UNIVERSIDAD CENTRAL	**ACUERDO DEL CONSEJO SUPERIOR** **N.° 27 de 2025**	**Única Versión** **Noviembre 18 de 2025**

"Por el cual se establece la Política de Seguridad de la Información de la Universidad Central"

EL CONSEJO SUPERIOR DE LA UNIVERSIDAD CENTRAL,

en uso de sus facultades estatutarias y,

CONSIDERANDO:

Que el artículo 3º de la Ley 30 de 1992, de conformidad con la Constitución Política de Colombia, garantiza la autonomía administrativa universitaria.

Que de conformidad con lo establecido en el numeral 3° del artículo 31 del Estatuto General, es función del Consejo Superior definir y establecer las políticas académicas, administrativas y financieras de la Institución.

Que, con el objetivo de proteger los activos de información de la Universidad Central, se ve en la necesidad de establecer las directrices que permitan asegurar su confidencialidad, integridad, disponibilidad, autenticidad y no repudio de los mismos, promoviendo la protección de la información en sustento de sus procesos estratégicos y operativos, procurando los objetivos institucionales, de sostenibilidad y la racionalización de recursos tecnológicos y financieros, la implementación, seguimiento y mejora continua.

Que, en virtud de lo anterior, el Consejo Superior, en sesión ordinaria del 30 de octubre de 2025 consideró y aprobó la expedición de la Política de Seguridad de la Información en los términos y condiciones establecidos en el presente Acuerdo.

En mérito de lo anterior,

ACUERDA:

ARTÍCULO 1°. Expídase la Política de Seguridad de la Información de la Universidad Central, como se evidencia en el documento anexo que hace parte integral del presente Acuerdo.

ARTÍCULO 2°. Vigencia. El presente Acuerdo rige a partir de la fecha de su expedición y deroga las normas que le sean contrarias.

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE.

Dado en Bogotá, D. C., a los dieciocho (18) días del mes de noviembre del año de dos mil veinticinco (2025).

RAFAEL SANTOS CALDERÓN Presidente	**CAROLINA ORTEGÓN PLAZAS** Secretaria

UNIVERSIDAD CENTRAL

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

UNIVERSIDAD CENTRAL

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Consejo Superior
Rafael Santos Calderón (*presidente*)
Fernando Sánchez Torres (*consejero permanente*)
Jaime Arias (*consejero permanente*)
Augusto José Acosta (*consejero invitado*)
Carl Henrik Langebaek (*consejero invitado*)
Karen Tatiana Ramírez (*representante de los egresados*)
Aida Vanessa Wilches Morales (*representante de los docentes*)
Karen Sofía Cuervo (*representante de los estudiantes*)

Rectora
Paula López López

Vicerrector académico
Óscar Leonardo Herrera Sandoval

Vicerrector administrativo y financiero
Mario Henry Cárdenas García

Vicerrector de programas
Jorge Hernán Gómez Cardona

Primera edición: Bogotá, 2025
© Universidad Central

Preparación editorial
Centro de Recursos para el Aprendizaje y la Investigación (CRAI)
Directora: Luz Ángela González
Editor: Héctor Sanabria Rivera
Corrección de textos: Ignacio Cantillo Saade
Diseño y diagramación: Patricia Salinas Garzón

Publicado en Colombia - *Published in Colombia*

Todos los derechos reservados. Esta publicación no puede ser reproducida ni total ni parcialmente, ni registrada en sistemas de recuperación de información, ni transmitida en cualquier forma o por cualquier medio, sea este mecánico, fotoquímico, electrónico, magnético, electroóptico, por fotocopia o cualquier otro, sin el permiso previo y por escrito de los editores.

Contenido

1. Introducción 5
2. Normativa 6
3. Objetivo general 8
4. Alcance 10
5. Principios 12
6. Responsables, órganos de control y seguimiento 14

1. Introducción

La Política de Seguridad de la Información de la Universidad Central establece el marco institucional para proteger los activos de información académicos, administrativos, financieros y de investigación, en cualquier medio o plataforma, para garantizar su confidencialidad, integridad y disponibilidad para la continuidad de las operaciones.

Esta se alinea con marcos normativos y directrices institucionales y se rige por principios de autenticidad, no repudio, responsabilidad, concientización, capacitación y mejora continua. Es obligatoria para la comunidad universitaria y terceros con acceso a la información, con roles definidos que garantizan una gobernanza eficaz y una cultura de seguridad.

2. Normativa

La Política de Seguridad de la Información de la Universidad Central se fundamenta en marcos normativos, éticos y técnicos (nacionales e internacionales) para orientar la gestión y protección de los activos de información bajo principios de confidencialidad, integridad, disponibilidad, legalidad y responsabilidad institucional.

En el ámbito internacional, se reconocen normas, estándares y buenas prácticas que promueven un enfoque integral de la seguridad de la información, con criterios de confianza digital, gestión del riesgo, continuidad del negocio y respeto por los derechos fundamentales asociados al uso de la información.

En el contexto nacional, se incorporan políticas y regulaciones que definen lineamientos para la gobernanza de la seguridad, la protección de datos personales, la ciberseguridad, la prevención de incidentes y la garantía de transparencia en el uso de los sistemas de información, así como para la formación y fortalecimiento del talento humano en competencias digitales y de seguridad. Todo ello se desarrolla en coherencia con el marco legal colombiano y en sintonía con los principios misionales de la Universidad Central.

En el contexto institucional, la Universidad Central dispone de un sistema normativo sólido que respalda el desarrollo de esta Política. Este marco incluye el Estatuto General, el Código de Ética y Buen Gobierno, las políticas institucionales vigentes y el Proyecto Educativo Institucional (PEI) que establecen los principios pedagógicos, éticos y formativos que orientan el quehacer académico. Asimismo contempla directrices y proyecciones que fortalecen la cultura de seguridad, el aseguramiento de la calidad de la gestión universitaria, la innovación tecnológica responsable y el compromiso con una transformación digital segura y sostenible, en concordancia con los objetivos estratégicos de la Universidad.

3. Objetivo general

Establecer los mecanismos para salvaguardar los activos de información en la Universidad Central, con el fin de asegurar su confidencialidad, integridad y disponibilidad frente a amenazas internas o externas (sean deliberadas o accidentales), contribuyendo así a la continuidad de las operaciones institucionales.

3.1 Objetivos específicos

- Establecer directrices generales relacionadas con seguridad de la información y ciberseguridad.
- Comunicar de manera clara y oportuna los principios, normas, lineamientos y demás definidos por la Universidad Central en materia de seguridad de la información y ciberseguridad.
- Fortalecer la cultura institucional de la seguridad de la información y fomentar el compromiso de todos los integrantes de la comunidad universitaria frente a esta.
- Establecer y comunicar la responsabilidad y autoridad de la Universidad sobre el manejo de la seguridad de la información y la ciberseguridad.

- Orientar la gestión de la seguridad de la información y la ciberseguridad con base en los principios de confidencialidad, integridad y disponibilidad de los activos de información.
- Establecer un orden y marco de actuación en temas de seguridad de la información y ciberseguridad para todas las personas que presten sus servicios a la Universidad Central.
- Contribuir a la confiabilidad, imagen y credibilidad de la Universidad Central con toda su comunidad universitaria.
- Definir un lenguaje común sobre la seguridad de la información y la ciberseguridad dentro de la Universidad.

4. Alcance

La Política de Seguridad de la Información de la Universidad Central se extiende a la totalidad de los activos de información institucional, comprendiendo datos científicos, académicos, administrativos, financieros y de gestión, sin importar su formato (físico o digital) ni el medio en el que se encuentren almacenados, procesados o transmitidos. Esta cobertura incluye, entre otros, bases de datos, sistemas académicos, plataformas de investigación, servicios en la nube, repositorios institucionales y cualquier otro entorno tecnológico empleado en el desarrollo de las funciones misionales y de apoyo de la Universidad.

Esta Política es de aplicación obligatoria para todos los integrantes de la comunidad universitaria, así como para proveedores, contratistas y terceros que, por razón de sus funciones o vínculos contractuales, accedan o gestionen información institucional. Se espera que cada uno de estos actores conozca, entienda y cumpla con las disposiciones definidas en la presente Política.

La Universidad Central, en concordancia con su compromiso institucional, promoverá la protección de la información en sustento de

sus procesos estratégicos y operativos, procurando, en coherencia con los objetivos institucionales de sostenibilidad y la racionalización de recursos tecnológicos y financieros, la implementación, seguimiento y mejora continua de esta Política.

5. Principios

5.1 Confidencialidad

Garantizar que la información institucional esté protegida contra accesos no autorizados, implementando los controles necesarios, en cumplimiento de las leyes de protección de datos personales y *habeas data*.

5.2 Integridad

Establecer que la información institucional sea precisa, fiable y completa y que no sea modificada sin autorización.

5.3 Disponibilidad

Garantizar que la información y los servicios estén disponibles de manera oportuna y confiable, en el momento y forma requeridos por los procesos académicos, administrativos y de investigación, a través de planes de continuidad y recuperación que aseguren el acceso adecuado a los activos de información frente a interrupciones, fallos o situaciones imprevistas, para fortalece así la resiliencia operativa institucional.

5.4 Autenticidad

Busca verificar la identidad de los usuarios, procesos o dispositivos que acceden a la información, mediante contraseñas seguras, autenticación de múltiples factores y certificados digitales.

5.5 No repudio

Proporciona evidencia de que una transacción o comunicación ha ocurrido y que no puede ser negada por ninguna de las partes involucradas.

5.6 Responsabilidad

La Universidad Central define claramente los roles y responsabilidades de cada persona dentro de la Institución en relación con la seguridad de la información.

5.7 Conciencia y capacitación

La Universidad Central promueve la conciencia sobre la seguridad de la información entre todos los miembros de la Universidad y les proporciona la capacitación necesaria para cumplir con la Política.

5.8 Mejora continua

La Universidad Central identifica las oportunidades de mejora e implementa los cambios para garantizar la eficacia y relevancia de la gestión de seguridad de la información a lo largo del tiempo.

6. Responsables, órganos de control y seguimiento

La implementación y sostenibilidad de la Política de Seguridad de la Información en la Universidad Central requiere la participación activa y articulada de diversos actores institucionales, cada uno con responsabilidades específicas según su rol dentro del ecosistema universitario. A nivel estratégico, existen instancias que tienen a su cargo la revisión y aprobación de la estrategia de seguridad de la información y ciberseguridad, garantizando que esta se encuentre alineada con los objetivos institucionales y con los marcos normativos aplicables.

Al Consejo Superior, como máxima instancia de gobierno institucional, le corresponde discutir y aprobar la Política, su sentido y estructura o las modificaciones pertinentes. De igual manera, recibir informes periódicos del avance de la Política y sus desarrollos más destacados.

Auditoría Interna será responsable de validar los resultados de las evaluaciones de riesgos, los diagnósticos de estado y los incidentes significativos, así como de hacer seguimiento a las acciones derivadas de auditorías y del cumplimiento de requisitos legales y contractuales.

En el ámbito operativo y técnico, el Comité TIC tiene funciones orientadas a la gestión de los activos de información, la administración

de riesgos críticos, el diseño de estrategias de continuidad y recuperación ante desastres y la supervisión de la infraestructura tecnológica. Se lideran procesos de fortalecimiento de la seguridad, implementación de controles, gestión de accesos, análisis de no conformidades y desarrollo de campañas institucionales de concientización. Estas tareas se coordinan de forma permanente con diferentes áreas para asegurar la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI).

Por su parte, los responsables de procesos académicos, administrativos y de gestión tienen el deber de identificar, valorar y proteger los activos de información bajo su cargo, asegurar la implementación de acciones correctivas, gestionar riesgos asociados y promover el cumplimiento de la Política en sus equipos de trabajo. Su compromiso es fundamental para establecer un entorno seguro, confiable y resiliente dentro de la Universidad.

En conclusión, toda la comunidad universitaria tiene la responsabilidad de cumplir con los lineamientos establecidos, participar en los procesos de capacitación, proteger los activos de información asignados según sus funciones y reportar oportunamente cualquier incidente de seguridad o situación que pueda poner en riesgo la integridad de la información institucional.

Este modelo de responsabilidades compartidas permite una gobernanza efectiva de la seguridad de la información, donde cada actor reconoce su papel y contribuye activamente a consolidar una cultura institucional orientada a la protección de los activos de información y al cumplimiento de los principios de confidencialidad, integridad y disponibilidad.

UNIVERSIDAD CENTRAL