

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Hombres nuevos para tiempos nuevos



**ACUERDO NUMERO 025 DE 2025
(AGOSTO 22)**

Por el cual se expide la Política de Seguridad de la Información de la Universidad CESMAG

**EL CONSEJO DIRECTIVO DE LA UNIVERSIDAD CESMAG
en uso de sus facultades, y**

CONSIDERANDO:

Que el Estatuto General de la Universidad, aprobado mediante Acuerdo 016 de 28 de septiembre del 2020, dentro de las funciones asignadas al Rector, en el literal b. del artículo 25 señala: "proponer al Consejo Directivo las políticas institucionales de la Universidad CESMAG de acuerdo con la legislación vigente, el Estatuto General y los reglamentos, y fijar las políticas específicas".

Que según el literal b del artículo 20 del Estatuto General de la Universidad, es función del Consejo Directivo "aprobar, a propuesta del Rector y orientación del Consejo Máximo, las políticas de la Universidad CESMAG, en coherencia con su modelo de gestión y arquitectura institucional, de acuerdo con la legislación vigente, el Estatuto General, los reglamentos, y velar por su implementación y cumplimiento".

Que, en coherencia con la Misión, Visión y los principios institucionales, y en articulación con el Plan Estratégico de Desarrollo (PED) 2022–2029, la Universidad CESMAG asume la seguridad de la información como un compromiso estratégico fundamental. Esta decisión se alinea directamente con el Objetivo Estratégico 3, orientado a la implementación de los Lineamientos para el desarrollo de una arquitectura institucional basada en el buen gobierno y los principios éticos (LE011), así como en la toma de decisiones sustentadas en información confiable (LE013)

Que la Política de Seguridad de la Información de la Universidad CESMAG establece las directrices fundamentales para la protección de sus activos informáticos, asegurando la confidencialidad, integridad y disponibilidad de la información gestionada en el marco de sus procesos académicos, administrativos y misionales.

Que dicha política promueve la adopción de estándares nacionales e internacionales en materia de seguridad y ciberseguridad, así como una gestión proactiva de riesgos, incidentes y eventos relacionados; y adicionalmente, impulsa una cultura organizacional orientada a la responsabilidad, el uso ético y adecuado de la información, y el compromiso con la mejora continua.

Que la Universidad CESMAG reconoce la importancia estratégica de la seguridad de la información como un componente esencial para la protección de sus procesos académicos, investigativos, de proyección y administrativos; y en consecuencia, promueve la consolidación de entornos digitales confiables, resilientes y alineados con los principios institucionales, contribuyendo al fortalecimiento de la gobernanza tecnológica y al cumplimiento de sus objetivos misionales.

Que el Decreto Rectoral 003 del 3 de mayo de 2023, creo el Comité de Tecnologías de la Información CoTI de la Universidad CESMAG, encargado de *identificar y recomendar la formulación, seguimiento y cumplimiento de los procesos, proyectos y políticas sobre el tema.*





Que una de las funciones del Comité CoTI es la de *"asesorar los procesos, procedimientos, proyectos y políticas que permitan el manejo consistente e integral de la gestión de la información y su ciclo (recopilación, procesamiento, almacenamiento, uso y disposición) además de su seguridad para el funcionamiento pertinente de los procesos administrativos y académicos, que faciliten la toma de decisiones en el nivel directivo y estratégico de la Universidad"*.

Que, en la sesión celebrada el 6 de agosto de 2025, el Comité de CoTI aprobó la presentación ante el Honorable Consejo Directivo de la Política de Seguridad de la Información y del Manual de Gestión de Incidentes o Eventos, con el fin de que sean analizados, revisados y aprobados.

Que el Consejo Directivo, mediante Acuerdo 014 del 26 de agosto de 2022, reguló el proceso de formulación, implementación, competencia de aprobación, responsabilidades y clasificación de las políticas en la Universidad CESMAG.

Que el Rector de la Universidad CESMAG presenta a consideración del Consejo Directivo, la Política de Seguridad de la Información, para su implementación.

En mérito de lo expuesto,

ACUERDA:

ARTÍCULO 1. Aprobar la Política de Seguridad de la Información de la Universidad CESMAG y del Manual de Gestión de Incidentes o Eventos, anexos al presente acuerdo.

ARTÍCULO 2. El Consejo Directivo será el intérprete del presente Acuerdo y resolverá las ambigüedades y conflictos que se puedan presentar para su aplicación.

ARTÍCULO 3. El presente Acuerdo se divulgará en los términos de lo establecido en el Acuerdo 038 del 26 de noviembre de 2021 del Consejo Directivo.

ARTÍCULO 4. La Política de Seguridad de la Información, debe ser revisada periódicamente y, de requerirse debe actualizarse de acuerdo con los cambios que susciten.

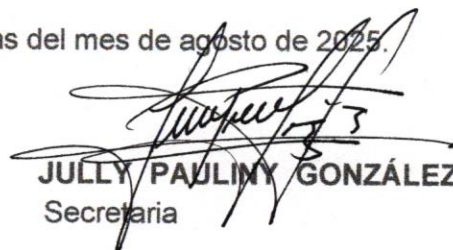
ARTÍCULO 5. Es responsabilidad de todos los integrantes de la Institución, de acuerdo con sus competencias, velar por el cumplimiento de la Política de Seguridad de la Información de la Universidad CESMAG y su desconocimiento no puede invocarse como causal de justificación de su incumplimiento.

ARTÍCULO 6. El presente Acuerdo rige a partir de las fechas su expedición y deja sin efecto cualquier disposición que le sea contraria.

COMUNÍQUESE Y CÚMPLASE

Dado en San Juan de Pasto, a los veintidós (22) días del mes de agosto de 2025.


CHRISTIAN CAMILO RAMIREZ CASTAÑO
Presidente


JULLY PAULINY GONZÁLEZ LÓPEZ
Secretaria





ANEXO 1

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad de la información de la Universidad CESMAG define las directrices para salvaguardar los activos de información, asegurando su confidencialidad, integridad y disponibilidad. Promueve el cumplimiento normativo, la adopción de estándares de seguridad y ciberseguridad, así como la gestión proactiva de riesgos, incidentes y eventos. Además, fomenta una cultura de responsabilidad, ética y manejo adecuado de la información, alineados con los valores y principios institucionales para el mejoramiento continuo y buenas prácticas de seguridad de la información.

ALCANCE

La Política de Seguridad de la Información de la Universidad CESMAG aplica a todos los usuarios internos y externos, procesos, sistemas, activos tecnológicos y datos, independientemente de su formato o medio. Incluye la gestión ética y responsable de información académica, administrativa, financiera y personal, garantizando su confidencialidad, integridad y disponibilidad. Abarca la alineación con normativas, gestión de riesgos, incidentes y el uso adecuado de recursos tecnológicos para proteger los activos de información institucionales.

OBJETIVO

Establecer los lineamientos estratégicos para la gestión integral de la seguridad de la información en la Universidad CESMAG, asegurando el cumplimiento normativo y la protección de la confidencialidad, integridad y disponibilidad de los datos. Implementando un marco de control y responsabilidad en seguridad de la información, así como adoptar tecnologías robustas para fortalecer la protección de los activos de información institucionales.

LINEAS DE ACCIÓN

1. Fomentar una cultura de seguridad de la información.
2. Gestión y asignación de recursos.
3. Protección de la información (Integridad, Disponibilidad y Confidencialidad).
4. Prevención de incidentes o eventos de ciberseguridad.
5. Cumplimiento Normativo.

ESTRATEGIAS

El Comité de Tecnología de la Información, en conjunto con el asesor de seguridad de la información y gobierno de datos, liderará la gestión integral de la política de seguridad en la Universidad CESMAG. Promoviendo la articulación de estrategias, asignación de roles clave, supervisión de la implementación de mecanismos de protección y el fortalecimiento de una cultura institucional orientada a la seguridad de la información, garantizando su cumplimiento en todos los niveles organizacionales.

- 1. Comunicación y participación de todos los colaboradores y campañas de concientización.**





El recurso humano corresponde un factor fundamental en la protección de la información en formato digital y físico, siendo responsabilidad de todos los colaboradores de LA UNIVERSIDAD CESMAG conocer y cumplir los lineamientos aquí contemplados. La Universidad pone a disposición de todos los colaboradores canales y herramientas institucionales, para divulgar los lineamientos, normas, procedimientos y políticas de seguridad de la información, para el cumplimiento de todo el personal del alma mater. La Universidad de manera periódica definirá y ejecutará campañas de concientización para todos los colaboradores de la Universidad en materia de seguridad de la información y dejará registros de dichas campañas, así como también, definirá las mejores estrategias de capacitación y actualización del material sobre las mismas.

2. Gestión y asignación de recursos.

La Universidad CESMAG con el apoyo de su recurso humano interno, tales como estudiantes en práctica, grupos de investigación, docentes de facultades y áreas relacionadas con infraestructura de tecnología de la información, buscará permanentemente innovar, investigar e integrarse a tecnologías seguras en materia de seguridad de la información. Además, la universidad busca de manera constante propender por el uso e implementación de infraestructuras tipo OPEN SOURCE o de código abierto o tipo GNU, buscando siempre la madurez, el posicionamiento y la innovación de estas en el campus universitario.

Dado que se requiera invertir en recursos o paquetes de software licenciados, se llevará la propuesta a Comité de Tecnología de la Información y a la Vicerrectoría Financiera y Desarrollo Institucional para asignar recursos económicos destinados a la adquisición de equipos o software que sea necesario y que no se pueda solventar con infraestructura OPEN SOURCE.

3. Gestión segura de la información.

Con el propósito de garantizar el tratamiento idóneo y protección segura de la información, la Universidad CESMAG identifica, clasifica, valora y trata sus activos de información en función de sus características de Confidencialidad, Integridad y Disponibilidad. Para tal propósito la Universidad imparte los siguientes lineamientos y/o directrices como requisitos mínimos de seguridad de la información:

3.1. Controles de acceso.

El acceso a los sistemas de información y datos debe estar basado en el principio de necesidad de conocer y controlado de tal forma que cada usuario tiene un compromiso para reducir los riesgos asociados a la alteración, destrucción o fuga de información. El acceso a los sistemas de información se debe hacer con claves de carácter personal e intransferible.

Cada usuario de los sistemas de información y herramientas tecnológicas de la Universidad es responsable de proteger la información e infraestructura tecnológica que usa o tiene a su cargo, así mismo debe desarrollar y ejecutar las acciones necesarias para evitar que se produzcan eventos que afecten su integridad, disponibilidad y confidencialidad.

Características de las claves de acceso:

- ✓ Personales e intransferibles.
- ✓ Deben cambiarse periódicamente.
- ✓ Deben guardarse de manera cifrada con protocolos seguros.
- ✓ Debe tener una longitud mínima de 12 caracteres.





- ✓ Debe tener en su composición combinaciones mayúsculas, minúsculas, números y caracteres especiales.
- ✓ Nunca debe incluir palabras de diccionario o combinaciones consecutivos de números.

3.2. Activos de información.

Los activos de información electrónica relacionados con información alojada en equipos de cómputo deben ser asegurados mediante controles que prevengan su daño o pérdida. Así mismo, la información en medio físico debe protegerse frente a accesos no autorizados y daño o pérdida. Se debe contar con mecanismos tecnológicos y/o manuales de control de acceso que permitan establecer un perímetro de seguridad claramente definido y acorde con los resultados de la identificación de riesgos relacionados con seguridad física y electrónica.

3.3. Protección de equipos de cómputo.

Todos los equipos deben estar registrados en un inventario, situarse y resguardarse de tal forma que se reduzca el riesgo de daño o de acceso no autorizado a los mismos. Los equipos principales de cómputo tales como servidores y elementos de interconexión deben estar alojados en sitios seguros con acceso restringido.

3.4. Reutilización o eliminación segura de equipos de cómputo.

La Universidad cuenta con controles para instalar, configurar las herramientas y/o programas de software en respectivos en los equipos de cómputo en la organización, así como de su actualización permanente. Además, cuenta con mecanismos y procedimientos de control para la reutilización de equipos, re-potencialización y/o desuso de estos incluyendo mecanismos de borrado seguro de la información y destrucción de discos duros en desuso.

3.5. Ambientes segregados

La Universidad establece y gestiona entornos de pruebas, producción e integración, garantizando la segregación de datos y la integridad de la información. La data almacenados en las bases de datos del entorno de producción no se comparten ni se combinan con los entornos de pruebas o desarrollo. Estos entornos están diseñados para fomentar un desarrollo seguro, alineado con las mejores prácticas y directrices definidas por el responsable de seguridad de la información.

3.6. Control de Software y propiedad intelectual

Toda nueva producción de programas de software desarrollados en el campus de o en los ambientes de cómputo de la Universidad, es propiedad intelectual de la misma, incluyendo el código fuente y los objetos relacionados con las distribuciones liberadas y corresponderá a la Universidad hacer el registro de las dichas producciones ante los entes de control respectivos.

3.7. Seguridad en redes y teleinformática

La Universidad propende por una gestión segura de sus redes de datos, la cual demanda configuración de elementos de seguridad tales como antivirus, firewall y elementos de cómputo relacionados en brindar protección a los activos informáticos de la Universidad. Las redes deben estar segmentadas y ofrecer niveles de seguridad adecuados a toda la comunidad Universitaria.

3.8. Gestión segura de información compartida con proveedores

Se debe mantener un nivel apropiado de seguridad de la información que se entrega a los servicios contratados con terceros, mediante la implementación de los acuerdos contractuales con los mismos. Para el caso de tratamiento de datos de personas naturales aplicará la ley 1581 de 2012 y la política de protección de datos personales de la Universidad CESMAG.





3.9. Cumplimiento y alineación con la política de comunicaciones

El área de comunicaciones de la Universidad CESMAG es la única área autorizada para divulgar o comunicar información de la universidad en redes sociales. Los empleados o colaboradores de la universidad deben utilizar las redes sociales, con responsabilidad y nunca deben compartir contenido de la Universidad en las mismas sin la autorización del área de comunicaciones y mercadeo.

3.10. Uso de quipos de escritorio y portátiles institucionales

La Universidad otorga equipos de cómputo personales o portátiles a todos sus colaboradores y tiene a disposición de todos los estudiantes del campus universitario salas de cómputo especializadas y actualizadas. Es deber de todos los colaboradores alojar la información de trabajo en carpetas compartidas en RED CORPORATIVA y/o en las carpetas en el servicio de DRIVE institucional.

3.11. Uso herramientas institucionales

Todo colaborador debe dar un correcto uso a las herramientas institucionales citadas de continuación:

Correo corporativo: Debe incluir una firma con el número de extensión y una cuenta con imagen legible. La autenticación debe ser en dos pasos mediante el uso del teléfono celular. Todo correo institucional incluye la leyenda Habeas Data acorde a la ley 1581 de 2012.

Drive: Solo se debe almacenar información institucional, y es obligación realizar una copia de seguridad en el repositorio del grupo de trabajo asignado en la red corporativa.

Calendario: Herramienta que permite planificar cronológicamente los espacios de reuniones entre colaboradores y citar reuniones con el uso de dicha herramienta.

Chat: Medio autorizado exclusivamente para tratar temas corporativos, permitiendo el envío de documentos institucionales y la realización de teleconferencias de manera segura.

Forms: Todo formulario utilizado para recolectar información de terceros debe incluir una leyenda de consentimiento, de acuerdo con lo estipulado por la Ley 1581 de 2012. Redes sociales públicas gratuitas no están autorizadas para el envío de documentos privados o sensibles de la institución. Para este propósito, deben emplearse exclusivamente las herramientas institucionales aprobadas, siendo el correo electrónico el medio digital permitido para compartir dicha información.

Se debe utilizar únicamente software y herramientas licenciadas, aprobadas por la Universidad, con el objetivo de mitigar riesgos en los activos de información.

4. Incidentes y eventos

4.1. Implementar monitoreo continuo

Establecer sistemas de monitoreo de seguridad para detectar amenazas en tiempo real y actuar proactivamente ante posibles incidentes, asimismo, la verificación continua de redes y sistemas de información los cuales deben estar protegidos con firewalls, antivirus, cifrado y otras medidas de seguridad robustas como análisis de vulnerabilidades detectivas y correctivas.





4.2. Capacitación en ciberseguridad y seguridad de la información

Ofrecer programas de formación periódica a todos los colaboradores sobre las mejores prácticas en seguridad de la información, identificación de amenazas y manejo seguro de la información.

4.3. Promover entornos de desarrollo de software seguro

Promover buenas prácticas basadas en estándares de desarrollo seguro, garantizando que todas las aplicaciones y sistemas sean diseñados, implementados y mantenidos de acuerdo con las mejores prácticas de seguridad de la información.

4.4. Desarrollar un plan de respuesta a incidentes

Crear y mantener un plan de respuesta ante incidentes de ciberseguridad, con procedimientos claros para mitigar el impacto y recuperar rápidamente los sistemas afectados.

5. Cumplimiento normativo

La Universidad CESMAG garantiza el cumplimiento de las normativas regulatorias en seguridad de la información incluyendo:

- ✓ Constitución Política de Colombia: artículos 15 y 20, que reconocen los derechos a la intimidad, el buen nombre y la libertad de expresión, y establecen la protección de datos personales y el derecho al habeas data.
- ✓ Ley 1266 de 2008: por la cual se dictan disposiciones generales sobre el habeas data y se regula el manejo de la información contenida en bases de datos personales, especialmente lo relacionado con datos financieros, crediticios, comerciales, de servicios y provenientes de terceros países.
- ✓ Ley 1581 de 2012: por la cual se establecen disposiciones generales para la protección de datos personales y se regulan los derechos de los titulares de los datos y las obligaciones de quienes realicen su tratamiento.
- ✓ Ley 1273 de 2009 o ley de Delitos Informáticos en Colombia, establecida para proteger la información, los datos y los sistemas que utilizan tecnologías de la información y las comunicaciones.
- ✓ Ley-2502-de-2025 referente al delito de falsedad personal para la modalidad de suplantación utilizando herramientas de Inteligencia Artificial.
- ✓ Decreto 1074 de 2015: decreto único reglamentario del sector comercio, industria y turismo, que compila y reglamenta las normas relacionadas con la protección de datos personales, incluyendo: (i) Decreto 1377 de 2013 que reglamenta parcialmente la Ley 1581 de 2012, estableciendo lineamientos sobre el tratamiento de datos personales y (ii) Decreto 886 de 2014 que reglamenta el artículo 25 de la Ley 1581 de 2012, sobre las medidas de seguridad de la protección de datos personales.
- ✓ Circulares y guías de la Superintendencia de Industria y Comercio (SIC) que orientan la correcta implementación de la normativa sobre protección de datos personales y atención de consultas y reclamos.

SEGUIMIENTO

El seguimiento al desarrollo de los compromisos establecidos en la presente política se realizará mediante la fase de monitoreo estratégico establecida metodológicamente en planes de acción





acordes al cumplimiento de los objetivos y líneas definidas por el Plan Estratégico de Desarrollo vigente el cual incluye la evaluación de indicadores y monitoreo flexible, todo ello dentro de la apropiación de la mejora continua institucional y de programas académicos.

APLICACIÓN

Esta política se entiende como parte de las políticas de la Universidad CESMAG, es de obligatorio cumplimiento y su desconocimiento no puede invocarse como causal de justificación de su incumplimiento.

REVISIÓN

La política de seguridad de la información debe ser revisada periódicamente y de requerirse debe actualizarse de acuerdo con los cambios que susciten.

COMUNICACIÓN

La presente versión de la política deberá ser divulgada y difundida por intermedio de Rectoría a todo el personal de la Universidad CESMAG y deberá incluirse en la página web de la Universidad para ser accesible a todos los miembros de la comunidad universitaria.

