

Preámbulo

La Universidad Católica de Córdoba, institución confiada a la Compañía de Jesús, reconoce que el avance de las tecnologías digitales avanzadas — en particular la Inteligencia Artificial (IA) y el Internet de las Cosas (IoT) — representa una oportunidad histórica para fortalecer la calidad educativa, la eficiencia administrativa y la prestación de servicios a la comunidad universitaria.

La adopción responsable de estas tecnologías debe estar orientada por los valores institucionales de la UCC: el respeto por la dignidad humana, la búsqueda de la verdad, la excelencia académica, la justicia y el bien común. En consecuencia, la presente política establece el marco normativo para el uso ético, seguro y eficiente de las tecnologías digitales avanzadas en todos los procesos de la Universidad.

CAPÍTULO I — Disposiciones Generales

Artículo 1. Objeto

La presente Política tiene por objeto:

- Establecer los principios, reglas y responsabilidades que rigen el uso de tecnologías de Inteligencia Artificial (IA) y del Internet de las Cosas (IoT) en la Universidad Católica de Córdoba.
- Garantizar un uso ético, transparente y seguro de dichas tecnologías en apoyo a la toma de decisiones, la eficiencia operativa y la prestación de servicios.
- Proteger los derechos de los miembros de la comunidad universitaria frente a los riesgos derivados del uso de estas tecnologías.

Artículo 2. Ámbito de aplicación

La presente Política es de aplicación obligatoria para:

- El personal directivo y las autoridades de los órganos de gobierno de la UCC.
- El personal administrativo y de gestión en todas sus dependencias.
- El personal docente y de investigación.
- El estudiantado de grado, posgrado y formación continua.
- Todo tercero que, en virtud de un contrato, convenio o relación de colaboración, utilice sistemas o infraestructura tecnológica de la Universidad.

Artículo 3. Definiciones

A los efectos de la presente Política, se entiende por:

- **Inteligencia Artificial (IA):** sistemas informáticos que realizan tareas que, cuando son ejecutadas por humanos, requieren inteligencia, tales como reconocimiento de patrones, toma de decisiones, generación de texto o imágenes, traducción automática y análisis predictivo.
- **Internet de las Cosas (IoT):** red de dispositivos físicos interconectados que recopilan, intercambian y procesan datos a través de internet, incluyendo sensores, cámaras, sistemas de control de acceso y equipamiento de aulas inteligentes.
- **Sistema de apoyo a la decisión:** toda aplicación tecnológica que procesa datos institucionales para sugerir, recomendar o fundamentar decisiones administrativas o académicas.
- **Dato personal:** toda información que permita identificar o hacer identificable a una persona física, conforme a la Ley N° 25.326 de Protección de Datos Personales.
- **Usuario:** toda persona comprendida en el ámbito de aplicación del artículo anterior.

CAPÍTULO II — Principios Rectores

Artículo 4. Principios

El uso de tecnologías digitales avanzadas en la UCC se regirá por los siguientes principios:

- **Centralidad de la persona:** la tecnología está al servicio de la persona humana y no a la inversa. Ninguna decisión de relevancia para derechos individuales podrá adoptarse exclusivamente mediante procesos automatizados sin intervención humana.
- **Transparencia:** los miembros de la comunidad universitaria tienen derecho a conocer cuándo interactúan con sistemas de IA, qué datos son recopilados por dispositivos IoT y de qué manera se utilizan.
- **Responsabilidad:** todo uso de tecnología avanzada implica responsabilidad. Quien incorpore, implemente o utilice estas herramientas responde por sus resultados.
- **Privacidad por diseño:** los sistemas deben incorporar mecanismos de protección de datos desde su concepción, minimizando la recopilación de información personal a lo estrictamente necesario.
- **No discriminación:** queda prohibido el uso de sistemas de IA que generen sesgos o discriminación basada en género, origen étnico, religión, condición económica, discapacidad u otras categorías protegidas.
- **Sostenibilidad:** se priorizarán soluciones tecnológicas que minimicen el impacto ambiental y promuevan el uso eficiente de recursos.
- **Complementariedad:** las tecnologías avanzadas complementan la labor docente, administrativa y de gestión, sin reemplazar el juicio profesional y la responsabilidad institucional.

CAPÍTULO III — Usos Autorizados y Prohibidos

Artículo 5. Usos autorizados en procesos académicos

Se autoriza el uso de herramientas de IA e IoT en el ámbito académico para:

- Asistencia en la elaboración y revisión de materiales de estudio, con declaración expresa de su uso.
- Apoyo en la investigación científica, análisis de datos y procesamiento de información.
- Herramientas de accesibilidad para el estudiantado con necesidades educativas especiales.
- Sistemas de detección de similitud o plagio como herramienta de orientación pedagógica.
- Plataformas de tutoría virtual y personalización del aprendizaje, bajo supervisión del personal docente.
- Monitoreo ambiental de aulas y espacios educativos mediante sensores IoT para mejorar condiciones pedagógicas.

Artículo 6. Usos autorizados en procesos administrativos

Se autoriza el uso de herramientas de IA e IoT en la gestión institucional para:

- Automatización de procesos administrativos de bajo riesgo (gestión documental, clasificación de correspondencia, generación de reportes).
- Sistemas de apoyo a la toma de decisiones en planificación estratégica, gestión presupuestaria y seguimiento académico.
- Control de acceso y seguridad perimetral mediante dispositivos IoT, conforme a la normativa de protección de datos.
- Mantenimiento predictivo de infraestructura y equipamiento.
- Atención inicial a consultas de la comunidad universitaria mediante asistentes virtuales, con derivación humana disponible en todo momento.

Artículo 7. Usos prohibidos

Queda expresamente prohibido:

- El uso de sistemas de IA para adoptar decisiones definitivas sobre calificaciones, sanciones disciplinarias, admisiones o desvinculación de personal sin revisión y validación humana.

- La recopilación de datos biométricos de miembros de la comunidad universitaria sin consentimiento informado previo y habilitación expresa de la autoridad competente.
- El uso de herramientas de IA para vigilancia, monitoreo o perfilamiento de la actividad política, sindical o religiosa de los miembros de la comunidad.
- La introducción de dispositivos IoT no homologados por el área de Tecnología de la Información en la infraestructura de red de la Universidad.
- El uso de herramientas de generación de contenido con IA para presentar como propias producciones ajenas, sin declaración de uso, en el marco de instancias de evaluación académica.
- El tratamiento de datos personales sensibles mediante herramientas de IA externas sin la debida garantía contractual de confidencialidad y cumplimiento normativo.

CAPÍTULO IV — Protección de Datos y Seguridad

Artículo 8. Protección de datos personales

El tratamiento de datos personales en el marco del uso de tecnologías digitales avanzadas se regirá por:

- La Ley N° 25.326 de Protección de los Datos Personales y su normativa reglamentaria.
- Las disposiciones de la Agencia de Acceso a la Información Pública (AAIP).
- Los principios de finalidad, proporcionalidad, calidad y seguridad en el tratamiento de datos.

Todo sistema de IA que procese datos personales de miembros de la comunidad universitaria deberá contar con una evaluación de impacto de privacidad previa a su implementación.

Artículo 9. Seguridad de la información

La incorporación de sistemas de IA e IoT deberá cumplir con:

- Los estándares de seguridad informática vigentes en la UCC y las mejores prácticas internacionales (ISO/IEC 27001).
 - La obligación de realizar auditorías periódicas de los sistemas implementados.
 - Protocolos de respuesta ante incidentes de seguridad que afecten sistemas de IA o dispositivos IoT.
 - La prohibición de conectar dispositivos IoT a redes críticas institucionales sin evaluación previa del área de Tecnología de la Información.
-

CAPÍTULO V — Responsabilidades Institucionales

Artículo 10. Órganos responsables

Se establecen las siguientes responsabilidades institucionales:

- Rectorado: aprobación de la presente política y sus actualizaciones; asignación de recursos para su implementación efectiva.
- Secretaría General (SG): coordinación general de la política, seguimiento normativo, articulación entre vicerrectorados y actualización del marco regulatorio. Es el órgano de referencia ante consultas institucionales sobre la presente normativa.
- Vicerrectorado de Innovación y Desarrollo (VRI): evaluación técnica e implementación de los sistemas de IA e IoT en la infraestructura universitaria; homologación de dispositivos y plataformas; gestión de la seguridad informática; supervisión de proveedores tecnológicos y elaboración de estándares técnicos institucionales.
- Vicerrectorado Académico (VRA): supervisión del uso de tecnologías avanzadas en los procesos de enseñanza, aprendizaje e investigación; coordinación de la formación del personal docente; articulación con las unidades académicas para el cumplimiento de la política en el ámbito curricular y de evaluación.
- Decanos, Decanas y Directores/Directoras de Unidades Académicas: supervisión del cumplimiento en el ámbito de sus dependencias, con reporte periódico a la Secretaría General.

Artículo 11. Comité de Gobernanza de Tecnologías Avanzadas

Créase el Comité de Gobernanza de Tecnologías Avanzadas (CGTA), integrado por:

- La persona titular del Vicerrectorado Académico, quien lo presidirá.
- La persona titular de la Secretaría General.
- La persona titular del Vicerrectorado de Innovación y Desarrollo o su representante.
- La persona titular de la Dirección de Recursos Humanos.
- La persona titular de la Secretaría de Investigación
- Una persona representante del Honorable Consejo Académico.

El CGTA tendrá a su cargo: la supervisión de la implementación de la presente política, la evaluación de nuevos proyectos tecnológicos, la resolución de consultas y la elaboración de reportes anuales de cumplimiento.

CAPÍTULO VI — Formación y Capacitación

Artículo 12. Alfabetización digital avanzada

La UCC promoverá la formación continua de todos los miembros de su comunidad en materia de tecnologías avanzadas, incluyendo:

- Programas de capacitación obligatoria para el personal administrativo en el uso de herramientas de IA institucionales.
- Formación del personal docente en pedagogía mediada por tecnología y uso ético de la IA en entornos educativos.
- Espacios de sensibilización para el estudiantado sobre uso responsable, sesgos algorítmicos y derechos digitales.
- Actualización periódica de las autoridades sobre el panorama normativo y ético en materia de IA.

CAPÍTULO VII — Régimen de Incumplimiento

Artículo 13. Sanciones

El incumplimiento de la presente Política podrá dar lugar a:

- Para el personal docente y administrativo: las medidas disciplinarias previstas en el Régimen del Personal Docente (RR 4662/23) o el régimen del personal administrativo según corresponda, graduadas conforme a la gravedad de la infracción.
- Para el estudiantado: las sanciones previstas en el Reglamento de Disciplina para Estudiantes (RR 1350/20).
- Para proveedores y terceros: la rescisión del contrato o convenio correspondiente, sin perjuicio de las acciones legales que pudieren corresponder.

La graduación de la sanción considerará la intencionalidad, el daño ocasionado, la reincidencia y la colaboración en la investigación del hecho.

CAPÍTULO VIII — Disposiciones Finales

Artículo 14. Revisión y actualización

La presente Política será revisada con una periodicidad no mayor a dos (2) años, o en forma extraordinaria cuando así lo requieran cambios normativos, tecnológicos o institucionales significativos. Las actualizaciones serán aprobadas por el Rectorado a propuesta de la Secretaría General.

Artículo 15. Difusión



La Secretaría General dispondrá la publicación de la presente Política en el sitio web institucional y su comunicación a todos los miembros de la comunidad universitaria dentro de los treinta (30) días hábiles de su aprobación.

Artículo 16. Entrada en vigencia

La presente Política entrará en vigencia a partir de su aprobación por el órgano de gobierno competente, sin perjuicio de lo cual se recomienda un período de implementación gradual de seis (6) meses para la adecuación de sistemas y procesos existentes.