software y cumplimiento de la presentepolítica.
- ✓ Mantener actualizados los usuarios; existen 85 usuarios creados en OwnCloud, con una capacidad de 1GB, 3 GB, 5 GB, 10 GB y 18 GB para cada usuario (La capacidad varía por usuario).
- ✓ El director del proceso o su delegado deberá gestionar las medidas de protección lógica y física adecuadas.

Soporte de sincronización automática Google Drive en modalidad teletrabajo o trabajo en casa. 5.3. Administrador (Responsable) de las Bases de Datos:

- ✓ Realizar diariamente copia de seguridad de la(s) base(s) de datos, asociada(s) a los sistemas de información institucional.
- ✓ Realizar pruebas de restauración de los Backups con la periodicidad establecida dentro de su plan de mantenimiento, de manera aleatoria para garantizar que sean leídas y restauradas correctamente, deben dejar registro de los resultados obtenidos.
- ✓ Almacenar por lo menos en dos sitios físicos/virtuales diferentes las copias de seguridad de las bases de datos relevantes, con el fin de garantizar la continuidad de los procesos críticos.

- **Manual Políticas contables**

Ver documento 1.0.D.10

CONTROL DE CAMBIOS

FECHA DE CAMBIO	CAMBIOS REALIZADOS
31/01/2020	Inclusión de la Política de Gestión Estadística como nueva Política de MIPG.

	Aprobadas mediante Resolución No. 228 del 31 de enero de 2020.
29/01/2021	Incluyen y actualizan políticas del sistema de seguridad de la información y Gestión documental/ se incluye dentro del documento políticas de MIPG el manual de políticas contables. **Aprobadas mediante Resolución No. 105 de 2021.**
26/01/2022	Se revisan actualizan políticas del Modelo integrado de planeación y gestión/ se adicionan políticas del sistema de seguridad de la información y Gestión documental. **Aprobadas mediante Resolución No. 001 de 2022.**
26/01/2023	Se actualizan y aprueban política de MIPG. **Aprobadas mediante Resolución No. 001 de 2023**
09/02/2024	Se actualiza el documento de acuerdo a TRD aprobadas por el Consejo Departamental de Archivos.
13-08-2024	Actualización denominación Política Uso de correo electrónico y/o sistemas de información.
03-02-2025	Se incluye logo institucional en el encabezado de la política