CORPORACIÓN UNIVERSITARIA COMFACAUCA – UNICOMFACAUCA
CONSEJO SUPERIOR

ACUERDO 019 DE 2026
(24 de junio de 2026)

Por el cual se establece la Política de Seguridad de la Información y Ciberseguridad de la Corporación Universitaria Comfacauca — Unicomfacauca, y se derogan los Acuerdos del Consejo Superior 003 y 004 de 2018, y se dictan otras disposiciones.

El Consejo Superior de la Corporación Universitaria Comfacauca — Unicomfacauca, en uso de sus atribuciones legales y estatutarias, y

CONSIDERANDO

Que la Constitución Política de Colombia, en su artículo 15, reconoce el derecho fundamental al habeas data y la protección de la intimidad personal y familiar, lo cual exige a las instituciones que tratan información personal adoptar medidas técnicas, administrativas y humanas suficientes para garantizarlo.

Que la Ley 1273 de 2009 tipificó como delitos las conductas atentatorias contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos, lo que impone a Unicomfacauca el deber de prevención y de protección activa de su infraestructura y de sus activos de información.

Que la Ley 1581 de 2012 y su Decreto Reglamentario 1377 de 2013 obligan a los responsables y encargados del tratamiento de datos personales a implementar medidas apropiadas y efectivas para garantizar el debido tratamiento de los datos, deber que se reglamentó internamente mediante el Acuerdo 001 de 2024 del Consejo Superior.

Que la Resolución 15224 de 2020 dl Ministerio de Educación Nacional, que establece los parámetros de autoevaluación, verificación y evaluación de las condiciones de calidad institucional reglamentadas en el Decreto 1075 de 2015 modificado por el Decreto 1330 de 2019, contempla expresamente la existencia y aplicación de una política de seguridad de la información como condición de calidad de carácter institucional para las instituciones de educación superior.

Que los documentos CONPES 3854 de 2016 y CONPES 3995 de 2020, sobre seguridad y confianza digital, establecen lineamientos de política pública en materia de gestión de riesgos digitales que la Corporación adopta como referente para la formulación de la presente Política.

Que las normas técnicas internacionales NTC ISO/IEC 27001:2022 y NTC ISO/IEC 27002:2022 proporcionan los requisitos y los controles para establecer, implementar, mantener y mejorar de manera continua un Sistema de Gestión de Seguridad de la Información, y constituyen el referente técnico que se adopta como guía para la implementación de la presente Política.

Que mediante Acuerdos del Consejo Superior 003 de 2018 (Política de Confidencialidad y buen uso de los Recursos Tecnológicos) y 004 de 2018 (Política de Privacidad y Seguridad de la Información), se adoptaron los primeros instrumentos institucionales en la materia, los cuales requieren ser actualizados, integrados y derogados, en razón de la evolución del marco normativo, de las amenazas cibernéticas, de las modalidades de trabajo remoto, de la adopción de servicios en la nube y de la incorporación de inteligencia artificial en las labores académicas y administrativas.

Que Unicomfacauca cuenta con instrumentos del Sistema de Gestión de Calidad vigentes en materia de seguridad y protección de la información, en particular el Manual de Seguridad de la Información (MGT-01), el Manual de Procedimientos de Protección de Datos Personales (MGT-02) y los procedimientos asociados, los cuales se articulan con la presente Política y deberán actualizarse para reflejar sus disposiciones.

Que mediante Resolución de Rectoría 059 de 2025 se actualizó la denominación del antiguo Comité de Tecnologías de la Información a Comité de Seguridad de la Información, y se reorganizó su composición, funciones y periodicidad de sesiones, instrumento con el cual la presente Política se articula.

Que mediante Acuerdo 017 de 2021 el Consejo Superior estableció la Política de Administración del Riesgo de Unicomfacauca, con la cual la presente Política se articula en cuanto los riesgos de seguridad de la información y ciberseguridad constituyen un componente del mapa de riesgos institucional.

Que la información, en sus distintas formas y soportes, constituye un activo estratégico para Unicomfacauca, y su protección es una responsabilidad institucional que excede a la Sección de Sistemas de Información y compromete a toda la estructura organizacional, bajo el liderazgo de la Alta Dirección.

En mérito de lo expuesto,

ACUERDA

ARTÍCULO 1°. Establecer la Política de Seguridad de la Información y Ciberseguridad de la Corporación Universitaria Comfacauca — Unicomfacauca, y derogar los Acuerdos No. 003 y No.004 de 2018.

CAPÍTULO I
DISPOSICIONES GENERALES

ARTÍCULO 2°. OBJETO Y ALCANCE.

La Corporación Universitaria Comfacauca adopta la Política de Seguridad de la Información y Ciberseguridad, a fin de preservar la confidencialidad, la integridad, la disponibilidad, la autenticidad, la trazabilidad y la resiliencia de la información institucional, así como la ciberseguridad de su infraestructura tecnológica, de sus servicios digitales y de su comunidad universitaria, en cumplimiento del marco constitucional, legal y técnico aplicable.

La presente Política aplica a:

- **a)** Toda la información que Unicomfacauca recolecte, procese, almacene, comunique, transfiera o disponga, en cualquier soporte (físico, digital, oral o de cualquier otra naturaleza).
- **b)** Todos los activos de información, sistemas de información, infraestructura tecnológica, redes, servicios en la nube, dispositivos móviles, aplicaciones y servicios digitales de Unicomfacauca.
- **c)** Todos los colaboradores de Unicomfacauca, incluidos: directivos, docentes de tiempo completo, docentes de medio tiempo, docentes hora cátedra, administrativos, contratistas, proveedores, practicantes y pasantes; así como los estudiantes, aspirantes, graduados, egresados, visitantes, conferencistas, usuarios del Consultorio Jurídico, del Centro de Conciliación, del Núcleo de Apoyo Contable y Fiscal (NAF), del Consultorio

Empresarial y, en general, cualquier persona que acceda a información o a recursos tecnológicos institucionales.

d) Toda relación contractual o de cualquier otra naturaleza que implique acceso, tratamiento o custodia de información de Unicomfacauca por parte de terceros.

ARTÍCULO 3°. ARTICULACIÓN NORMATIVA. La presente Política se articula con los siguientes instrumentos institucionales, cuya vigencia se mantiene y cuyas actualizaciones deberán reflejar las disposiciones aquí contenidas:

a) Acuerdo C.S. 001 de 2024 — Política de Protección de Datos Personales, en cuanto al tratamiento de datos personales conforme a la Ley 1581 de 2012 y normas concordantes.

b) Acuerdo C.S. 017 de 2021 — Política de Administración del Riesgo, con la cual se integran los riesgos de seguridad de la información y ciberseguridad.

c) Acuerdo C.S. 013 de 2020 — Código de Ética y Buen Gobierno.

d) Acuerdo C.S. 005 de 2023 — Política de Gestión Documental.

e) Resolución de Rectoría 059 de 2025 — por la cual se reorganiza el Comité de Seguridad de la Información.

f) Manual de Seguridad de la Información (MGT-01) y Manual de Procedimientos de Protección de Datos Personales (MGT-02), del Sistema de Gestión de Calidad de Unicomfacauca.

g) Procedimientos del Sistema de Gestión de Calidad asociados, entre otros: PGT-01 (creación y configuración de usuarios y perfiles en el Sistema Integrado Universitario — SIU), PGT-02 (control de versiones), PGT-03 (atención de consultas y reclamos de titulares de datos personales) y PGT-08 (procedimiento de copias de seguridad).

h) Reglamento Interno de Gestión Documental (Acuerdo C.S. 021 de 2019) y Tablas de Retención Documental.

i) Reglamento Estudiantil, Reglamento Profesoral, Reglamento Interno de Trabajo y demás reglamentos que regulen el régimen disciplinario aplicable.

Parágrafo. En caso de duda interpretativa sobre el tratamiento de datos personales prevalecerá lo dispuesto en el Acuerdo 001 de 2024.

ARTÍCULO 4°. MARCO NORMATIVO. La presente Política se adopta en aplicación del siguiente marco normativo:

a) Constitución Política de Colombia, artículos 15, 20 y 74.

b) Ley 23 de 1982 (derechos de autor) y normas concordantes.

c) Ley 527 de 1999 (comercio electrónico, mensaje de datos y firma digital).

d) Ley 1266 de 2008 (Habeas Data financiero).

e) Ley 1273 de 2009 (delitos informáticos).

f) Ley 1581 de 2012 y Decreto 1377 de 2013 (protección de datos personales).

g) Ley 1712 de 2014 (Transparencia y Acceso a la Información Pública).

h) Ley 1928 de 2018 (aprobación del Convenio sobre la Ciberdelincuencia de Budapest).

i) Resolución 15224 de 2020 del Ministerio de Educación Nacional.

j) CONPES 3854 de 2016 y CONPES 3995 de 2020.

k) Circular Externa 002 de 2022 de la Superintendencia de Industria y Comercio (notificación de incidentes de seguridad).

l) NTC ISO/IEC 27001:2022, NTC ISO/IEC 27002:2022, NTC ISO/IEC 27005, ISO/IEC 27032 y NIST Cybersecurity Framework, en su versión vigente, como referentes técnicos.

ARTÍCULO 5°. DEFINICIONES. Para efectos de la interpretación y aplicación de la presente Política se adoptan las siguientes definiciones, sin perjuicio de las contenidas en la política de protección de datos de Unicomfacauca:

a) **Activo de información:** todo elemento que tenga valor para la organización y que requiera ser protegido, incluyendo información en cualquier soporte, software, hardware, servicios, personas y reputación institucional.

b) **Amenaza:** causa potencial de un incidente no deseado que puede ocasionar daño a un activo o a la organización.

c) **Autenticidad:** propiedad que asegura que la identidad de un sujeto o de un recurso es la que dice ser.

d) **Brecha de seguridad:** violación de la seguridad que ocasiona la destrucción, pérdida, alteración, divulgación o acceso no autorizado a la información, accidental o deliberadamente.

e) **Ciberseguridad:** conjunto de prácticas, tecnologías y procesos diseñados para proteger sistemas informáticos, redes, programas y datos frente a accesos no autorizados, ataques, daños o robo de información.

f) **Colaborador:** toda persona que, bajo cualquier modalidad de vínculo institucional con Unicomfacauca, participa o contribuye al desarrollo de sus procesos misionales, estratégicos, administrativos, académicos o de apoyo. Esta categoría incluye, entre otros, directivos, docentes, administrativos, contratistas, prestadores de servicios, proveedores, practicantes, pasantes y demás personas que actúen en nombre de la Institución o en articulación con sus procesos.

g) **Confidencialidad:** propiedad de la información de no ser puesta a disposición ni revelada a personas, entidades o procesos no autorizados.

h) **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad autorizada.

i) **Incidente de seguridad:** evento o serie de eventos no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones institucionales y de amenazar la seguridad de la información.

j) **Integridad:** propiedad de exactitud y completitud de la información y de los activos.

k) **Niveles de clasificación de la información:** Unicomfacauca clasifica la información en tres niveles: PÚBLICA (información de libre acceso), RESERVADA (información de uso institucional, sin acceso al público externo) y CONFIDENCIAL (información cuya divulgación no autorizada puede causar perjuicio a la Corporación, a terceros o a titulares de datos personales, incluyendo datos personales sensibles, información financiera detallada, propiedad intelectual y secretos profesionales).

l) **No repudio:** garantía de que un emisor o receptor de información no pueda negar haberla emitido o recibido.

m) **Privacidad por diseño y por defecto:** principio según el cual la protección de la información personal se incorpora desde la concepción y el diseño de los sistemas, procesos y servicios, y se mantiene en su configuración por defecto.

n) **Resiliencia:** capacidad de adaptarse y recuperarse ante incidentes, manteniendo el funcionamiento de los procesos esenciales.

o) **Riesgo de seguridad de la información:** efecto de la incertidumbre sobre los objetivos de seguridad de la información.

p) **SGSI (Sistema de Gestión de la Seguridad de la Información):** conjunto coordinado de políticas, procedimientos, recursos y actividades para gestionar y proteger los activos de información.

q) **SIU (Sistema Integrado Universitario):** sistema de información académico institucional de Unicomfacauca.

r) **Trazabilidad:** propiedad que permite registrar y reconstruir el conjunto de acciones realizadas sobre un activo de información.

s) **Vulnerabilidad:** debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

CAPÍTULO II

GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 6°. PRINCIPIOS DE GOBIERNO. El gobierno de la seguridad de la información en Unicomfacauca se rige por los siguientes principios:

a) **Responsabilidad de la Alta Dirección**. La seguridad de la información es responsabilidad institucional de la Alta Dirección y se delega operativamente en las instancias previstas en la presente Política.

b) **Transversalidad.** La seguridad de la información compromete a toda la estructura organizacional, sin que su responsabilidad recaiga exclusivamente en la Sección de Sistemas de Información.

c) **Mejora continua.** El Sistema de Gestión de la Seguridad de la Información se gestiona bajo un ciclo de mejora continua (Planear–Hacer–Verificar–Actuar).

d) **Gestión basada en riesgos.** Las decisiones de seguridad se toman con base en la identificación, análisis, evaluación y tratamiento sistemático de los riesgos.

e) **Privacidad por diseño y por defecto.** Los sistemas, procesos y servicios incorporan la protección de la información personal desde su diseño.

ARTÍCULO 7°. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN. El Comité de Seguridad de la Información, creado mediante Acuerdo del Consejo Superior 007 de 2022 como Comité de Tecnologías de la Información y reorganizado mediante Resolución de Rectoría 059 de 2025, es la instancia institucional encargada de proponer políticas y estrategias de seguridad de la información, hacer seguimiento al Sistema de Gestión de la Seguridad de la Información (SGSI) y ejercer las demás funciones previstas en la presente Política y en la normativa institucional.

Su composición, periodicidad de sesiones y secretaría se rigen por la Resolución de Rectoría 059 de 2025 o por las normas que la modifiquen, sustituyan o complementen.

Parágrafo. Las funciones del Comité previstas en el Artículo 8° del presente Acuerdo se entienden complementarias y armónicas con las establecidas en la Resolución de Rectoría 059 de 2025.

ARTÍCULO 8°. FUNCIONES COMPLEMENTARIAS DEL COMITÉ EN EL MARCO DEL SGSI. Sin perjuicio de las funciones establecidas en la Resolución de Rectoría 059 de 2025, en el marco del Sistema de Gestión de la Seguridad de la Información, son funciones del Comité de Seguridad de la Información:

a) Aprobar la metodología de gestión de riesgos de seguridad de la información, articulada con la Política de Administración del Riesgo.

b) Aprobar los lineamientos, manuales y procedimientos derivados de la presente Política, incluidas las actualizaciones del Manual de Seguridad de la Información (MGT-01) y demás instrumentos del Sistema de Gestión de Calidad relacionados.

c) Aprobar el plan anual de seguridad de la información y ciberseguridad.

d) Recomendar al Consejo Superior actualizaciones a la presente Política cuando se requiera.

e) Rendir informe anual al Consejo Superior sobre el estado del Sistema de Gestión de la Seguridad de la Información (SGSI).

ARTÍCULO 9°. GOBERNANZA OPERATIVA DEL SGSI. La gobernanza operativa del Sistema de Gestión de la Seguridad de la Información (SGSI) corresponde al Comité de Seguridad de la Información, en los términos del Artículo 7° del presente Acuerdo y de la Resolución de Rectoría 059 de 2025.

En el marco de sus funciones colegiadas, el Comité se apoyará en:

a) **La Sección de Sistemas de Información** y demás secciones del proceso de Gestión Tecnológica (Infraestructura Tecnológica y Comunicaciones), para la elaboración operativa de manuales, procedimientos, gestión de incidentes y demás funciones técnicas, conforme a la competencia de cada sección.

b) **El Oficial de Protección de Datos** a que se refiere el Acuerdo 001 de 2024, para todo lo relacionado con el tratamiento de datos personales, en articulación obligatoria con las funciones del Comité.

c) **La Dirección de Planeación y Desarrollo Institucional**, para la articulación con la Política de Administración del Riesgo y para el seguimiento al avance del plan plurianual de implementación.

d) **La sección de Talento Humano**, para la implementación operativa del plan anual de sensibilización y formación.

Parágrafo. Cuando la naturaleza de un asunto del SGSI requiera una decisión operativa urgente que no admita esperar a la siguiente sesión del Comité, el Presidente del Comité podrá convocar a sesión extraordinaria conforme a la Resolución 059 de 2025, o instruir al Comité para adoptar la medida provisional pertinente, con cargo a ratificación posterior por el Comité.

ARTÍCULO 10°. RESPONSABILIDADES DE LOS ACTORES. Cada miembro de la comunidad universitaria es responsable, en el ámbito de sus funciones, del cumplimiento de la presente Política. En particular:

a) Los directivos son responsables de promover el cumplimiento de la Política en sus áreas y de asignar los recursos necesarios.

b) Los propietarios de activos de información son responsables de su clasificación y de los controles aplicables a ellos.

c) Los administradores de sistemas son responsables de la implementación técnica de los controles.

d) Los colaboradores y usuarios son responsables del uso adecuado de los recursos y de la protección de las credenciales que les sean asignadas.

e) Los contratistas, proveedores y terceros son responsables del cumplimiento de los términos de seguridad y privacidad pactados en sus contratos.

CAPÍTULO III
POLÍTICA Y PRINCIPIOS DE SEGURIDAD

ARTÍCULO 11°. DECLARACIÓN DE LA POLÍTICA. Unicomfacauca declara que la información, en todas sus formas y soportes, es un activo estratégico institucional. Por tanto, se compromete a establecer, implementar, mantener y mejorar de manera continua un Sistema de Gestión de la Seguridad de la Información que preserve la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y resiliencia de los activos de información, mediante una gestión basada en riesgos, alineada con las normas técnicas internacionales de referencia y articulada con el cumplimiento de las obligaciones legales y contractuales que le son aplicables.

ARTÍCULO 12°. PRINCIPIOS DE SEGURIDAD. La presente Política se rige por los siguientes principios:

a) Confidencialidad, integridad y disponibilidad.

b) Autenticidad, trazabilidad y no repudio.

c) Privacidad por diseño y por defecto.

d) Mínimo privilegio: cada usuario o proceso recibe únicamente los privilegios necesarios para cumplir su función.

e) Segregación de funciones: las funciones críticas se separan para reducir el riesgo de fraude, error o uso indebido.

f) Defensa en profundidad: la seguridad se implementa en múltiples capas (físicas, lógicas, de procesos y humanas).

g) Proporcionalidad: los controles guardan proporción con el riesgo, el valor del activo y los recursos disponibles.

h) Mejora continua y resiliencia.

CAPÍTULO IV
LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 13°. GESTIÓN DE ACTIVOS DE INFORMACIÓN. Unicomfacauca mantendrá un inventario actualizado de sus activos de información críticos. Cada activo tendrá un propietario y un custodio asignados. Los activos se clasificarán según los siguientes niveles:

a) **Pública**: información de libre acceso.

b) **Reservada**: información de uso institucional, sin acceso al público externo.

c) **Confidencial**: información cuya divulgación no autorizada puede causar perjuicio a la Corporación, a terceros o a titulares de datos personales, incluyendo datos personales sensibles, información financiera detallada, propiedad intelectual y secretos profesionales.

Parágrafo. Los manuales operativos, en particular el Manual de Seguridad de la Información (MGT-01), definirán los controles aplicables a cada nivel de clasificación y los lineamientos de etiquetado en los sistemas de información.

ARTÍCULO 14°. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN. Unicomfacauca gestionará los riesgos de seguridad de la información y ciberseguridad de manera sistemática, continua y articulada con la Política de Administración del Riesgo (Acuerdo C.S. 017 de 2021), conforme a los siguientes lineamientos:

a) **Metodología.** La metodología de gestión de riesgos de seguridad de la información se basará en la NTC ISO/IEC 27005, en armonía con el marco metodológico institucional de gestión del riesgo, y será aprobada por el Comité de Seguridad de la Información.

b) **Ciclo de gestión.** El ciclo comprenderá las fases de establecimiento del contexto, identificación, análisis, evaluación, tratamiento, comunicación, monitoreo y revisión de los riesgos.

c) **Inventario de riesgos.** Se mantendrá un inventario actualizado de riesgos de seguridad de la información asociados a los activos críticos, integrado al mapa de riesgos institucional administrado por la Dirección de Planeación y Desarrollo Institucional.

d) **Tratamiento.** Para cada riesgo identificado se definirá una opción de tratamiento (mitigar, transferir, evitar o aceptar), un responsable, un plazo y los controles correspondientes.

e) **Riesgos especiales.** Recibirán tratamiento específico los riesgos derivados de: (i) servicios en la nube y proveedores tecnológicos; (ii) uso de inteligencia artificial; (iii) transferencias internacionales de datos; (iv) trabajo remoto y dispositivos personales; y (v) cadena de suministro tecnológico.

f) **Revisión.** Los riesgos de seguridad de la información se revisarán al menos anualmente y cada vez que se presenten cambios significativos en los activos, el entorno tecnológico o el marco normativo.

Parágrafo. Los resultados de la gestión de riesgos serán insumo obligatorio para el plan anual de seguridad de la información y ciberseguridad a que se refiere el Artículo 8° del presente Acuerdo.

ARTÍCULO 15°. CONTROL DE ACCESO. El acceso a los activos de información se otorgará con base en los principios de mínimo privilegio y necesidad de saber. Como mínimo:

a) Cada usuario tendrá una identidad única, intransferible y trazable.

b) El ciclo de vida de las cuentas (alta, modificación, baja) será gestionado formalmente, en articulación con el procedimiento PGT-01 vigente.

c) Las contraseñas cumplirán los estándares mínimos de complejidad establecidos en los manuales operativos.

d) El uso de autenticación multifactor (MFA, por sus siglas en inglés Multi-Factor Authentication) será obligatorio para cuentas privilegiadas, accesos remotos y servicios que tratan información clasificada como CONFIDENCIAL.

e) Los accesos serán revisados con periodicidad mínima semestral.

ARTÍCULO 16°. USO ACEPTABLE DE LOS RECURSOS TECNOLÓGICOS. Los recursos tecnológicos institucionales se usarán exclusivamente para fines relacionados con la misión y las funciones asignadas. Los lineamientos detallados de uso aceptable se desarrollan en los Anexos 1 (colaboradores) y 2 (estudiantes) del presente Acuerdo, los cuales hacen parte integral del mismo, así como en el Manual de Seguridad de la Información (MGT-01).

ARTÍCULO 17°. SEGURIDAD FÍSICA Y DEL ENTORNO. Los centros de datos, cuartos de equipos, archivos físicos con información sensible y demás zonas críticas deberán contar progresivamente con los siguientes tipos de control, conforme a la criticidad de cada zona y al plan de implementación previsto en el Artículo 34°:

a) **Control de acceso físico:** mecanismos que permitan restringir el ingreso al personal autorizado, tales como cerraduras electrónicas con autenticación (tarjeta, PIN o biometría) o equivalentes.

b) **Monitoreo:** sistemas de circuito cerrado de televisión (CCTV) u otros mecanismos de vigilancia, con conservación de los registros conforme al régimen aplicable.

c) **Protección eléctrica:** sistemas de respaldo de energía y protección contra fluctuaciones, conforme a la criticidad de los servicios alojados.

d) **Control ambiental:** sistemas de climatización para mantener temperatura y humedad adecuadas, así como sensores de detección de incendio y humo, en los espacios donde la criticidad lo justifique.

e) **Registro de ingresos:** mecanismos que permitan documentar quién accede a las zonas críticas y cuándo.

Los requisitos específicos por tipo de zona y nivel de criticidad serán definidos en el Manual de Seguridad de la Información (MGT-01) y demás manuales operativos.

Parágrafo. Dentro de los seis (6) meses siguientes a la entrada en vigencia del presente Acuerdo, la Coordinación de Infraestructura Tecnológica, en coordinación con el Comité de Seguridad de la Información, realizará un diagnóstico del estado actual de los controles físicos en las zonas críticas y presentará al Comité de Seguridad de la Información un plan de cierre de brechas, articulado con el plan plurianual de implementación previsto en el Artículo 34°.

ARTÍCULO 18°. SEGURIDAD EN OPERACIONES. Las operaciones tecnológicas se ejecutarán con procedimientos documentados, gestión formal de cambios, protección contra software malicioso, gestión de capacidad, separación de ambientes (producción, pruebas, desarrollo) y monitoreo de eventos de seguridad.

ARTÍCULO 19°. SEGURIDAD EN COMUNICACIONES Y REDES. Las redes institucionales se protegerán mediante segmentación, control perimetral, monitoreo y aseguramiento del tráfico. Las comunicaciones que involucren información clasificada como CONFIDENCIAL se cifrarán mediante protocolos seguros (Transport Layer Security — TLS 1.2 o superior, o equivalente).

ARTÍCULO 20°. CRIPTOGRAFÍA. Unicomfacauca aplicará controles criptográficos para proteger la confidencialidad e integridad de la información, conforme a los siguientes lineamientos mínimos:

a) Cifrado en tránsito mediante TLS 1.2 o superior para servicios públicos y portales institucionales.

b) Cifrado en reposo para bases de datos y repositorios que contengan información clasificada como CONFIDENCIAL.

c) Gestión centralizada del ciclo de vida de claves criptográficas y de certificados digitales.

ARTÍCULO 21°. DESARROLLO Y ADQUISICIÓN SEGURA DE SOFTWARE. Los desarrollos internos y las adquisiciones de software incorporarán requisitos de seguridad y privacidad desde la fase de diseño. Antes de su puesta en producción se realizarán pruebas de seguridad proporcionales al nivel de criticidad del sistema.

ARTÍCULO 22°. TRABAJO REMOTO, EQUIPOS INSTITUCIONALES Y DISPOSITIVOS PERSONALES. El acceso a información y recursos institucionales desde fuera de las instalaciones de Unicomfacauca, así como el uso de equipos institucionales y de dispositivos personales (BYOD, Bring Your Own Device), se sujetará a los siguientes lineamientos diferenciados según la clasificación de la información:

a) **Equipos institucionales.** Los equipos asignados por Unicomfacauca a sus colaboradores son herramientas de trabajo, propiedad de la Corporación, y se utilizarán conforme a la presente Política, al Anexo 1 y a los manuales operativos. Estos equipos contarán con los controles técnicos definidos por la Coordinación de Infraestructura Tecnológica (antivirus, cifrado de disco cuando aplique, gestión centralizada, actualizaciones automatizadas, capacidad de borrado remoto).

b) **Acceso desde equipos personales (BYOD).** El uso de dispositivos personales para acceder a información institucional se regirá por la clasificación de la información, así:

   i. Información PÚBLICA: podrá ser consultada desde cualquier dispositivo sin restricción adicional, conforme al uso aceptable previsto en el Anexo 1.

   ii. Información RESERVADA: requerirá autorización previa, autenticación multifactor (MFA), uso de redes privadas virtuales (VPN) cuando se acceda fuera de la red institucional, y cumplimiento de los requisitos mínimos de seguridad del dispositivo (sistema operativo soportado y actualizado, antivirus, bloqueo de pantalla con contraseña o biometría).

   iii. Información CONFIDENCIAL: está prohibido su acceso, almacenamiento o procesamiento desde dispositivos personales no inscritos en el esquema de gestión de dispositivos móviles (MDM) institucional o equivalente. Las excepciones requerirán autorización expresa del Comité de Seguridad de la Información y la implementación de controles compensatorios.

c) **Trabajo remoto.** El trabajo remoto desde cualquier ubicación distinta a las instalaciones institucionales requerirá: (i) conexión a través de VPN institucional o servicios equivalentes aprobados; (ii) autenticación multifactor; (iii) cumplimiento de los lineamientos del Anexo 1; (iv) compromiso del colaborador de proteger la privacidad de pantallas, conversaciones y documentos físicos en su entorno de trabajo.

d) **Prohibiciones generales aplicables tanto a equipos institucionales como personales.** Está prohibido: (i) almacenar información institucional clasificada como CONFIDENCIAL en servicios personales en la nube o en medios extraíbles no autorizados; (ii) reenviar correo institucional de manera sistemática a cuentas personales; (iii) conectar dispositivos personales a la red institucional sin la autorización y los controles previstos; (iv) compartir credenciales con terceros, incluidos familiares.

e) **Terminación del vínculo.** Al término del vínculo laboral o contractual, el colaborador devolverá los equipos institucionales asignados y eliminará toda información institucional alojada en dispositivos personales autorizados, con cargo a la verificación correspondiente por parte de Talento Humano y de la Coordinación de Infraestructura Tecnológica.

Parágrafo. Los lineamientos técnicos específicos de configuración, controles obligatorios por nivel de clasificación, listas de software autorizado y procedimientos de inscripción en el esquema MDM serán desarrollados en el Manual de Seguridad de la Información (MGT-01) en su versión 2.

ARTÍCULO 23°. SERVICIOS EN LA NUBE Y TRANSFERENCIAS INTERNACIONALES DE DATOS. La adopción de servicios en la nube (infraestructura, plataforma o software como

servicio — IaaS, PaaS, SaaS, por sus siglas en inglés) y la transferencia internacional de datos personales se sujetarán a los siguientes lineamientos:

a) **Evaluación previa del proveedor (due diligence).** Antes de contratar un servicio en la nube se realizará una evaluación que comprenda, como mínimo: jurisdicción y país de alojamiento de los datos, certificaciones de seguridad del proveedor (ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 2 o equivalentes), niveles de servicio (SLA) ofrecidos, mecanismos de portabilidad y reversión de datos, antecedentes de incidentes y postura ante autoridades de protección de datos.

b) **Clasificación de la información a procesar en la nube.** La información clasificada como CONFIDENCIAL solo podrá ser procesada en servicios en la nube que cuenten con cifrado en reposo y en tránsito, controles de acceso robustos y garantías contractuales suficientes. La información RESERVADA podrá procesarse en servicios en la nube con controles equivalentes a los institucionales. La información PÚBLICA podrá procesarse sin restricciones particulares.

c) **Cláusulas contractuales mínimas.** Los contratos de servicios en la nube incorporarán las cláusulas previstas en el Anexo 3 del presente Acuerdo y, cuando aplique, las del Acuerdo 001 de 2024 o de la norma que lo modifique, sustituya o complemente. En todos los casos se pactará: titularidad de los datos en cabeza de Unicomfacauca, prohibición de uso secundario de los datos por el proveedor, derecho de auditoría, notificación de incidentes en los términos del Anexo 3, y obligaciones de devolución y eliminación segura al término del contrato.

d) **Transferencia internacional de datos personales.** Cuando la prestación del servicio en la nube implique transferencia internacional de datos personales:

   i. Se observarán los requisitos del artículo 26 de la Ley 1581 de 2012, sus normas reglamentarias y las regulaciones que la Superintendencia de Industria y Comercio expida sobre la materia.

   ii. Se preferirán proveedores con presencia o alojamiento en países declarados de nivel adecuado de protección por la Superintendencia de Industria y Comercio.

   iii. Cuando se transfiera información a países que no cuenten con nivel adecuado, se adoptarán garantías contractuales específicas y, cuando corresponda, se solicitará la autorización previa del titular o de la autoridad.

e) **Continuidad y portabilidad.** Se evitarán dependencias críticas de un único proveedor (vendor lock-in) y se incluirán en los contratos cláusulas que garanticen la portabilidad de los datos y la continuidad del servicio ante terminación, suspensión o falla del proveedor.

f) **Inventario y supervisión.** La Coordinación de Infraestructura Tecnológica mantendrá un inventario actualizado de los servicios en la nube contratados y de la información que procesan, el cual será reportado al Comité de Seguridad de la Información.

ARTÍCULO 24°. USO RESPONSABLE DE INTELIGENCIA ARTIFICIAL. El uso de herramientas de inteligencia artificial generativa o predictiva con información de Unicomfacauca observará los siguientes lineamientos mínimos:

a) Se prohíbe cargar, suministrar o exponer en herramientas no aprobadas información clasificada como CONFIDENCIAL, incluidos datos personales sensibles.

b) El Comité de Seguridad de la Información mantendrá una lista de servicios de inteligencia artificial aprobados para uso institucional.

c) El uso de inteligencia artificial en la producción académica deberá garantizar la transparencia en su utilización, la adecuada citación cuando aplique, la originalidad de los contenidos y el respeto por los derechos de autor, sin perjuicio de lo dispuesto en el Reglamento Estudiantil, el Reglamento Profesoral y los demás reglamentos institucionales y normas vigentes aplicables a la integridad de la producción académica.

d) Las decisiones automatizadas que afecten significativamente a personas requerirán supervisión humana y trazabilidad.

e) Antes de cargar información en herramientas de inteligencia artificial, el colaborador o estudiante deberá verificar si dicha información contiene propiedad intelectual de Unicomfacauca, de terceros con quienes la Corporación tenga obligaciones contractuales de confidencialidad, o material protegido por derechos de autor. En tales casos, deberá abstenerse de cargarla salvo que se cuente con autorización expresa del titular o se utilicen instancias de la herramienta que garanticen contractualmente la no retención y no reutilización de la información (instancias empresariales con cláusulas de privacidad y propiedad intelectual).

f) El uso de contenido generado por herramientas de inteligencia artificial en producciones institucionales, académicas o de investigación se documentará de manera trazable. La Corporación no asume titularidad ni responsabilidad sobre contenidos generados por inteligencia artificial cuya procedencia o licenciamiento no haya sido verificado por el colaborador o estudiante que los utiliza, sin perjuicio de las obligaciones que correspondan a Unicomfacauca conforme al régimen aplicable.

g) El contenido generado por herramientas de inteligencia artificial deberá ser revisado, contrastado y validado por el colaborador o estudiante antes de utilizarse en documentos oficiales, informes, productos académicos, comunicaciones institucionales o procesos de toma de decisiones.

h) Las decisiones académicas, administrativas, financieras, disciplinarias, jurídicas o investigativas no podrán depender exclusivamente de herramientas de inteligencia artificial. En todos los casos se mantendrá la revisión, validación y responsabilidad humana.

ARTÍCULO 25°. GESTIÓN DE PROVEEDORES Y TERCEROS. Los contratos con proveedores y terceros que impliquen acceso, tratamiento o custodia de información de Unicomfacauca incluirán cláusulas de seguridad y privacidad conforme al Anexo 3. Los proveedores que traten información clasificada como CONFIDENCIAL estarán sujetos al derecho de auditoría por parte de Unicomfacauca.

ARTÍCULO 26°. CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN ANTE DESASTRES. Como parte del desarrollo del Sistema de Gestión de la Seguridad de la Información, Unicomfacauca elaborará, formalizará, mantendrá actualizados y probará periódicamente los siguientes instrumentos:

a) Un Plan de Continuidad del Negocio (BCP, por sus siglas en inglés Business Continuity Plan) que identifique los procesos críticos y los tiempos máximos tolerables de interrupción.

b) Un Plan de Recuperación ante Desastres (DRP, por sus siglas en inglés Disaster Recovery Plan) que defina, para cada sistema crítico, los objetivos de tiempo de recuperación (RTO) y de punto de recuperación (RPO).

c) Una política de copias de respaldo articulada con el procedimiento PGT-08 vigente, que como mínimo observe la regla 3-2-1: tres (3) copias en dos (2) medios distintos, con al menos una (1) copia conservada en una sede o ubicación distinta a la del original.

ARTÍCULO 27°. ARTICULACIÓN CON MANUALES Y PROCEDIMIENTOS OPERATIVOS. La presente Política, como instrumento marco, se desarrolla operativamente a través del Manual de Seguridad de la Información (MGT-01) en su versión 2 y de los procedimientos asociados del Sistema de Gestión de Calidad. El MGT-01 v2 contendrá, como mínimo, los siguientes bloques temáticos:

a) **Gobierno y roles:** identificación de los actores del SGSI, sus responsabilidades operativas, matriz RACI y articulación con el Comité de Seguridad de la Información.

b) **Gestión de activos y clasificación:** inventario, propietarios, custodios, niveles de clasificación (PÚBLICA, RESERVADA, CONFIDENCIAL), etiquetado, ciclo de vida y disposición segura.

c) **Control de acceso:** ciclo de vida de cuentas (alta, modificación, baja), estándares de contraseñas, autenticación multifactor (MFA), revisión periódica de accesos y articulación con el procedimiento PGT-01.

d) **Criptografía:** estándares mínimos de cifrado en tránsito y en reposo, gestión del ciclo de vida de claves y certificados.

e) **Seguridad física y del entorno:** requisitos por tipo de zona, controles específicos (acceso, monitoreo, protección eléctrica, control ambiental, registro de ingresos).

f) **Seguridad en operaciones:** procedimientos documentados, gestión de cambios, protección contra software malicioso, gestión de capacidad, separación de ambientes, monitoreo de eventos.

g) **Seguridad en comunicaciones y redes**: segmentación, control perimetral, monitoreo, aseguramiento del tráfico, configuración de VPN.

h) **Trabajo remoto, BYOD y gestión de dispositivos:** requisitos por nivel de clasificación, inscripción en MDM, listas de software autorizado, configuración mínima de dispositivos.

i) **Servicios en la nube:** criterios de selección y evaluación de proveedores, inventario de servicios contratados, controles compensatorios.

j) **Inteligencia artificial:** lista de servicios aprobados, procedimientos para autorización de nuevos servicios, trazabilidad del uso.

k) **Gestión de incidentes y notificación:** clasificación por severidad, equipo de respuesta, plazos internos, articulación con el procedimiento institucional vigente y con la notificación a la SIC.

l) **Gestión de copias de respaldo:** articulación con el procedimiento PGT-08, regla 3-2-1, pruebas periódicas de restauración.

m) **Gestión de vulnerabilidades:** escaneos, parches, pruebas de penetración, priorización por riesgo.

n) **Continuidad del negocio y recuperación ante desastres (BCP/DRP**): articulación con los Planes a que se refiere el Artículo 26°.

o) **Sensibilización, formación y cultura:** contenido mínimo, periodicidad, métricas de cobertura y eficacia.

Parágrafo. Los procedimientos PGT-01, PGT-02, PGT-03, PGT-08 y demás procedimientos del Sistema de Gestión de Calidad relacionados se mantendrán actualizados conforme a la presente Política y al MGT-01 v2. Las actualizaciones serán aprobadas por las instancias competentes del Sistema de Gestión de Calidad y serán de conocimiento del Comité de Seguridad de la Información.

CAPÍTULO V
CIBERSEGURIDAD Y GESTIÓN DE INCIDENTES

ARTÍCULO 28°. ESTRATEGIA DE CIBERSEGURIDAD. Unicomfacauca implementará una estrategia de ciberseguridad alineada con el NIST Cybersecurity Framework, en su versión vigente, y con la ISO/IEC 27032, organizada en torno a las funciones de gobernar, identificar, proteger, detectar, responder y recuperar.

ARTÍCULO 29°. GESTIÓN DE VULNERABILIDADES. Se mantendrá un programa de gestión de vulnerabilidades que comprenda escaneos periódicos, remediación priorizada por riesgo, gestión de parches y pruebas de penetración periódicas sobre los servicios expuestos a internet.

ARTÍCULO 30°. GESTIÓN DE INCIDENTES DE SEGURIDAD. Unicomfacauca contará con un procedimiento formal de gestión de incidentes de seguridad, el cual desarrollará y se articulará con el procedimiento institucional vigente para el tratamiento de incidentes de seguridad de la información y datos personales, y comprenderá:

a) Detección, registro y clasificación por severidad.

b) Contención, erradicación y recuperación.

c) Análisis de causa raíz y lecciones aprendidas.

d) Notificación interna a la Alta Dirección y al Comité de Seguridad de la Información cuando la severidad lo amerite.

e) Notificación externa a la Superintendencia de Industria y Comercio en los términos de la Circular Externa 002 de 2022, cuando se trate de violaciones de datos personales, dentro de los plazos legales aplicables.

f) Comunicación a los titulares de datos personales afectados, cuando corresponda, conforme al Acuerdo 001 de 2024 o a la norma que lo modifique, sustituya o complemente, y a las disposiciones legales.

g) Cooperación con autoridades judiciales y de policía cuando los hechos sean constitutivos de delito.

h) Articulación con el procedimiento de atención de consultas, reclamos, actualizaciones, revocaciones y supresiones de los titulares de datos personales previsto en el Acuerdo 001 de 2024 o en la norma que lo modifique, sustituya o complemente, y en el procedimiento PGT-03 vigente.

ARTÍCULO 31°. MONITOREO Y REGISTRO DE EVENTOS. Los sistemas críticos generarán registros de eventos (logs) que serán protegidos contra alteración, conservados durante el tiempo necesario para fines de auditoría, investigación y cumplimiento, y monitoreados con el objeto de detectar oportunamente eventos adversos.

CAPÍTULO VI
RÉGIMEN SANCIONATORIO Y CUMPLIMIENTO

ARTÍCULO 32°. RÉGIMEN SANCIONATORIO. El incumplimiento de la presente Política dará lugar a las consecuencias previstas en los reglamentos institucionales aplicables a cada actor, sin perjuicio de las responsabilidades civiles, penales y administrativas que correspondan:

a) Para estudiantes: Reglamento Estudiantil vigente.

b) **Para docentes:** Reglamento Profesoral vigente.

c) **Para administrativos:** Reglamento Interno de Trabajo vigente y Código Sustantivo del Trabajo.

d) **Para contratistas y proveedores:** las cláusulas contractuales aplicables, incluidas las del Anexo 3.

e) **Para usuarios externos:** las condiciones de uso aplicables.

ARTÍCULO 33°. DEBER DE REPORTE. Cualquier colaborador, estudiante o miembro de la comunidad universitaria que tenga conocimiento de un incidente, riesgo material o presunto incumplimiento a la presente Política tiene el deber de informarlo, a través de los canales institucionales, al Comité de Seguridad de la Información, al Oficial de Protección de Datos o a su superior jerárquico, según corresponda.

CAPÍTULO VII
IMPLEMENTACIÓN, REVISIÓN Y VIGENCIA

ARTÍCULO 34°. IMPLEMENTACIÓN PROGRESIVA. La implementación de la presente Política, incluidas las obligaciones técnicas previstas en los Capítulos IV y V, se realizará de manera progresiva, conforme a un plan plurianual aprobado por el Comité de Seguridad de la Información y por la Rectoría, el cual identificará el estado actual, las brechas y el cronograma de cierre para cada lineamiento, priorizando los activos y procesos de mayor criticidad. La Rectoría informará anualmente al Consejo Superior sobre el avance de la implementación.

ARTÍCULO 35°. INDICADORES Y SEGUIMIENTO. El Sistema de Gestión de la Seguridad de la Información (SGSI) contará, como mínimo, con los siguientes indicadores: cobertura del inventario de activos críticos, porcentaje de cumplimiento del plan anual de seguridad, número y severidad de incidentes, tiempo medio de detección y de respuesta a incidentes, cobertura del plan de sensibilización, y resultados de auditorías internas.

ARTÍCULO 36°. AUDITORÍA INTERNA. Anualmente se realizará una auditoría interna al SGSI, cuyos resultados serán presentados al Comité de Seguridad de la Información y a la Rectoría, e informados al Consejo Superior.

ARTÍCULO 37°. REVISIÓN DE LA POLÍTICA. La presente Política será revisada, como mínimo, cada tres (3) años, o antes cuando se presenten cambios normativos, tecnológicos u organizacionales que lo justifiquen. Las modificaciones requerirán aprobación del Consejo Superior.

CAPÍTULO VIII
DISPOSICIONES FINALES

ARTÍCULO 38°. ACTUALIZACIÓN DEL MANUAL DE SEGURIDAD DE LA INFORMACIÓN (MGT-01). Dentro de los seis (6) meses siguientes a la entrada en vigencia del presente Acuerdo, las secciones del proceso de Gestión Tecnológica (Sistemas de Información, Infraestructura Tecnológica y Comunicaciones), bajo la coordinación del Comité de Seguridad de la Información, actualizarán el Manual de Seguridad de la Información (MGT-01) a su versión 2, alineándolo con la presente Política, las normas técnicas referidas y el marco normativo vigente.

ARTÍCULO 39°. FORMALIZACIÓN DEL BCP (BUSINESS CONTINUITY PLAN) Y DEL DRP (DISASTER RECOVERY PLAN) – PLAN DE CONTINUIDAD DEL NEGOCIO Y PLAN DE RECUPERACIÓN DE DESASTRES. Dentro de los dieciocho (18) meses siguientes a la entrada en vigencia del presente Acuerdo, el Comité de Seguridad de la Información, en coordinación con las secciones del proceso de Gestión Tecnológica (Sistemas de Información, Infraestructura Tecnológica y Comunicaciones) y los demás procesos institucionales, formalizará el Plan de Continuidad del Negocio y el Plan de Recuperación ante Desastres a los que se refiere el Artículo 26°.

ARTÍCULO 40°. INTERPRETACIÓN. Las dudas que surjan en la aplicación y alcance del presente Acuerdo serán resueltas por la Rectoría de la Corporación.

ARTÍCULO 41°. VIGENCIA. El presente Acuerdo rige a partir de la fecha de su expedición y deroga los Acuerdos del Consejo Superior No. 003 de 2018 y No. 004 de 2018, así como todas las disposiciones que le sean contrarias.

COMUNÍQUESE Y CÚMPLASE

Dado en Popayán, a los veinticuatro (24) días del mes de junio de dos mil veintiséis (2026).

MARISOL VELASCO CHAGUENDO
Presidente (e)

ELIANA ANDREA HERNÁNDEZ BARRERA
Secretaria General