POLÍTICA DE USO DE CORREO ELECTRÓNICO

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

1. OBJETIVO GENERAL

Establecer las políticas y normas para asegurar el uso apropiado y eficaz del correo electrónico institucional para garantizar la confidencialidad, autenticidad y/o integridad de la información dentro de la Institución Universitaria Colegio Mayor del Cauca.

2. ALCANCE

Este documento aplica para todos los funcionarios, contratistas, docentes, estudiantes, egresados 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.

-**Correo electrónico:** Servicio de comunicación que permite a los usuarios enviar y recibir mensajes mediante canales de red de carácter electrónico.

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

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

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

4. MARCO NORMATIVO

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

- Ley 603:2000 Control de legalidad del Software
- Ley 734:2002 por la cual se expide el Código Disciplinario Único.
- Ley 1266:2008 Por la cual se dictan las disposiciones del Habeas Data y regulaciones del manejo de la información.
- CONPES 3701:2011 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

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. Responsabilidades del Usuario.

Dentro de la institución, los usuarios que cuenten con un correo institucional deberán cumplir con las siguientes responsabilidades:

- El usuario es responsable de las actividades que sean realizadas con la cuenta de correo asignada para él.
- La cuenta de correo institucional es creada para uso exclusivo de las funciones del usuario, por tanto, el usuario a quien se le asigna la cuenta de correo institucional debe velar por cumplir con la integridad, respeto, responsabilidad y seguridad de la información que se opere.

- Las cuentas de correo institucional son de carácter personal e intransferibles. La responsabilidad del usuario radica en el cuidado de su contraseña de acceso y su cambio periódico, esta cuenta no debe ser prestada a terceros.
- En caso de necesitar una cuenta compartida por uno o más usuarios, este requerimiento debe ser presentado al área TIC con el respectivo consentimiento de los usuarios que van a hacer uso de la cuenta institucional. El consentimiento o autorización no exime de responsabilidades por ser una cuenta compartida, es decir, las personas que hagan uso de la cuenta son responsables en simultáneo de las acciones realizadas por dicha cuenta.
- Se recomienda a los usuarios a omitir re-direccionamientos que provengan de remitentes desconocidos. En caso de sospechar de algún correo electrónico con contenido dudoso comunicarse con el área TIC para su evaluación.
- El uso de las cuentas institucionales es de carácter exclusivamente laboral o académico, la información almacenada en las cuentas institucionales es propiedad de la Institución Universitaria Colegio Mayor del Cauca. La IUCMC no se hará responsable de información personal que haya sido alojada en las cuentas institucionales.
- El usuario deberá asumir la responsabilidad de reportar a tiempo incidentes de seguridad ante el área TIC que no pueda solventar, como pueden ser accesos no autorizados, pérdida de contraseña, etc.
- Los mensajes de correo electrónico cuentan con la misma fuerza probatoria que los documentos físicos según la ley 527 de 1999.
- El usuario es responsable de realizar copias de seguridad o de solicitar dichas copias de seguridad al área TIC.
- Los correos que son dirigidos al apartado *SPAM* del buzón, deben ser omitidos. En caso de considerar que un correo no fue etiquetado correctamente en esa categoría, el usuario asumirá la responsabilidad de la evaluación de esa etiqueta de *SPAM*, a su vez, puede solicitar la evaluación del correo al área TIC.
- El usuario deberá validar antes de re-enviar o enviar un mensaje si es necesario incluir todos los datos, como destinatarios, historial o la información del mismo.
- Se debe evitar el envío de correos innecesarios que no tengan relación con las funciones asignadas que desempeña el usuario.
- Se debe tener especial cuidado con los mensajes que alberguen información *confidencial, secreta,* o *restringida*. El usuario asume desde su cuenta asignada el tratamiento de la información enviada o recibida.

6.2. Restricciones en uso de correo institucional.

Los usuarios deberán tener en cuenta:

- Se prohíbe el uso de correos personales con el fin de transferir o divulgar información institucional, puesto que la herramienta asignada para el desempeño de estas labores es la cuenta institucional.
- Se prohíbe copiar o renviar mensajes que cuenten con información de carácter *confidencial, secreta* o *restringida* sin tener la autorización para hacerlo.
- Se prohíbe la propagación de correos desconocidos, correo basura o no deseado, spam hacia otras cuentas institucionales.
- Está prohibido la divulgación o transferencia de información institucional a terceros.
- Se prohíben los correos con mensajes que atenten con las normas legales, orden público, moral, buen nombre o intimidad de las personas, que contengan contenido irrespetuoso, intimidación, acoso, discriminación, contenido difamatorio, racista, religioso-irrespetuoso, así mismo, mensajes que contengan videos, imágenes de carácter ilegal, ofensivo, material sexual, indecente o extorsivo.
- No se permite compartir listas de distribución con terceros, a excepción de una autorización justificada.

6.3. Envío de comunicaciones y correos masivos.

Los envíos masivos o de comunicaciones de cualquier índole son realizados por el área de comunicaciones exclusivamente. En caso de necesitar divulgar cualquier tipo de información se deberá presentar una solicitud donde será evaluada y se determinará si esta solicitud cumple con lo necesario para ser enviada masivamente, de ser así, el área de comunicaciones se encargará de hacerlo.

7. DISPOSICIONES FINALES

7.1. DIFUSIÓN

El personal autorizado por el subproceso Gestión de Recursos Tecnológicos realizará la socialización y/o difusión de esta política a la comunidad universitaria y grupos de interés, de acuerdo a las directrices del documento 104.01.02.D.13 plan de sensibilización de seguridad de la información.

7.2. ACTUALIZACIÓN

Para garantizar la vigencia, mejora continua y actualización de esta política, deberá ser revisada por lo menos una vez al año por personal competente y autorizado del subproceso Gestión de Recursos Tecnológicos y será el comité integral de planeación y gestión quien apruebe las mejoras a implementar.

Durante la actualización se deberá tener en cuenta la normatividad vigente, lineamientos institucionales y resultado de auditorías de seguridad y privacidad de la información.

7.3. SANCIONES

El incumplimiento de esta política se aplicará la normativa vigente en la Institución Universitaria Colegio Mayor del Cauca, además de las normas emitidas a nivel Nacional y Regional a través del proceso Gestión y Desarrollo del talento humano.

7.4. 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.