

REGLAMENTO PARA EL USO ÉTICO, RESPONSABLE Y SEGURO DE LA INTELIGENCIA ARTIFICIAL EN LA UNIVERSIDAD METROPOLITANA

CONSEJO ACADÉMICO SUPERIOR

RESOLUCIÓN No. 56-UMET-CAS-SO-07-2026

31 de julio de 2026

RESOLUCIÓN N°. 56-UMET-CAS-SO-07-2026**EL CONSEJO ACADÉMICO SUPERIOR DE LA UNIVERSIDAD
METROPOLITANA****Considerando**

- Que, el numeral 19 del artículo 66 de la Constitución reconoce el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección y dispone que la recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley;
- Que, los artículos 350 y 352 de la Constitución establecen que el sistema de educación superior tiene como finalidad la formación académica y profesional con visión científica y humanista y que las instituciones que lo integran ejercerán su autonomía responsable, con sujeción a los principios constitucionales y al ordenamiento jurídico vigente;
- Que, el artículo 8 letra m) de la Ley Orgánica de Educación Superior, incorporado por la Ley Orgánica para la Transformación Digital y Audiovisual, establece como fin del sistema de educación superior fortalecer la formación profesional en las nuevas tecnologías para afrontar los retos de la economía digital, identificando habilidades tecnológicas y adaptando las mallas curriculares al nivel de desarrollo de tecnologías digitales;
- Que, el artículo 17 de la Ley Orgánica de Educación Superior reconoce el principio de autonomía responsable, en virtud del cual las instituciones de educación superior pueden expedir sus estatutos, reglamentos y normas internas, en armonía con la Constitución y la Ley;
- Que, la Ley Orgánica de Protección de Datos Personales, su Reglamento General y la normativa secundaria emitida por la Superintendencia de Protección de Datos Personales constituyen el marco vinculante para todo tratamiento de datos personales realizado en territorio ecuatoriano, incluido aquel ejecutado mediante sistemas de inteligencia artificial;
- Que, la Resolución N° SPDP-SPD-2026-0005-R, por la que se expide la Norma General sobre el Tratamiento de Datos Personales a Gran Escala, contempla supuestos de calificación directa que comprenden, entre otros, el tratamiento de categorías especiales de datos, la videovigilancia sistemática, los datos biométricos, las decisiones automatizadas con efectos jurídicos, los datos de niños y adolescentes en entornos educativos y las transferencias sistemáticas de datos personales;

- Que, la Resolución N° SPDP-SPD-2026-0004-R, mediante la que se expidió la Norma General de Transferencias o Comunicaciones Nacionales e Internacionales de Datos Personales, regula la documentación, legitimación y garantías aplicables a las comunicaciones y transferencias internacionales de datos personales, lo que resulta directamente aplicable a los proveedores y herramientas de inteligencia artificial alojados fuera del territorio nacional;
- Que, la Resolución N° SPDP-SPD-2026-0009-R, mediante la que se expide la Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial, establece obligaciones específicas para los responsables y encargados del tratamiento que desarrollen, entrenen, implementen, desplieguen o provean sistemas de inteligencia artificial que traten datos personales de titulares ecuatorianos, con independencia de la ubicación del sistema o del proveedor e impone, entre otras garantías, el deber de informar al titular, realizar gestión de riesgos y evaluaciones de impacto, implementar medidas de seguridad administrativas, técnicas, físicas, organizativas y jurídicas, incorporar dichos tratamientos en el Registro de Actividades de Tratamiento y auditar el funcionamiento general del sistema en función del nivel de riesgo;
- Que, la Ley Orgánica para la Transformación Digital y Audiovisual y su Reglamento General reconocen el papel del Estado, la academia y el sector productivo en el fomento del uso ético y responsable de tecnologías digitales emergentes, incluida la inteligencia artificial y mandan a las universidades a determinar dentro de sus ofertas educativas los programas o materias que puedan ser cursadas mediante medios virtuales y a fortalecer la apropiación tecnológica;
- Que, mediante Acuerdo Ministerial N° MINTEL-MINTEL-2025-0030, publicado en el Registro Oficial Suplemento N° 206 de 19 de enero de 2026, el Ministerio de Telecomunicaciones y de la Sociedad de la Información expidió la Estrategia para el Fomento del Desarrollo y Uso Ético y Responsable de la Inteligencia Artificial en el Ecuador, cuyos principios rectores comprenden, entre otros, la privacidad y la protección de datos personales, la transparencia, la equidad, la rendición de cuentas y la supervisión humana;
- Que, la Conferencia General de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, UNESCO, aprobó el 23 de noviembre de 2021 la Recomendación sobre la Ética de la Inteligencia Artificial, en la que se consagran los principios de proporcionalidad e inocuidad, seguridad y protección, equidad y no discriminación, sostenibilidad, derecho a la intimidad y a la protección de datos, supervisión y decisión humanas, transparencia y explicabilidad, responsabilidad y rendición de cuentas y sensibilización y educación;

- Que, el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial, constituye un referente internacional relevante en cuanto al enfoque basado en niveles de riesgo, las prácticas prohibidas, las obligaciones aplicables a los sistemas de alto riesgo y las exigencias de transparencia, sin perjuicio de su carácter no vinculante para el Ecuador;
- Que, los artículos 15 letra a) y 17 letra a) del Estatuto de la Universidad Metropolitana imponen a estudiantes y profesores el deber de acatar y cumplir la Constitución, la Ley, el Estatuto Institucional, las normas internas y las regulaciones del Código de Ética Institucional, de la Investigación y los Aprendizajes;
- Que, el artículo 25 letras p) y q) del Estatuto Institucional faculta al Consejo Académico Superior para aprobar y reformar, en una sola discusión, los reglamentos internos de las funciones sustantivas de educación superior y los reglamentos y resoluciones normativas internas de los procesos de gobierno, funcionamiento, trabajo, estudiantes y demás procesos habilitantes de asesoría y apoyo, previo informe favorable del Consejo de Regentes;
- Que, el Reglamento General al Estatuto de la Universidad Metropolitana, aprobado mediante Resolución N° 17-UMET-CAS-SE-03-2026, reconoce expresamente las figuras del Responsable del Tratamiento y del Delegado de Protección de Datos Personales y precisa que, para fines de organización y gestión interna, el Vicerrector Administrativo actuará como Responsable del Tratamiento de datos personales de la Universidad Metropolitana;
- Que, mediante Resolución N° 81-UMET-CAS-SO-09-2025 el Consejo Académico Superior aprobó las Políticas de Protección de Datos Personales de la Universidad Metropolitana, las cuales reconocen a la institución como responsable del tratamiento de datos personales frente a los titulares, la sociedad y el Estado y contemplan expresamente el tratamiento de datos sensibles, datos biométricos, datos de menores de edad, decisiones automatizadas, elaboración de perfiles, videovigilancia y transferencias nacionales e internacionales de datos personales;
- Que, mediante Resolución N° 57-UMET-CAS-SO-07-2025 el Consejo Académico Superior expidió el Código de Ética Institucional, de la Investigación y el Aprendizaje, el cual contempla, entre las prohibiciones aplicables a la comunidad universitaria, el uso de herramientas tecnológicas o sistemas de inteligencia artificial para sustituir, automatizar o reemplazar de forma ilegítima la autoría, el razonamiento, la redacción o la evaluación que deben reflejar el dominio personal del autor;

- Que, el artículo 19 del Código de Ética Institucional, de la Investigación y el Aprendizaje dispone la implementación, mediante resolución rectoral, de la Política Institucional de Ética y Honestidad Intelectual y establece que dicha política contendrá criterios técnicos y pedagógicos para el uso ético de herramientas tecnológicas, inteligencia artificial y otros recursos digitales en el contexto universitario;
- Que, la Universidad Metropolitana ha sido jurídicamente calificada como responsable del tratamiento de datos personales a gran escala, lo que activa obligaciones reforzadas de cumplimiento, particularmente respecto de los tratamientos efectuados mediante sistemas de inteligencia artificial;
- Que, mediante Resolución N° 55-UMET-CAS-SO-07-2026 el Consejo Académico Superior expidió el Reglamento para la Protección de la Privacidad, de la Información y de los Datos Personales, instrumento de carácter general, transversal e integrador, que constituye la base normativa unificada de la institución en estas materias y que comprende el Sistema Institucional de Protección de la Privacidad, la Información y los Datos Personales —SIPPID— y el Comité Institucional de Protección de la Privacidad, la Información, los Datos Personales y de Uso Ético de la Inteligencia Artificial —CIPPIA—;
- Que, el presente Reglamento constituye el régimen normativo especial aplicable a la dimensión de inteligencia artificial dentro del marco general establecido por el Reglamento para la Protección de la Privacidad, de la Información y de los Datos Personales antes referido, con el cual se articula de manera coherente y armónica, sin sustitución, sino complementación, de los demás instrumentos institucionales aplicables;
- Que, resulta institucionalmente necesario expedir un instrumento normativo interno que regule, de manera específica, sistemática y armónica con el Reglamento para la Protección de la Privacidad, de la Información y de los Datos Personales y con el ordenamiento constitucional, legal, estatutario, reglamentario y ético vigente, las condiciones de uso, adquisición, desarrollo, despliegue, supervisión y control de los sistemas de inteligencia artificial dentro de la Universidad Metropolitana, sin sustituir las disposiciones del Código de Ética Institucional, de la Investigación y el Aprendizaje ni de las Políticas de Protección de Datos Personales, sino complementándolas;
- Que, mediante Resolución No. CR-UMET-00140-07-2026, de 24 de julio de 2026, el Consejo de Regentes emitió informe favorable sobre el proyecto y autorizó su remisión al Consejo Académico Superior para conocimiento y aprobación; y

En ejercicio de sus potestades constitucionales, legales y estatutarias, resuelve expedir el siguiente:

REGLAMENTO PARA EL USO ÉTICO, RESPONSABLE Y SEGURO DE LA INTELIGENCIA ARTIFICIAL EN LA UNIVERSIDAD METROPOLITANA

TÍTULO I

DISPOSICIONES PRELIMINARES

Capítulo I

Objeto, ámbito y finalidad

Artículo 1.- Objeto. El presente Reglamento tiene por objeto establecer los principios, reglas, procedimientos, deberes, prohibiciones, prácticas permitidas y mecanismos de supervisión y control aplicables al desarrollo, adquisición, contratación, implementación, despliegue, uso, evaluación y retiro de sistemas de inteligencia artificial en la Universidad Metropolitana. Asimismo, tiene por finalidad habilitar, orientar y promover sus usos legítimos, seguros, éticos, responsables y pertinentes para el fortalecimiento de las funciones académicas, investigativas, administrativas y de gestión institucional.

Este instrumento constituye la norma institucional especial en materia de inteligencia artificial y se aplicará de manera articulada, complementaria y armónica con el Reglamento de Privacidad de la Universidad Metropolitana (“el Reglamento de Privacidad”), el Código de Ética Institucional, de la Investigación y el Aprendizaje, las Políticas de Protección de Datos Personales y los demás instrumentos internos aplicables.

Artículo 2.- Ámbito material. Las disposiciones de este Reglamento son de cumplimiento obligatorio respecto de todo sistema de inteligencia artificial que sea desarrollado, adquirido, contratado, implementado, desplegado, utilizado, autorizado, financiado, auspiciado o promovido por la Universidad Metropolitana, así como respecto de todo uso institucional o asociado a la actividad universitaria que se realice de tales sistemas, con independencia de su ubicación tecnológica, del modelo de prestación, del proveedor, del país de origen o de su modalidad de acceso gratuita, de pago, propietaria, institucional, experimental o financiada con recursos de proyectos de investigación, desarrollo e innovación.

Para efectos de su aplicación, el presente Reglamento distingue entre:

- a) Las capacidades de inteligencia artificial incorporadas por proveedores externos en herramientas de uso ordinario, tales como herramientas ofimáticas, plataformas de colaboración, videoconferencia u otros servicios tecnológicos contratados, respecto de cuyo diseño, entrenamiento, modelos, filtros o funcionamiento técnico interno la Universidad no ejerce control; y,

- b) El uso institucional que las autoridades, el personal, los estudiantes y los terceros vinculados a la Universidad hagan de dichas capacidades y de los demás sistemas de inteligencia artificial.

La regulación de este Reglamento se concentra en las actividades descritas en el literal b). Sin perjuicio de ello, la existencia de una funcionalidad de inteligencia artificial dentro de una herramienta contratada por la Universidad no habilita por sí sola su uso irrestricto, ni exonera a los usuarios de observar sus deberes éticos, jurídicos, de confidencialidad y de protección de datos personales.

Artículo 3.- Ámbito subjetivo. Este Reglamento se aplica, sin distinción de jerarquía, función, sede o modalidad de vinculación, a todas las personas que integran la Comunidad Universitaria de la Universidad Metropolitana, conforme la definición prevista en el Estatuto Institucional, en el Reglamento de Privacidad, en el Código de Ética Institucional, de la Investigación y el Aprendizaje, comprendiendo, en particular:

- a) Las Primeras Autoridades, las autoridades académicas y administrativas, los directivos académicos y administrativos, los miembros del Consejo Académico Superior y del Consejo de Regentes, los promotores institucionales y demás autoridades;
- b) El personal académico, en sus distintas categorías, dedicaciones, escalafones y modalidades, incluidos los investigadores y el personal técnico docente;
- c) El personal administrativo, sin distinción del régimen jurídico de su vinculación;
- d) Los estudiantes de las carreras técnico-tecnológicas, de grado, de posgrado y de educación continua, en cualquier modalidad, así como los estudiantes en movilidad académica;
- e) Los aspirantes, postulantes, pasantes, practicantes, becarios, asistentes de investigación, docentes invitados y colaboradores en proyectos institucionales;
- f) Las personas naturales o jurídicas, nacionales o extranjeras, que en virtud de convenios, contratos, alianzas o relaciones de cooperación con la Universidad Metropolitana intervengan en el tratamiento de información o datos personales vinculados a la actividad institucional; y,
- g) Toda persona que, sin estar comprendida en los literales anteriores, acceda, trate o conozca información institucional o datos personales en el marco de actividades auspiciadas, financiadas, autorizadas o reconocidas por la Universidad Metropolitana.

Artículo 4.- Ámbito territorial. Este Reglamento será aplicable en todas las sedes de la Universidad Metropolitana, así como en sus extensiones, escenarios académicos, centros de apoyo, entornos virtuales institucionales y, en general, en cualquier ubicación física o digital en la que se desarrollen actividades universitarias, dentro o fuera del territorio nacional.

Artículo 5.- Finalidades. Son finalidades del presente Reglamento:

- a) Reconocer y promover el espíritu fundacional de la Universidad Metropolitana, orientado a la innovación tecnológica, habilitando y fomentando usos legítimos, seguros, pertinentes e innovadores de la inteligencia artificial en las funciones sustantivas y adjetivas;
- b) Garantizar que el uso institucional y comunitario de la inteligencia artificial respete la dignidad humana, los derechos fundamentales, los principios constitucionales, la ética universitaria, la libertad de cátedra, la libertad de investigación y la integridad académica;
- c) Delimitar y orientar los temas prioritarios de regulación ética del uso de la inteligencia artificial, en particular la transparencia, la responsabilidad humana, la protección de datos personales, la seguridad de la información, la no discriminación, la integridad académica, la trazabilidad, la supervisión institucional y la prevención de usos indebidos;
- d) Asegurar el cumplimiento del régimen ecuatoriano de protección de datos personales en todo tratamiento que se efectúe por o a través de sistemas de inteligencia artificial;
- e) Articular la gobernanza, supervisión y control de los sistemas de inteligencia artificial con el Sistema Institucional de Protección de la Privacidad, la Información y los Datos Personales, establecido por el Reglamento de Privacidad, bajo un enfoque basado en riesgos;
- f) Prevenir, identificar, mitigar y remediar los riesgos jurídicos, éticos, académicos, científicos, laborales, patrimoniales, reputacionales, de seguridad de la información y de protección de datos personales asociados a la inteligencia artificial;
- g) Promover el uso pedagógicamente apropiado, científicamente riguroso, técnicamente seguro y administrativamente eficiente de la inteligencia artificial como herramienta de apoyo a las funciones universitarias;
- h) Salvaguardar la integridad académica y la honestidad intelectual frente a usos indebidos de la inteligencia artificial, en complemento del Código de Ética Institucional, de la Investigación y el Aprendizaje; y,
- i) Establecer mecanismos de transparencia, rendición de cuentas, trazabilidad documental y auditabilidad respecto del uso institucional de sistemas de inteligencia artificial.

Artículo 6.- Especialidad, articulación y complementariedad normativa. El presente Reglamento constituye el régimen normativo especial aplicable al desarrollo, adquisición, contratación, implementación, despliegue, uso, evaluación y retiro de sistemas de inteligencia artificial en la Universidad Metropolitana.

Los aspectos generales relativos a privacidad, protección de datos personales, derechos de los titulares, seguridad de la información, clasificación de la información, confidencialidad, gestión de riesgos y responsabilidades institucionales se regirán por el Reglamento de Privacidad. Las disposiciones del presente Reglamento se aplicarán de manera preferente respecto de las materias específicas de inteligencia artificial, sin contradecir ni sustituir las reglas generales previstas en dicho instrumento.

Este Reglamento se aplicará, además, de manera complementaria y armónica con el Código de Ética Institucional, de la Investigación y el Aprendizaje, las Políticas de Protección de Datos Personales, el Reglamento que regula el Procedimiento Disciplinario para Estudiantes, Profesores e Investigadores, el Reglamento Interno de Trabajo y los demás reglamentos y normas internas aplicables.

En caso de concurrencia normativa, se observarán los principios de jerarquía, especialidad, complementariedad y aplicación más favorable a la protección de los derechos fundamentales, la integridad académica, la seguridad de la información y los intereses institucionales legítimos.

Artículo 7.- Jerarquía normativa. El presente Reglamento se interpretará y aplicará en consonancia con la Constitución de la República del Ecuador, los instrumentos internacionales de derechos humanos ratificados por el Ecuador, la Ley Orgánica de Educación Superior, la Ley Orgánica de Protección de Datos Personales y su Reglamento General, la Ley Orgánica para la Transformación Digital y Audiovisual y su Reglamento, la normativa secundaria expedida por la Superintendencia de Protección de Datos Personales y por el órgano rector de la transformación digital, el Reglamento de Privacidad, así como las demás disposiciones del ordenamiento jurídico ecuatoriano. Las referencias a normas externas deberán entenderse hechas a las disposiciones vigentes en cada momento de aplicación.

Capítulo II

Principios rectores

Artículo 8.- Principios rectores. El desarrollo, adquisición, contratación, implementación, despliegue, uso, supervisión y retiro de sistemas de inteligencia artificial dentro de la Universidad Metropolitana se rigen por los principios establecidos en el Reglamento de Privacidad y, complementariamente, por los siguientes principios específicos, interpretados de manera sistemática, integradora y conforme al ordenamiento jurídico vigente:

- a) **Dignidad humana y centralidad de la persona:** todo sistema de inteligencia artificial será concebido, implementado y utilizado como herramienta al servicio del ser humano, respetando su dignidad, autonomía e integridad y nunca como

sustituto del juicio humano en decisiones que afecten significativamente los derechos, intereses, formación o trayectoria de las personas.

- b) **Legalidad:** todo uso institucional de inteligencia artificial se sujetará al marco constitucional, legal, estatutario, reglamentario y ético aplicable, sin que la novedad o complejidad técnica del sistema constituya causal eximente del cumplimiento normativo.
- c) **Habilitación e innovación responsable:** la Universidad reconoce, habilita y promueve los usos legítimos, seguros y pertinentes de la inteligencia artificial; la regulación se orienta a posibilitar la innovación bajo condiciones de responsabilidad, y no únicamente a restringir.
- d) **Enfoque basado en riesgos:** las obligaciones aplicables a los sistemas de inteligencia artificial serán proporcionales al nivel de riesgo que estos representen para los derechos, libertades, intereses y bienes jurídicos protegidos, conforme a la clasificación contenida en el Título III del presente Reglamento.
- e) **Protección de datos personales:** todo tratamiento de datos personales realizado mediante sistemas de inteligencia artificial respetará íntegramente los principios y derechos consagrados en la Ley Orgánica de Protección de Datos Personales, su Reglamento General, la normativa secundaria de la Superintendencia de Protección de Datos Personales, el Reglamento de Privacidad y las Políticas de Protección de Datos Personales de la Universidad Metropolitana.
- f) **Privacidad desde el diseño y por defecto:** los sistemas de inteligencia artificial incorporarán, desde su concepción y de manera predeterminada, las medidas técnicas, organizativas y jurídicas necesarias para proteger los datos personales y minimizar los riesgos para los titulares.
- g) **Supervisión humana significativa:** todo sistema de inteligencia artificial que pueda producir efectos jurídicos, académicos, laborales, disciplinarios, financieros, sanitarios o administrativos relevantes sobre las personas estará sometido a supervisión humana efectiva, oportuna y dotada de capacidad real de intervención, modificación o anulación de las decisiones automatizadas.
- h) **Transparencia y explicabilidad:** los sistemas de inteligencia artificial utilizados en la Universidad Metropolitana operarán bajo condiciones de transparencia respecto de su existencia, finalidad, características, lógica de funcionamiento, limitaciones y posibles consecuencias, en términos comprensibles para los usuarios y los afectados.
- i) **No discriminación y equidad:** el desarrollo y uso de sistemas de inteligencia artificial evitará la generación, perpetuación o amplificación de sesgos, exclusiones o discriminaciones por razón de origen étnico, género, identidad de género, orientación sexual, discapacidad, nacionalidad, edad, condición

socioeconómica, convicciones religiosas, filiación política o cualquier otra condición protegida.

- j) **Integridad académica y honestidad intelectual:** el uso de inteligencia artificial dentro de las actividades académicas, evaluativas, investigativas y de producción intelectual respetará los principios de autoría personal, originalidad, atribución de fuentes y rigor metodológico, en los términos del Código de Ética Institucional, de la Investigación y el Aprendizaje.
- k) **Seguridad de la información y resiliencia:** los sistemas de inteligencia artificial estarán protegidos por medidas técnicas y organizativas adecuadas que garanticen su confidencialidad, integridad, disponibilidad, autenticidad y resiliencia frente a errores, fallos, ataques o usos malintencionados, conforme al Sistema de Gestión de Seguridad de la Información del Reglamento de Privacidad.
- l) **Trazabilidad y auditabilidad:** el ciclo de vida de los sistemas de inteligencia artificial utilizados institucionalmente será documentado de manera suficiente para permitir su auditoría, evaluación y revisión por parte de las instancias internas y de las autoridades de control competentes.
- m) **Rendición de cuentas y responsabilidad proactiva:** las autoridades, unidades y personas responsables del uso institucional de inteligencia artificial deberán demostrar, mediante evidencia verificable, el cumplimiento de las obligaciones derivadas de este Reglamento, del Reglamento de Privacidad, de la normativa de protección de datos personales y del marco ético aplicable.
- n) **Interés superior del niño y de la adolescencia:** todo tratamiento de datos personales o aplicación de inteligencia artificial que involucre a niños o adolescentes observará, de manera reforzada, el interés superior del niño, conforme a la Constitución, los instrumentos internacionales de derechos humanos y la legislación ecuatoriana.
- o) **Sostenibilidad:** se considerará el impacto ambiental, social y económico del ciclo de vida de los sistemas de inteligencia artificial, privilegiando soluciones coherentes con los compromisos institucionales en materia de sostenibilidad y responsabilidad ambiental.
- p) **Cooperación y diálogo de saberes:** el uso de inteligencia artificial en la Universidad Metropolitana respetará la diversidad cultural, epistémica y lingüística y no podrá emplearse de modo que sustituya, invisibilice o subordine los conocimientos colectivos, los saberes ancestrales o las tradiciones científicas y humanísticas que forman parte del quehacer universitario.
- q) **Proporcionalidad y minimización:** los sistemas de inteligencia artificial se utilizarán únicamente en la medida en que sean adecuados, necesarios y proporcionales para los fines institucionales perseguidos y los datos personales tratados se reducirán al mínimo indispensable para tales fines.

- r) **Interpretación más favorable:** ante dudas razonables sobre la interpretación de este Reglamento, prevalecerá la opción que ofrezca mayor protección a los derechos fundamentales, a la integridad académica y a la dignidad de las personas afectadas por el uso del sistema de inteligencia artificial.

Capítulo III

Planos de uso, reglas comunes y salvaguardas

Artículo 9.- Planos de uso de la inteligencia artificial. La regulación del presente Reglamento se concentra en el uso institucional de la inteligencia artificial y no en el control técnico del diseño, entrenamiento o funcionamiento interno de los sistemas administrados o controlados por proveedores externos. Sin perjuicio de ello, la UMET regula el uso que los miembros de la Comunidad Universitaria hagan de tales capacidades y sistemas, especialmente cuando puedan comprometer información institucional, académica, financiera, estratégica, reservada o datos personales.

En consecuencia, queda sujeto a este Reglamento el ingreso, carga, copia, procesamiento o comunicación, en sistemas de inteligencia artificial, de datos personales, información confidencial, información reservada o estratégica, documentos institucionales no públicos o expedientes académicos, financieros, laborales, disciplinarios o contractuales, salvo que exista habilitación expresa, base jurídica suficiente, autorización institucional y garantías adecuadas de seguridad, confidencialidad y protección de datos.

Artículo 10.- Reglas comunes e independencia de la modalidad de acceso. El régimen aplicable a un sistema de inteligencia artificial no depende de si la herramienta es gratuita, de pago, propietaria, institucional, experimental o financiada con recursos de proyectos de investigación, desarrollo e innovación, sino del tipo de uso, de la información tratada, del nivel de riesgo y del grado de control institucional existente. Sin perjuicio de las reglas reforzadas aplicables a las herramientas que procesen información sensible, confidencial, institucional o datos personales, todo uso de inteligencia artificial observará, al menos, las siguientes reglas comunes mínimas:

- a) Autorización institucional previa para los usos de alto riesgo, conforme al presente Reglamento;
- b) Prohibición de ingresar información no pública o datos personales en herramientas no autorizadas;
- c) Evaluación de riesgos cuando se utilicen herramientas de inteligencia artificial en proyectos de investigación, desarrollo e innovación;
- d) Trazabilidad del uso cuando exista impacto académico, administrativo o investigativo relevante; y,
- e) Responsabilidad del usuario por el uso ético, seguro y legal de la herramienta empleada.

Artículo 11.- Salvaguardas del proveedor y deberes institucionales y personales. Se reconoce que diversas plataformas y aplicaciones de inteligencia artificial incorporan mecanismos propios de mitigación de riesgos, tales como filtros de contenido, restricciones de uso, políticas de seguridad, controles contra la generación de contenidos dañinos, medidas de moderación, configuraciones de privacidad, registros de actividad y condiciones contractuales.

Para evitar atribuir a la Universidad obligaciones que corresponden al diseño técnico de las herramientas, sin debilitar su responsabilidad de regular el uso, se distinguen:

- a) Las salvaguardas técnicas incorporadas por el proveedor;
- b) Las condiciones de uso y políticas contractuales de la plataforma;
- c) Los controles institucionales de autorización, trazabilidad y supervisión; y,
- d) Los deberes del usuario final.

La existencia de salvaguardas del proveedor no sustituye ni desplaza los deberes institucionales y personales de uso responsable, confidencialidad, protección de datos personales, seguridad de la información e integridad académica.

TÍTULO II

GOBERNANZA INSTITUCIONAL DE LA INTELIGENCIA ARTIFICIAL

Capítulo I

Articulación con el SIPPID

Artículo 12.- Gobernanza dentro del SIPPID. La gobernanza institucional del uso, desarrollo, adquisición, contratación, despliegue, supervisión y control de los sistemas de inteligencia artificial en la Universidad Metropolitana se ejerce dentro del Sistema Institucional de Protección de la Privacidad, la Información y los Datos Personales — SIPPID— establecido por el Reglamento de Privacidad. El presente Reglamento constituye el régimen normativo especial aplicable a la dimensión de inteligencia artificial dentro de dicho Sistema.

Artículo 13.- Articulación funcional. La integración, los componentes, los principios de funcionamiento y las atribuciones generales del SIPPID son los establecidos en el Reglamento de Privacidad. Las instancias del SIPPID ejercen, sobre la dimensión de inteligencia artificial, las funciones que les corresponden de manera articulada y bajo el principio de unidad institucional, en concordancia con las especificaciones contenidas en el presente Reglamento, sin que ello suponga crear competencias nuevas ni duplicar las ya previstas en el orgánico funcional.

Artículo 14.- Principio de unidad institucional. Las instancias del Sistema Institucional actuarán de manera coordinada, articulada y bajo el principio de unidad institucional. Los criterios técnicos, jurídicos, éticos y operativos emitidos por las

instancias competentes vincularán a las demás unidades en sus respectivos ámbitos, sin perjuicio de las competencias propias que el ordenamiento, el Estatuto y el Reglamento General al Estatuto atribuyen a cada órgano, autoridad, dirección o responsable funcional.

Capítulo II

Comité Institucional

Artículo 15.- Comité competente. El órgano competente para la articulación, coordinación, seguimiento y gobierno de la dimensión de inteligencia artificial es el Comité Institucional de Protección de la Privacidad, la Información, los Datos Personales y de Uso Ético de la Inteligencia Artificial —CIPPIA—, cuya naturaleza, integración, sesiones, *quórum* y régimen de confidencialidad son los regulados por el Reglamento de Privacidad. El Comité no sustituye ni desplaza las competencias propias del

Vicerrectorado Administrativo, de la Dirección de Tecnologías Informáticas, del Especialista en Cumplimiento, del Delegado de Protección de Datos Personales, de la Procuraduría Nacional ni del Comité Universitario de Ética.

Artículo 16.- Atribuciones específicas del Comité en materia de inteligencia artificial. Sin perjuicio de las funciones generales que le atribuye el Reglamento de Privacidad, el Comité ejerce, en materia de inteligencia artificial, las siguientes atribuciones específicas, concentradas en el gobierno, la coordinación y el seguimiento del sistema, sin asumir la ejecución que corresponde a las áreas competentes:

1. Aprobar o proponer, según corresponda, los lineamientos, directrices, guías, formularios y plantillas para la implementación operativa del presente Reglamento, asegurando su coherencia con los instrumentos generales del SIPPID;
2. Coordinar la distribución de responsabilidades institucionales en materia de inteligencia artificial entre las autoridades, direcciones y responsables funcionales competentes;
3. Mantener actualizado, con apoyo de las áreas competentes, el Inventario Institucional de Sistemas de Inteligencia Artificial, articulándolo con el Inventario de Activos de Información del Reglamento general;
4. Validar la clasificación de los sistemas de inteligencia artificial conforme al enfoque basado en riesgos del Título III y revisar periódicamente dicha clasificación;
5. Revisar los indicadores y métricas de desempeño de la dimensión de inteligencia artificial y supervisar los riesgos asociados;

6. Emitir criterio previo no vinculante respecto de los proyectos de adquisición, contratación, desarrollo o despliegue de sistemas de inteligencia artificial calificados de alto riesgo;
7. Articular las acciones correctivas y de mejora continua frente a incidentes, desviaciones o riesgos identificados;
8. Recibir y canalizar las consultas, alertas, denuncias y reportes vinculados al uso institucional de inteligencia artificial, en articulación con los procedimientos generales del SIPPID;
9. Promover, en coordinación con las unidades competentes, las acciones de capacitación, sensibilización y alfabetización en inteligencia artificial;
10. Elevar al Rector y al Consejo Académico Superior los reportes y el acápite específico de inteligencia artificial dentro del informe anual integrado de seguimiento del SIPPID;
11. Coordinar con el Comité Universitario de Ética y sus Subcomités de Ética de Sede en los asuntos en que confluyan dimensiones éticas; y,
12. Proponer al Consejo Académico Superior, a través del Rector, las reformas y actualizaciones del presente Reglamento.

En todos los casos el Comité gobierna, coordina y supervisa; las áreas técnicas ejecutan en el ámbito de sus competencias; el Delegado de Protección de Datos Personales asesora y verifica en su materia; la Dirección de Tecnologías Informáticas administra los controles técnicos viables; el Especialista en Cumplimiento realiza el seguimiento del cumplimiento; la Procuraduría Nacional emite criterio jurídico no vinculante cuando corresponda; y, el Comité Universitario de Ética conoce los asuntos éticos de su competencia.

Artículo 17.- Régimen de funcionamiento. El régimen de funcionamiento del Comité, incluida la convocatoria, conducción de sesiones, deliberación, votación, levantamiento de actas, custodia documental y archivo, así como los deberes de confidencialidad, son los previstos en el Reglamento de Privacidad. Las decisiones del Comité en materia de inteligencia artificial gozarán de igual eficacia institucional que aquellas adoptadas en el ámbito general del SIPPID.

Artículo 18.- Confidencialidad reforzada en asuntos sensibles. Sin perjuicio del régimen general de confidencialidad previsto en el Reglamento de Privacidad, los miembros del Comité, sus alternos, secretarios e invitados observarán confidencialidad reforzada cuando, en el conocimiento de asuntos relacionados con sistemas de inteligencia artificial, tengan acceso a información reservada o estratégica institucional, código fuente, modelos, datos de entrenamiento, evaluaciones disciplinarias o académicas en curso o información sensible o delicada en los términos del citado Reglamento.

Capítulo III

Roles institucionales en materia de inteligencia artificial

Artículo 19.- Autoridad interna responsable del Tratamiento. El Vicerrector Administrativo, en su calidad de autoridad interna responsable del Tratamiento de Datos Personales reconocida en el Estatuto Institucional, en el Reglamento General al Estatuto y en el Reglamento de Privacidad, asumirá la coordinación de la aplicación del presente Reglamento en sus dimensiones de protección de datos personales, sin perjuicio de la responsabilidad indelegable de la Universidad Metropolitana frente a los titulares, la sociedad y el Estado.

Artículo 20.- Delegado de Protección de Datos Personales. El Delegado de Protección de Datos Personales ejercerá sus funciones con independencia técnica y funcional y actuará como instancia de asesoría, supervisión, vigilancia, alerta y recomendación especializada respecto de los tratamientos de datos personales efectuados mediante sistemas de inteligencia artificial.

En particular, le corresponderá:

- a) Asesorar al Vicerrectorado Administrativo, al Comité Institucional y a las unidades académicas, administrativas y tecnológicas sobre el cumplimiento de la normativa de protección de datos personales aplicable a los sistemas de inteligencia artificial;
- b) Supervisar y emitir recomendaciones respecto de la identificación de bases jurídicas, el cumplimiento de los deberes de información, la atención de los derechos de los titulares y la aplicación de los principios de privacidad desde el diseño y por defecto;
- c) Asesorar y supervisar la elaboración de las Evaluaciones de Impacto del Tratamiento y emitir las recomendaciones técnicas que correspondan, sin asumir su ejecución operativa ni su aprobación;
- d) Supervisar la incorporación y actualización de los tratamientos efectuados mediante sistemas de inteligencia artificial en el Registro de Actividades de Tratamiento y recomendar las medidas correctivas necesarias;
- e) Emitir criterios y recomendaciones respecto de las transferencias nacionales o internacionales de datos personales asociadas al uso de sistemas de inteligencia artificial;
- f) Supervisar la gestión de incidentes que involucren datos personales y recomendar las medidas de contención, corrección, notificación y prevención que correspondan;

- g) Cooperar con la Superintendencia de Protección de Datos Personales y actuar como punto de contacto institucional en los asuntos comprendidos dentro de sus competencias; y,
- h) Elaborar informes, alertas y recomendaciones sobre el nivel de cumplimiento institucional en materia de protección de datos personales y uso de inteligencia artificial.

El Delegado no determinará los fines y medios del tratamiento, no decidirá sobre la procedencia de las solicitudes de los titulares, no aprobará Evaluaciones de Impacto, transferencias, tratamientos o sistemas de inteligencia artificial y no asumirá funciones operativas o de ejecución directa propias del responsable del tratamiento, de los encargados, de la Dirección de Tecnologías Informáticas, de las unidades tratantes o de las demás instancias institucionales competentes. Su intervención no sustituirá las decisiones ni responsabilidades que correspondan a dichas autoridades y unidades.

Artículo 21.- Dirección de Tecnologías Informáticas. Corresponde a la Dirección de Tecnologías Informáticas intervenir en la evaluación, habilitación, configuración, integración, control de accesos, seguridad y monitoreo técnicamente disponible de los sistemas de inteligencia artificial institucionalmente adoptados; administrar usuarios y copias de respaldo; emitir criterios técnicos sobre el uso de funcionalidades de inteligencia artificial incorporadas en plataformas contratadas por la Universidad; y coordinar los controles institucionales con el Comité, el Delegado de Protección de Datos Personales, el Especialista en Cumplimiento y las áreas usuarias.

La Dirección de Tecnologías Informáticas no es responsable de controlar el diseño, funcionamiento interno, entrenamiento, filtros, modelos o salvaguardas técnicas de las capacidades de inteligencia artificial incorporadas por proveedores externos en herramientas de uso ordinario, sin perjuicio de su responsabilidad en la administración tecnológica, la seguridad de la información, la gestión de usuarios, el monitoreo disponible, las copias de respaldo, los lineamientos de uso seguro y la evaluación técnica de herramientas.

Artículo 22.- Especialista en Cumplimiento. El Especialista en Cumplimiento ejercerá, dentro del ámbito del presente Reglamento, funciones de seguimiento, verificación, alerta y evaluación del cumplimiento normativo en materia de inteligencia artificial, conforme a las atribuciones previstas en el Reglamento General al Estatuto y sin asumir funciones operativas cuya regularidad deba posteriormente controlar.

En particular, le corresponderá:

- a) Verificar el grado de cumplimiento de las obligaciones establecidas en este Reglamento y en los instrumentos institucionales relacionados;

- b) Proponer, con base en los riesgos identificados, el programa anual de revisión y control de la dimensión de inteligencia artificial;
- c) Dar seguimiento a la ejecución de las revisiones, auditorías y evaluaciones dispuestas por la autoridad competente;
- d) Verificar el cumplimiento de los planes de acción, medidas correctivas y recomendaciones emitidas como resultado de auditorías, revisiones o incidentes;
- e) Emitir alertas e informes sobre desviaciones, incumplimientos, riesgos o debilidades de control identificadas;
- f) Coordinar el flujo de información necesario para las actividades de revisión y control, sin intervenir en la ejecución material de los procesos evaluados; y,
- g) Informar al Comité Institucional, al Rector y a las autoridades competentes sobre los resultados del seguimiento realizado.

Las auditorías, revisiones técnicas o evaluaciones independientes serán ejecutadas por equipos técnicos *ad hoc* que no hayan intervenido en los procesos objeto de examen o por auditores externos especializados, según la naturaleza y complejidad del asunto. El Especialista en Cumplimiento no podrá auditar, revisar ni calificar actuaciones en cuya planificación, ejecución, aprobación o implementación haya participado directamente.

Artículo 23.- Procuraduría Nacional. La Procuraduría Nacional asesorará jurídicamente a las autoridades, órganos colegiados y unidades en la aplicación e interpretación del presente Reglamento, intervendrá en la revisión de las cláusulas contractuales relativas a sistemas de inteligencia artificial, emitirá criterio jurídico no vinculante en los casos previstos en este Reglamento y patrocinará a la Universidad en los asuntos administrativos, judiciales o constitucionales que se deriven del uso institucional de inteligencia artificial.

Artículo 24.- Responsables operativos. Cada autoridad académica o administrativa, decano, director de escuela, coordinador de carrera, director departamental, director de sede o responsable de unidad será responsable, en su ámbito funcional, de la observancia del presente Reglamento por parte del personal y los estudiantes a su cargo, así como de la documentación, supervisión y control del uso de sistemas de inteligencia artificial bajo su responsabilidad funcional.

Artículo 25.- Comunidad Universitaria. Toda persona integrante de la Comunidad Universitaria será responsable, en el ámbito de sus actividades, del uso ético, lícito, transparente y diligente de los sistemas de inteligencia artificial, conforme a los principios y reglas del presente Reglamento, del Reglamento de Privacidad, del Código de Ética Institucional, de la Investigación y el Aprendizaje y de las Políticas de Protección de Datos Personales.

TÍTULO III

CLASIFICACIÓN DE LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL POR NIVEL DE RIESGO

Capítulo I

Enfoque general

Artículo 26.- Enfoque basado en riesgos. Los sistemas de inteligencia artificial utilizados, contratados o desarrollados por la Universidad Metropolitana se clasifican, conforme a su impacto potencial sobre los derechos, libertades, intereses y bienes jurídicos protegidos, en cinco niveles:

- a) Prácticas fomentadas y permitidas;
- b) Prácticas prohibidas;
- c) Sistemas de alto riesgo;
- d) Sistemas de riesgo limitado; y,
- e) Sistemas de riesgo mínimo.

Esta clasificación servirá de base para determinar las obligaciones aplicables conforme al presente Reglamento y atenderá al tipo de uso, a la información tratada y al grado de control institucional, antes que a la modalidad de acceso o financiamiento de la herramienta.

Artículo 27.- Inventario Institucional de Sistemas. La Universidad Metropolitana mantendrá un Inventario Institucional de Sistemas de Inteligencia Artificial, coordinado por el Comité y articulado con el Inventario de Activos de Información del Reglamento de Privacidad, en el que se registrarán, al menos, la denominación del sistema, su proveedor o desarrollador, su finalidad institucional, las unidades que lo utilizan, las categorías de datos personales tratadas, su clasificación por nivel de riesgo, la fecha de incorporación, la documentación técnica disponible, los responsables operativos y las observaciones relevantes en materia de seguridad, privacidad y ética. El Inventario se actualizará al menos semestralmente, sin perjuicio de las actualizaciones inmediatas que requieran las altas, modificaciones o bajas de sistemas.

Artículo 28.- Calificación de riesgo. La calificación inicial de riesgo de un sistema de inteligencia artificial será propuesta por la unidad o área requirente que lo solicita, contrata o despliega y será validada por el Comité, con intervención del Delegado de Protección de Datos Personales cuando el sistema implique tratamiento de datos personales. La calificación podrá ser revisada cuando varíen las condiciones técnicas, normativas o de uso del sistema. La calificación de un sistema como de alto riesgo obliga a adoptar las salvaguardas correspondientes y no constituye, por sí sola, causal automática de no adquisición.

Capítulo II

Prácticas permitidas, fomentadas y prohibidas

Artículo 29.- Prácticas permitidas y fomentadas. La Universidad Metropolitana reconoce, habilita y promueve el uso de la inteligencia artificial como herramienta de apoyo a las funciones sustantivas y adjetivas, siempre que se respeten la protección de datos personales, la confidencialidad, la seguridad de la información, la integridad académica, la propiedad intelectual, la supervisión humana y las autorizaciones institucionales aplicables. Se reconocen como prácticas permitidas y fomentadas, entre otras:

- a) El apoyo en la elaboración de borradores, resúmenes, matrices, presentaciones, informes preliminares y documentos de trabajo, siempre sujetos a revisión humana;
- b) La asistencia en actividades académicas, investigativas y de innovación, sin sustitución del criterio docente, académico o científico;
- c) El análisis de información pública, anonimizada o previamente autorizada;
- d) La mejora de procesos administrativos, la atención al usuario, la organización documental y la automatización de tareas repetitivas;
- e) La generación de materiales de apoyo pedagógico, recursos de accesibilidad, traducción, corrección lingüística y adaptación de contenidos;
- f) El apoyo en programación, análisis de datos, simulaciones y visualización de información, cuando no se comprometan datos personales o información confidencial;
- g) El uso de herramientas institucionalmente autorizadas para ciberseguridad, detección de riesgos, gestión documental y mejora continua; y,
- h) Cualquier otro uso legítimo, proporcional y trazable que contribuya al cumplimiento de los fines universitarios, siempre que respete la confidencialidad, la protección de datos personales, la propiedad intelectual, la integridad académica, la seguridad de la información, la supervisión humana y las autorizaciones institucionales aplicables.

Artículo 30.- Prácticas prohibidas. Sin perjuicio de las prohibiciones contenidas en la Constitución, la Ley Orgánica de Protección de Datos Personales, el Reglamento de Privacidad, el Código de Ética Institucional, de la Investigación y el Aprendizaje y demás normativa aplicable, queda expresamente prohibido el desarrollo, adquisición, contratación, implementación, despliegue o uso institucional, dentro de la Universidad Metropolitana, de sistemas de inteligencia artificial cuya finalidad o efecto principal sea:

- a) Manipular subliminalmente, mediante técnicas que escapen al control consciente de las personas, su comportamiento, decisiones, opiniones o convicciones, en

forma que pueda causarles perjuicio físico, psicológico, académico, laboral o patrimonial;

- b) Explotar las vulnerabilidades de personas o grupos asociadas a su edad, discapacidad, condición socioeconómica o cualquier otra circunstancia análoga, con el fin de alterar materialmente su conducta o decisiones, en forma que les cause o pueda causarles perjuicio;
- c) Clasificar o calificar a las personas con base en su comportamiento social, características personales o de personalidad, con la finalidad o el efecto de generar consecuencias desfavorables, desproporcionadas o inconexas respecto del contexto en que los datos fueron recogidos;
- d) Realizar valoraciones predictivas de la comisión de infracciones disciplinarias, académicas o de cualquier otra naturaleza basadas exclusivamente en la elaboración de perfiles, en rasgos de personalidad o en categorías protegidas;
- e) Inferir emociones, estados afectivos o estados de salud mental de los miembros de la Comunidad Universitaria en contextos académicos, laborales de evaluación, salvo cuando exista habilitación legal expresa, finalidad médica o de seguridad estrictamente justificada y se cuente con consentimiento libre, informado y específico, así como con las garantías técnicas, éticas y jurídicas pertinentes;
- f) Categorizar biométricamente a las personas para inferir o deducir su origen étnico, sus convicciones políticas, religiosas o filosóficas, su afiliación sindical, sus datos de salud, su vida o su orientación sexuales;
- g) Realizar identificación biométrica remota, masiva o indiscriminada en espacios universitarios o de acceso público, salvo en supuestos estrictamente excepcionales, debidamente habilitados por la ley, con base jurídica específica, autorizados por la autoridad competente y sometidos a las garantías pertinentes;
- h) Tomar decisiones jurídicamente vinculantes, con efectos significativos sobre derechos académicos, laborales, disciplinarios, financieros o sanitarios de las personas, basadas única o predominantemente en valoraciones automatizadas, sin posibilidad real de intervención humana significativa;
- i) Generar, replicar o difundir contenidos deliberadamente engañosos, desinformación, suplantaciones de identidad, hipertrucajes o contenidos sintéticos que puedan inducir a error sobre la autoría o veracidad de hechos, declaraciones, imágenes o producciones académicas y científicas;
- j) Producir, distribuir o utilizar contenidos sintéticos que vulneren la integridad sexual, el honor, la imagen, la intimidad o la dignidad de las personas, en particular cuando se trate de niños y adolescentes;
- k) Sustituir, automatizar o reemplazar de manera ilegítima la autoría, el razonamiento, la redacción o la evaluación que deban reflejar el dominio personal del autor en actividades académicas, evaluativas, investigativas o de producción

intelectual, conforme a las prohibiciones del Código de Ética Institucional, de la Investigación y el Aprendizaje;

- l) Desplegar, dentro o desde la Universidad Metropolitana, sistemas cuyo propósito sea facilitar el fraude académico, el plagio o la vulneración de la propiedad intelectual; y,
- m) Cualquier otro uso que vulnere los principios constitucionales, los derechos fundamentales, la ética universitaria o el ordenamiento jurídico aplicable.

Artículo 31.- Consecuencias de las prácticas prohibidas. La realización de cualquiera de las prácticas prohibidas previstas en el artículo precedente dará lugar a la suspensión inmediata del uso o despliegue del sistema de inteligencia artificial involucrado y, cuando corresponda, a su bloqueo, desinstalación, retiro o inhabilitación preventiva, sin perjuicio de las medidas necesarias para preservar evidencias, contener riesgos y proteger a las personas afectadas.

La determinación de responsabilidades y la imposición de sanciones se sujetarán al régimen ético, disciplinario, laboral, contractual, civil, administrativo o penal aplicable, según la calidad de la persona involucrada y la naturaleza de la conducta. Para establecer la gravedad de la infracción se considerarán, entre otros criterios, la intencionalidad, el daño causado, el nivel de riesgo generado, la naturaleza de los derechos afectados, el carácter sensible o reservado de la información comprometida, el beneficio obtenido, la reincidencia, la afectación institucional y las medidas adoptadas para contener o reparar sus efectos.

La calificación de la conducta como leve, grave o muy grave no se efectuará automáticamente por este artículo, sino conforme a la tipificación y al procedimiento previstos en el Reglamento Interno de Trabajo, el Reglamento que regula el Procedimiento Disciplinario para Estudiantes, Profesores e Investigadores, el Código de Ética Institucional, de la Investigación y el Aprendizaje, los contratos aplicables y las demás normas institucionales o legales pertinentes.

Las medidas preventivas previstas en este artículo no tendrán carácter sancionador y podrán adoptarse de manera inmediata cuando resulten necesarias para evitar la continuidad del riesgo, proteger datos personales, preservar la seguridad de la información, impedir afectaciones académicas o institucionales y asegurar la integridad de la investigación o del procedimiento correspondiente.

Capítulo III

Sistemas de alto riesgo

Artículo 32.- Sistemas de alto riesgo. Se consideran sistemas de inteligencia artificial de alto riesgo, sin perjuicio de aquellos que el Comité califique en tal condición de manera fundada, aquellos que mediante inteligencia artificial adopten o condicionen

decisiones relevantes sin intervención humana suficiente, o que se utilicen, en todo o en parte, para:

- a) La admisión, selección, calificación o asignación de cupos a estudiantes, así como la elaboración de perfiles de aspirantes con efectos materiales sobre el ingreso, la matrícula o el régimen académico;
- b) La evaluación automatizada de aprendizajes, el aprovechamiento académico, la promoción, la titulación o la deserción de estudiantes, con efectos jurídicos o significativos sobre su trayectoria académica;
- c) La detección automatizada de fraude académico, plagio o conductas atribuibles a estudiantes, profesores o investigadores, cuando sus resultados tengan o puedan tener efectos disciplinarios o académicos relevantes;
- d) La supervisión, monitoreo o vigilancia automatizada de exámenes, evaluaciones o actividades académicas, incluido el proctoring, cuando intervenga sobre dispositivos personales, espacios privados o categorías especiales de datos;
- e) La selección, evaluación de desempeño, promoción, sanción o terminación del vínculo del personal académico o administrativo, así como la asignación de cargas, distributivos o estímulos con efectos laborales o académicos relevantes;
- f) La asignación, denegación o revisión de becas, ayudas económicas, beneficios estudiantiles o financiamiento académico;
- g) La videovigilancia con análisis de comportamiento, biometría o reconocimiento facial dentro de los campus, sedes, extensiones u otros espacios universitarios;
- h) El reconocimiento, identificación o autenticación biométrica de los miembros de la Comunidad Universitaria, así como la geolocalización sistemática;
- i) El tratamiento sistemático de datos de niños y adolescentes en el contexto educativo;
- j) La elaboración de perfiles de salud, salud mental, condición socioeconómica o de cualquier otra categoría especial o sensible de datos, respecto de cualquier integrante de la Comunidad Universitaria;
- k) Las investigaciones que utilicen inteligencia artificial sobre seres humanos, datos sensibles, comunidades vulnerables o pueblos y nacionalidades indígenas;
- l) Las decisiones administrativas que generen efectos jurídicos relevantes sobre las personas o sobre el patrimonio institucional; y,
- m) Aquellos que el Comité califique como tales en virtud de su impacto potencial.

No se considerarán, por sí solas, sistemas de alto riesgo las funcionalidades ordinarias de evaluación automatizada incorporadas en las plataformas de gestión del aprendizaje, tales como cuestionarios, reactivos, retroalimentación general o por ítem, generación de reportes y personalización del aprendizaje, cuando se limiten a ejecutar criterios, rúbricas o parámetros previamente definidos por el docente o la unidad académica competente y

exista posibilidad de revisión, trazabilidad y supervisión humana. Tales funcionalidades se tratarán como herramientas ordinarias de apoyo académico.

Asimismo, los certificados automatizados, códigos únicos alfanuméricos, códigos *QR*, mecanismos de verificación digital y soluciones basadas en cadena de bloques u otros sistemas destinados a reforzar la autenticidad, trazabilidad y confiabilidad documental, incluidos los regulados por la normativa institucional aplicable al CESDEL, no serán tratados automáticamente como riesgosos, sino evaluados según su finalidad, nivel de automatización, datos tratados, efectos jurídicos o académicos y existencia de controles humanos e institucionales.

Artículo 33.- Obligaciones aplicables a los sistemas de alto riesgo. El despliegue institucional de un sistema de inteligencia artificial calificado como de alto riesgo requerirá, además de las obligaciones generales aplicables conforme al presente Reglamento y al Reglamento de Privacidad:

1. La realización previa de una Evaluación de Impacto del Tratamiento de Datos Personales, cuando el sistema implique tratamiento de tales datos, conforme a la normativa de la Superintendencia de Protección de Datos Personales y a los procedimientos internos de la Universidad;
2. La elaboración de un análisis de riesgos institucional, que comprenda riesgos jurídicos, éticos, académicos, laborales, patrimoniales, reputacionales y de seguridad de la información, articulado con la metodología de gestión de riesgos del SIPPID;
3. El criterio previo no vinculante del Comité, así como, cuando corresponda, del Comité Universitario de Ética y de la Procuraduría Nacional;
4. La adopción de medidas técnicas y organizativas adecuadas para asegurar la calidad de los datos de entrenamiento, validación y prueba, así como su pertinencia, suficiencia y representatividad para los fines perseguidos;
5. La definición y documentación de la lógica subyacente, las limitaciones, los supuestos de uso esperado y los supuestos de uso inapropiado del sistema;
6. La implementación de mecanismos de supervisión humana significativa, con personal capacitado y dotado de capacidad real de intervención, modificación o anulación de los resultados del sistema;
7. La conservación de registros de actividad, trazabilidad y auditoría que permitan documentar el funcionamiento del sistema durante todo su ciclo de vida;
8. La elaboración y entrega de información clara y comprensible a los usuarios y afectados sobre la existencia, finalidad, alcance, lógica y limitaciones del sistema, así como sobre sus derechos;

9. La definición de protocolos de revisión periódica, monitoreo de desempeño, detección de sesgos, gestión de incidentes y eventual desactivación del sistema; y,
10. La incorporación, en los contratos celebrados con proveedores externos, de las cláusulas mínimas previstas en este Reglamento y en el Reglamento de Privacidad.

Capítulo IV

Sistemas de riesgo limitado

Artículo 34.- Sistemas de riesgo limitado. Son sistemas de riesgo limitado aquellos que, sin estar comprendidos en los capítulos II o III del presente Título, presentan riesgos relevantes para los derechos o intereses de las personas, especialmente porque interactúan directamente con ellas o producen contenidos sintéticos. Se consideran, entre otros:

- a) Los asistentes virtuales, agentes conversacionales o *chatbots* institucionales que interactúan con miembros de la Comunidad Universitaria o con terceros;
- b) Los sistemas que generan o manipulan textos, imágenes, audio o vídeo con apariencia de autoría humana o de hechos reales;
- c) Los sistemas de recomendación, sugerencia o personalización de contenidos académicos, bibliográficos o de servicios institucionales;
- d) Los sistemas de análisis automatizado de comunicaciones institucionales no destinados a producir decisiones jurídicas relevantes; y,
- e) Los demás sistemas que el Comité determine.

El uso de inteligencia artificial generativa para la elaboración o el apoyo en textos, imágenes, audios, vídeos, diseños, ilustraciones, artes institucionales, simulaciones y materiales de aprendizaje constituye una herramienta legítima y útil y no queda comprendido, por sí solo, en este nivel de riesgo cuando se trate de actividades ordinarias de edición, corrección, ajuste de estilo, diagramación, traducción o mejora de documentos. La regulación se concentra en los contenidos generados o modificados con inteligencia artificial que puedan presentarse falsamente como de autoría humana, reproducir hechos inexistentes como reales, afectar la honra o imagen de terceros, suplantar identidades, distorsionar evidencias, vulnerar derechos de autor o inducir a error sobre la autenticidad, fuente, autoría o veracidad del contenido. Se reconoce, asimismo, que la inteligencia artificial generativa puede favorecer la creación de materiales más pertinentes, inclusivos e interculturales, siempre que su uso sea transparente, verificable y compatible con la ética institucional.

Artículo 35.- Obligaciones aplicables a los sistemas de riesgo limitado. Para los sistemas de riesgo limitado se observarán, sin perjuicio de las demás obligaciones de este Reglamento y del Reglamento de Privacidad, las siguientes:

1. Informar de manera clara y previa a los usuarios o interlocutores que están interactuando con un sistema de inteligencia artificial y no con una persona;
2. Identificar de manera visible los contenidos sintéticos generados o manipulados por inteligencia artificial cuando se publiquen, difundan o compartan en contextos institucionales;
3. Establecer mecanismos sencillos para que el usuario solicite atención humana cuando lo prefiera o lo requiera la naturaleza del asunto;
4. Documentar la finalidad, los datos tratados, las limitaciones del sistema y los responsables operativos; y,
5. Implementar mecanismos para reportar errores, sesgos, incidentes o respuestas inadecuadas.

Capítulo V

Sistemas de riesgo mínimo

Artículo 36.- Sistemas de riesgo mínimo. Son sistemas de riesgo mínimo aquellos que, por su finalidad, alcance, datos tratados o contexto de uso, presentan riesgos bajos para los derechos o intereses de las personas, tales como herramientas ofimáticas con asistencia de inteligencia artificial, traductores automáticos, correctores ortográficos, motores de búsqueda académica o herramientas equivalentes. A estos sistemas se aplicarán las disposiciones generales de este Reglamento y del Reglamento de Privacidad, sin las obligaciones reforzadas previstas para los sistemas de alto riesgo o de riesgo limitado, sin perjuicio de las obligaciones generales en materia de protección de datos personales, propiedad intelectual y honestidad académica.

TÍTULO IV

PROTECCIÓN DE DATOS PERSONALES Y PRIVACIDAD EN EL USO DE INTELIGENCIA ARTIFICIAL

Capítulo I

Marco aplicable y calidad institucional

Artículo 37.- Marco normativo aplicable. Todo tratamiento de datos personales realizado, en todo o en parte, mediante sistemas de inteligencia artificial dentro de la Universidad Metropolitana se sujetará íntegramente a la Constitución, a la Ley Orgánica de Protección de Datos Personales y su Reglamento General, a la normativa secundaria expedida por la Superintendencia de Protección de Datos Personales y, en particular, a la Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial, al Reglamento de Privacidad y a las Políticas

de Protección de Datos Personales de la Universidad Metropolitana. Las reglas generales sobre principios, bases jurídicas, derechos de los titulares y deberes institucionales se rigen por dichos instrumentos; el presente Título regula los aspectos específicos del tratamiento mediante inteligencia artificial.

Artículo 38.- Calidad de responsable del tratamiento y gestión funcional de responsabilidades. Frente a los titulares, la sociedad y el Estado, la responsable del tratamiento es la Universidad Metropolitana en su calidad de persona jurídica. La gestión funcional y administrativa de esa responsabilidad ha sido radicada en el Vicerrectorado Administrativo, sin perjuicio de las atribuciones del Rector como máxima autoridad ejecutiva. Cuando, conforme a las funciones desempeñadas, una persona, unidad o proveedor trate datos personales por cuenta de la Universidad, actuará como encargado del tratamiento y se aplicarán las disposiciones legales, reglamentarias y contractuales correspondientes a esa figura.

Artículo 39.- Principios reforzados. Sin perjuicio de los principios establecidos en la Ley Orgánica de Protección de Datos Personales y en el Reglamento de Privacidad, los tratamientos efectuados mediante sistemas de inteligencia artificial observarán, de manera reforzada, los principios de licitud, lealtad, transparencia, finalidad, minimización, exactitud, calidad, conservación limitada, integridad, confidencialidad, responsabilidad demostrada, privacidad desde el diseño y privacidad por defecto.

Capítulo II

Obligaciones según el rol en el tratamiento

Artículo 40.- Obligaciones institucionales de la Universidad Metropolitana como responsable del tratamiento. En el desarrollo, adquisición, contratación, implementación, despliegue o uso institucional de sistemas de inteligencia artificial que traten datos personales, la Universidad Metropolitana, en su calidad de responsable del tratamiento, a través de las instancias competentes, deberá:

- a) Informar al titular, de manera clara, específica, determinada y transparente, sobre el tratamiento efectuado, su carácter automatizado, sus finalidades, plazos de conservación, destinatarios, transferencias internacionales y derechos que le asisten;
- b) Identificar la base jurídica del tratamiento y obtener, cuando corresponda, el consentimiento libre, informado, específico e inequívoco del titular;
- c) Realizar la gestión de riesgos y, cuando corresponda, la Evaluación de Impacto del Tratamiento;

- d) Incluir el tratamiento en el Registro de Actividades de Tratamiento e inscribirlo, cuando corresponda, en el Registro Nacional de Protección de Datos Personales;
- e) Implementar medidas técnicas, organizativas, físicas, jurídicas y de seguridad de la información proporcionales al nivel de riesgo;
- f) Garantizar el ejercicio efectivo de los derechos de los titulares;
- g) Adoptar mecanismos para la detección, gestión y notificación de incidentes de seguridad y vulneraciones de datos personales; y,
- h) Conservar evidencia verificable del cumplimiento de estas obligaciones.

Artículo 41.- Obligaciones de las unidades, cargos o servidores responsables de la gestión funcional del tratamiento. Las unidades académicas, administrativas, tecnológicas, de cumplimiento, protección de datos, investigación o gestión institucional que intervengan en el uso de sistemas de inteligencia artificial deberán, dentro de su ámbito de competencia:

- a) Aplicar las políticas, lineamientos y controles aprobados por la Universidad;
- b) Verificar que el tratamiento cuente con autorización institucional, base jurídica y finalidad legítima;
- c) Coordinar con el Delegado de Protección de Datos Personales, la Dirección de Tecnologías Informáticas, el Especialista en Cumplimiento y la Procuraduría Nacional, según corresponda;
- d) Documentar las decisiones automatizadas que generen efectos jurídicos o afecten significativamente a los titulares;
- e) Auditar o facilitar la auditoría del funcionamiento general del sistema según su nivel de riesgo y criticidad institucional; y,
- f) Reportar incidentes, desviaciones, usos indebidos o riesgos identificados.

Artículo 42.- Obligaciones de los encargados del tratamiento. Cuando una persona natural o jurídica, unidad, proveedor, contratista o tercero trate datos personales por cuenta de la Universidad, deberá cumplir las obligaciones legales, reglamentarias, contractuales y técnicas aplicables a los encargados del tratamiento, incluyendo confidencialidad, seguridad, trazabilidad, limitación de finalidad, asistencia para el ejercicio de derechos, gestión de incidentes, devolución o supresión de datos y prohibición de subencargo no autorizado.

Artículo 43.- Obligaciones individuales de los miembros de la Comunidad Universitaria. Toda autoridad, docente, investigador, servidor, trabajador, estudiante, practicante, becario, consultor, proveedor o tercero vinculado a la Universidad que utilice sistemas de inteligencia artificial deberá:

- a) Usar dichas herramientas únicamente para finalidades legítimas, autorizadas y compatibles con sus funciones o actividades académicas;
- b) Abstenerse de ingresar, cargar, copiar, compartir o procesar datos personales, información confidencial, documentos institucionales no públicos, expedientes académicos, financieros, laborales, disciplinarios o contractuales en sistemas de inteligencia artificial no autorizados;
- c) Respetar la confidencialidad, la protección de datos personales, la propiedad intelectual, la integridad académica y la seguridad de la información;
- d) Verificar, bajo responsabilidad personal, la calidad, pertinencia, exactitud y licitud de los resultados generados por inteligencia artificial antes de utilizarlos o incorporarlos en actuaciones académicas, administrativas, jurídicas, financieras o institucionales;
- e) Transparentar el uso de inteligencia artificial cuando corresponda, especialmente en actividades académicas, investigativas, evaluativas o de producción institucional; y,
- f) Reportar de inmediato cualquier incidente, uso indebido, acceso no autorizado, vulneración de datos personales o riesgo relevante del que tenga conocimiento.

Artículo 44.- Regla general de responsabilidad. La existencia de un sistema de inteligencia artificial propio o provisto por terceros, no exime a la Universidad, a sus unidades competentes, ni a los usuarios individuales de cumplir sus obligaciones legales, éticas, contractuales y de confidencialidad. Cada sujeto responderá conforme a su rol, nivel de intervención, deber funcional y grado de control sobre el tratamiento o uso realizado.

Capítulo III

Evaluación de impacto del tratamiento

Artículo 45.- Procedencia de la Evaluación de Impacto del Tratamiento. La Universidad Metropolitana realizará, con carácter previo al inicio del tratamiento, una Evaluación de Impacto del Tratamiento de Datos Personales cuando, de conformidad con la Ley Orgánica de Protección de Datos Personales, su Reglamento General y la normativa secundaria aplicable, el uso de un sistema de inteligencia artificial pueda generar un alto riesgo para los derechos y libertades de los titulares.

Para determinar la existencia de alto riesgo se considerarán, entre otros, los siguientes factores:

- a) El tratamiento de categorías especiales o sensibles de datos personales, incluidos datos de salud, biométricos, genéticos o relativos a niños y adolescentes;
- b) La adopción o apoyo de decisiones automatizadas que produzcan efectos jurídicos, académicos, laborales, económicos, disciplinarios o significativos sobre los titulares;
- c) La elaboración de perfiles, evaluación sistemática o predicción de comportamientos, capacidades, rendimiento, situación económica, salud, preferencias o características personales;
- d) La observación, vigilancia, monitoreo o seguimiento sistemático de personas en espacios físicos o digitales;
- e) El tratamiento de datos personales a gran escala;
- f) Las transferencias internacionales sistemáticas de datos personales o el uso de proveedores ubicados fuera del territorio nacional;
- g) El empleo de tecnologías emergentes, biometría, reconocimiento facial, inferencia de emociones, videovigilancia inteligente o mecanismos equivalentes;
- h) La intervención sobre grupos en situación de vulnerabilidad o sobre personas que puedan encontrarse en una relación de dependencia, subordinación o especial asimetría frente a la Universidad;
- i) La combinación de distintas fuentes, bases de datos o categorías de información que incremente el riesgo de identificación, discriminación, exclusión, afectación reputacional o uso incompatible; y,

j) La magnitud, probabilidad, reversibilidad y gravedad de los posibles impactos sobre los derechos y libertades de los titulares.

La sola concurrencia de uno de estos factores no determinará automáticamente la obligación de realizar una Evaluación de Impacto, salvo que la normativa aplicable establezca expresamente lo contrario. La procedencia de la evaluación deberá determinarse mediante un análisis documentado del riesgo, considerando la naturaleza, alcance, contexto, finalidad, tecnología utilizada, categorías de datos, número y condición de los titulares y medidas de mitigación previstas.

El área requirente será responsable de iniciar y documentar el análisis previo de riesgos, con el apoyo técnico de la Dirección de Tecnologías Informáticas y de las unidades tratantes correspondientes. El Delegado de Protección de Datos Personales asesorará y supervisará el proceso y emitirá las recomendaciones que estime pertinentes, sin asumir su ejecución operativa ni su aprobación. El Comité Institucional podrá conocer el análisis y emitir criterio técnico no vinculante sobre la conveniencia de realizar la Evaluación de Impacto.

La aprobación de la Evaluación de Impacto y la decisión institucional sobre el inicio, continuidad, modificación o suspensión del tratamiento corresponderán al Vicerrectorado Administrativo, en calidad de responsable interno del tratamiento, sin perjuicio de las atribuciones del Rector y de las demás autoridades competentes.

Cuando del análisis resulte que persiste un alto riesgo que no pueda ser razonablemente mitigado, el tratamiento no podrá iniciarse o continuar hasta que se adopten medidas adicionales y, cuando corresponda, se efectúe la consulta previa ante la autoridad de protección de datos personales.

Artículo 46.- Contenido mínimo de la Evaluación de Impacto. La Evaluación de Impacto del Tratamiento contendrá, al menos:

1. La descripción detallada del sistema, sus finalidades, los datos personales tratados, las categorías de titulares involucrados, los flujos de información y los destinatarios;
2. La identificación de la base jurídica del tratamiento;
3. El análisis de necesidad y proporcionalidad respecto de las finalidades perseguidas;
4. La identificación y valoración de los riesgos para los derechos y libertades de los titulares;
5. Las medidas técnicas, organizativas, jurídicas y éticas previstas para mitigar dichos riesgos;

6. El análisis específico del componente automatizado, de los posibles sesgos y de la adecuación de los mecanismos de supervisión humana;
7. El análisis de transferencias nacionales o internacionales asociadas al sistema;
8. Las conclusiones y recomendaciones; y,
9. El plan de seguimiento, revisión y actualización periódica.

Capítulo IV

Decisiones automatizadas y elaboración de perfiles

Artículo 47.- Derecho a no ser objeto de decisiones automatizadas. Ninguna persona será sometida, dentro de la Universidad Metropolitana, a decisiones que produzcan efectos jurídicos sobre ella o que la afecten significativamente, basadas única o predominantemente en el tratamiento automatizado de sus datos personales o en la elaboración de perfiles, sin que medie supervisión humana significativa. Esta garantía no podrá ser eludida mediante intervenciones humanas meramente formales o aparentes.

Artículo 48.- Garantías mínimas. En los procesos institucionales en que se utilicen sistemas de inteligencia artificial para apoyar decisiones que afecten a personas, se garantizarán, al menos, las siguientes condiciones: información previa al titular sobre la existencia y características del tratamiento automatizado; intervención humana significativa por parte de personal capacitado y autorizado; posibilidad de que el titular exprese su punto de vista; derecho a impugnar la decisión; motivación adecuada y trazable de la decisión final; y conservación documental suficiente para permitir su revisión posterior.

Artículo 49.- Elaboración de perfiles. La elaboración de perfiles de los miembros de la Comunidad Universitaria mediante sistemas de inteligencia artificial requerirá base jurídica específica, finalidad legítima, información transparente al titular, supervisión humana significativa y aplicación reforzada de las medidas previstas en este Título. Queda prohibida la elaboración de perfiles que infiera categorías especiales o sensibles de datos sin habilitación legal expresa.

Capítulo V

Transferencias y comunicaciones internacionales

Artículo 50.- Transferencias internacionales. Las comunicaciones o transferencias internacionales de datos personales asociadas al uso institucional de sistemas de inteligencia artificial, incluidas aquellas que se generen por el alojamiento de servicios en la nube, la utilización de proveedores extranjeros, las integraciones con plataformas internacionales o las colaboraciones académicas y de investigación, observarán las

disposiciones de la Ley Orgánica de Protección de Datos Personales, su Reglamento General, la Norma General de Transferencias o Comunicaciones Nacionales e Internacionales de Datos Personales expedida por la Superintendencia de Protección de Datos Personales y el Reglamento de Privacidad.

Artículo 51.- Documentación mínima. Cada transferencia internacional asociada a un sistema de inteligencia artificial deberá quedar documentada en el Registro de Actividades de Tratamiento y contar, al menos, con:

- a) Identificación del destinatario y del país de destino;
- b) Categorías de datos transferidos y categorías de titulares;
- c) Finalidad de la transferencia y base jurídica;
- d) Garantías adecuadas o mecanismos de legitimación aplicables;
- e) Instrumentos contractuales suscritos con el destinatario; y,
- f) Evaluación de riesgos, cuando corresponda.

Artículo 52.- Datos institucionales en herramientas externas. Queda prohibido cargar, ingresar o procesar en herramientas externas de inteligencia artificial datos personales sensibles, datos confidenciales institucionales, información sometida a deber de reserva, información reservada o estratégica, información protegida por propiedad intelectual de la Universidad o de terceros, evaluaciones académicas o disciplinarias en curso, información de procesos contractuales en negociación o información protegida por relación profesional o cliente, salvo cuando la herramienta haya sido institucionalmente autorizada y se hayan adoptado las garantías técnicas, contractuales y jurídicas pertinentes, en consonancia con la clasificación de la información establecida por el Reglamento de Privacidad.

TÍTULO V

ÉTICA EN EL USO DE LA INTELIGENCIA ARTIFICIAL

Artículo 53.- Articulación con el Código de Ética. Las disposiciones del presente Título se aplicarán de manera complementaria, armónica y sin sustitución de las contenidas en el Código de Ética Institucional, de la Investigación y el Aprendizaje, particularmente las relativas al fraude académico, al uso ético de tecnologías digitales e inteligencia artificial, a la honestidad intelectual y a las responsabilidades éticas de la Comunidad Universitaria. Las dimensiones éticas del uso de inteligencia artificial son competencia del Comité Universitario de Ética y de los Subcomités de Ética de Sede, en los términos de dicho Código.

Artículo 54.- Deberes éticos en el uso de la inteligencia artificial. Los miembros de la Comunidad Universitaria, en el uso de sistemas de inteligencia artificial, deberán:

- a) Actuar con honestidad intelectual y respetar la autoría, las fuentes y la propiedad intelectual de terceros;
- b) Verificar la veracidad, exactitud, pertinencia y suficiencia de los contenidos generados o intermediados por la inteligencia artificial antes de utilizarlos en actividades académicas, investigativas, administrativas o de comunicación institucional;
- c) Citar de manera explícita la intervención de sistemas de inteligencia artificial en los productos académicos, investigativos o institucionales, conforme a las directrices que dicte el Comité y a las normas del Código de Ética Institucional, de la Investigación y el Aprendizaje;
- d) Abstenerse de utilizar la inteligencia artificial para sustituir el razonamiento, la reflexión, la redacción o la evaluación que deban reflejar el dominio personal del autor;
- e) Respetar la confidencialidad y la protección de datos personales propios y ajenos al introducir información en sistemas de inteligencia artificial;
- f) Reportar oportunamente errores, sesgos, alucinaciones, incidentes o usos contrarios a la ética detectados en sistemas de inteligencia artificial institucionales o de uso institucional;
- g) Denunciar el uso indebido de inteligencia artificial cuando tomen conocimiento de hechos que afecten la integridad académica, la ética universitaria o los derechos de las personas; y,
- h) Capacitarse de manera permanente y participar en las acciones formativas que la Universidad implemente en materia de inteligencia artificial, ética y protección de datos personales.

Artículo 55.- Prohibiciones éticas reforzadas. Sin perjuicio de las prohibiciones generales contenidas en este Reglamento, en el Reglamento de Privacidad y en el Código de Ética Institucional, de la Investigación y el Aprendizaje, queda prohibido el uso de sistemas de inteligencia artificial para suplantar la identidad de personas, falsificar documentos institucionales, generar contenidos discriminatorios, incitar al odio o a la violencia, vulnerar la dignidad o la intimidad de las personas, manipular procesos electorales o de representación universitaria o difundir desinformación atribuida a la Universidad o a sus integrantes.

TÍTULO VI

APLICACIÓN SEGÚN ÁMBITOS UNIVERSITARIOS

Capítulo I

Personal académico y de investigación

Artículo 56.- Uso pedagógico de la inteligencia artificial. El personal académico podrá incorporar sistemas de inteligencia artificial como apoyo a las actividades de docencia, tutoría, evaluación, asesoría académica y gestión curricular, siempre que:

- a) Su uso sea pedagógicamente justificado, coherente con los resultados de aprendizaje, los *syllabus* aprobados y las metodologías institucionales;
- b) Se informe a los estudiantes, de manera previa y clara, sobre la utilización del sistema, sus finalidades, las reglas aplicables y, cuando corresponda, los datos personales tratados;
- c) Se respeten los derechos de los estudiantes y los principios establecidos en este Reglamento, en el Reglamento de Privacidad, en el Código de Ética y en las Políticas de Protección de Datos Personales;
- d) El sistema utilizado se encuentre dentro de los autorizados institucionalmente o, en su defecto, se gestione su autorización conforme al procedimiento previsto; y,
- e) Se ejerza supervisión humana significativa sobre las decisiones derivadas del sistema.

Artículo 57.- Reglas para evaluaciones. En las evaluaciones académicas, el personal académico deberá:

- a) Definir, comunicar y documentar las condiciones de uso o no uso permitido de sistemas de inteligencia artificial en cada evaluación, trabajo, proyecto o producto académico;
- b) Establecer mecanismos razonables de verificación de la autoría, sin recurrir a métodos invasivos, desproporcionados o discriminatorios;
- c) Utilizar herramientas institucionales de detección de similitud, análisis de coincidencias, paráfrasis o contenido generado por inteligencia artificial como medios técnicos de apoyo a la verificación de autoría e integridad académica. Sus reportes deberán ser ponderados conforme a su alcance, metodología, segmentos identificados, fuentes asociadas, proporción del texto comprometido y demás elementos verificables. La atribución de fraude académico y la eventual imposición de sanciones no se producirán por el solo resultado automático de la herramienta, sino mediante valoración académica o disciplinaria motivada y con observancia del procedimiento previsto en la normativa institucional;

d) No exigir a los estudiantes la contratación, adquisición o pago individual de suscripciones a herramientas externas de inteligencia artificial, detección de similitud, verificación de autoría o integridad académica. Esta prohibición no impedirá que la Universidad disponga el uso obligatorio de plataformas, sistemas o herramientas institucionalmente provistos, autorizados o financiados, siempre que su utilización haya sido comunicada previamente y se garantice el acceso en condiciones de igualdad; y,

e) Adecuar los métodos de evaluación, cuando resulte pedagógicamente pertinente, para integrar el uso ético, crítico, transparente y verificable de la inteligencia artificial como competencia formativa. Esta adecuación podrá comprender, entre otros mecanismos, defensas orales, entregas progresivas, bitácoras o evidencias del proceso de elaboración, resolución de casos, actividades prácticas, verificación de fuentes, reflexión crítica sobre los resultados generados, declaración del uso de inteligencia artificial y revisión de la coherencia entre el producto presentado y el desempeño demostrado por el estudiante.

Artículo 58.- Investigación con inteligencia artificial. La utilización de sistemas de inteligencia artificial en proyectos de investigación deberá observar los principios y normas del Código de Ética Institucional, de la Investigación y el Aprendizaje, del Reglamento de Privacidad, del Reglamento de Investigación e Innovación y de las normas aplicables a la ética de la investigación en general; y, cuando corresponda, requerirá pronunciamiento del Comité de Ética en Investigación con Seres Humanos. Los proyectos que utilicen inteligencia artificial sobre datos personales, comunidades vulnerables, pueblos y nacionalidades indígenas o que generen riesgos significativos serán calificados como de alto riesgo conforme al Título III.

Artículo 59.- Atribución de autoría y créditos. Los productos académicos, científicos o de divulgación elaborados con apoyo de sistemas de inteligencia artificial cumplirán las siguientes reglas:

a) La autoría corresponderá únicamente a personas naturales; los sistemas de inteligencia artificial no serán reconocidos como autores ni coautores;

b) Deberá declararse de manera explícita el uso del sistema de inteligencia artificial, indicando, al menos, su denominación, finalidad de uso, alcance y, cuando proceda, las versiones empleadas;

c) Las personas autoras asumirán responsabilidad plena por el contenido del producto, incluida la verificación de su veracidad, originalidad y respeto a derechos de terceros; y,

d) Se respetarán los lineamientos editoriales, científicos y profesionales aplicables al respectivo campo del conocimiento.

Capítulo II

Estudiantes

Artículo 60.- Uso responsable por parte de los estudiantes. Los estudiantes podrán utilizar sistemas de inteligencia artificial como apoyo a sus procesos de aprendizaje, análisis, consulta y elaboración de ideas, en los términos del Código de Ética Institucional, de la Investigación y el Aprendizaje. En tal virtud, deberán:

- a) Conocer y observar las reglas que el docente o la Institución hayan definido para el uso o no uso de inteligencia artificial en cada actividad académica;
- b) Citar de manera explícita la intervención de sistemas de inteligencia artificial en los productos entregados, conforme a las pautas institucionales;
- c) Asumir la autoría y responsabilidad plena del producto entregado, incluida la verificación de su veracidad y originalidad;
- d) Abstenerse de utilizar la inteligencia artificial para sustituir, automatizar o reemplazar de manera ilegítima la autoría, el razonamiento, la redacción o la evaluación que les corresponde personalmente;
- e) Proteger sus datos personales y los de terceros al utilizar herramientas externas, evitando ingresar información sensible o confidencial que no sea estrictamente indispensable; y,
- f) Reportar al docente o a la autoridad competente los errores, sesgos o conductas indebidas detectadas en sistemas de inteligencia artificial.

Artículo 61.- Participación informada. La Universidad garantizará a los estudiantes información clara, accesible y oportuna sobre los sistemas de inteligencia artificial utilizados en los procesos académicos, sus finalidades, alcance, limitaciones y los derechos que les asisten, incluido el derecho a no ser objeto de decisiones basadas única o predominantemente en valoraciones automatizadas que produzcan efectos jurídicos o significativos.

Artículo 62.- Tutela del estudiante menor de edad. Cuando, en el marco de actividades académicas, administrativas, educativas, de investigación, desarrollo e innovación, vinculación con la sociedad o prestación de servicios institucionales, intervengan niños o adolescentes y se utilicen sistemas de inteligencia artificial que impliquen tratamiento de sus datos personales, la Universidad observará su interés superior, el respeto de sus derechos fundamentales y las garantías reforzadas previstas en la normativa aplicable.

Cuando la base legitimadora del tratamiento sea el consentimiento, este se recabará de acuerdo con la edad, capacidad y condiciones previstas en la Ley Orgánica de Protección de Datos Personales y su Reglamento General. La Universidad aplicará medidas

reforzadas de seguridad, privacidad desde el diseño, minimización de datos, transparencia, supervisión humana y control de acceso.

Se evitará la elaboración de perfiles, la inferencia de emociones, el reconocimiento biométrico, la videovigilancia inteligente y las decisiones automatizadas que produzcan efectos jurídicos o significativos sobre niños o adolescentes, salvo que exista una finalidad legítima, una base jurídica suficiente, necesidad y proporcionalidad demostradas, evaluación previa de riesgos y garantías adecuadas para la protección de sus derechos.

Capítulo III

Personal administrativo

Artículo 63.- Uso institucional. El personal administrativo podrá utilizar sistemas de inteligencia artificial como apoyo a sus actividades, observando las siguientes reglas:

- a) Utilizar únicamente sistemas autorizados institucionalmente, en los términos definidos por el Comité y la Dirección de Tecnologías Informáticas;
- b) Respetar el deber de confidencialidad y reserva respecto de la información institucional y los datos personales a los que tenga acceso, conforme al régimen de protección perpetua establecido en el Reglamento de Privacidad;
- c) Abstenerse de cargar, ingresar o compartir en sistemas externos información protegida por reserva, deber de confidencialidad, propiedad intelectual o relación profesional, salvo autorización institucional expresa y con las garantías correspondientes;
- d) Reportar de inmediato a su superior jerárquico y a la Dirección de Tecnologías Informáticas cualquier incidente, error o vulnerabilidad detectada; y,
- e) Documentar los procesos institucionales en los que se utilice inteligencia artificial, garantizando trazabilidad y auditabilidad.

Artículo 64.- Decisiones administrativas. Las decisiones administrativas que afecten derechos o intereses de personas no podrán fundarse única o predominantemente en valoraciones automatizadas. La autoridad administrativa competente conservará la responsabilidad de adoptar la decisión, motivarla adecuadamente y garantizar el debido proceso, sin perjuicio del apoyo que la inteligencia artificial pueda brindar como herramienta auxiliar.

Capítulo IV

Autoridades universitarias

Artículo 65.- Estándar reforzado. Las Primeras Autoridades, las autoridades académicas y administrativas, los directivos académicos y administrativos, los miembros del Consejo Académico Superior y del Consejo de Regentes y los promotores

institucionales, en su calidad de representantes institucionales, observarán un estándar reforzado de conducta en el uso de sistemas de inteligencia artificial, conforme al Código de Ética Institucional, de la Investigación y el Aprendizaje. En tal virtud, evitarán cualquier uso que pudiera comprometer la imparcialidad, la transparencia, la confidencialidad o la legalidad de sus decisiones y se abstendrán de utilizar inteligencia artificial para fines de proselitismo, beneficio personal o conflicto de intereses.

TÍTULO VII

ADQUISICIÓN, DESARROLLO, CONTRATACIÓN Y DESPLIEGUE DE SISTEMAS DE INTELIGENCIA ARTIFICIAL

Capítulo I

Reglas comunes

Artículo 66.- Procedimiento institucional. La adquisición, contratación, desarrollo o despliegue institucional de sistemas de inteligencia artificial se sujetará al procedimiento institucional ordinario aplicable, incluida la planificación, convocatoria, evaluación, dictamen, aprobación de proyectos, aprobación de planes operativos anuales y adquisición de licencias de *software*, sin alterar la distribución de competencias orgánicas prevista en el Estatuto y en el Reglamento General al Estatuto. Cuando corresponda por el nivel de riesgo o por el tipo de datos tratados, el procedimiento deberá contar con:

- a) La justificación de la necesidad institucional por parte del área requirente, según su finalidad académica, investigativa, administrativa o de gestión;
- b) El informe de viabilidad técnica de la Dirección de Tecnologías Informáticas, que verifique la compatibilidad, seguridad, integración, licenciamiento y sostenibilidad tecnológica;
- c) El análisis de riesgos y de cumplimiento por las instancias competentes;
- d) La Evaluación de Impacto del Tratamiento de Datos Personales, cuando resulte exigible conforme al artículo 45 de este Reglamento, a la Ley Orgánica de Protección de Datos Personales, su Reglamento General y la normativa secundaria aplicable;
- e) La revisión jurídica de los contratos, términos de licenciamiento o instrumentos vinculantes por la Procuraduría Nacional, con carácter no vinculante; y,
- f) La autorización de la autoridad competente conforme al Estatuto, al Reglamento General al Estatuto, al Plan Operativo Anual y a la normativa interna de contratación.

La aprobación de la adquisición, contratación, desarrollo o despliegue corresponderá a la autoridad competente conforme al Estatuto, al Reglamento General al Estatuto, al Plan Operativo Anual, al presupuesto institucional y al procedimiento contractual aplicable. Ninguna unidad técnica, consultiva o requirente podrá comprometer recursos institucionales ni autorizar por sí sola la contratación definitiva fuera de las competencias que le hayan sido expresamente atribuidas.

La Dirección de Tecnologías Informáticas conserva su rol técnico y no constituye la única instancia decisoria sobre la adquisición o despliegue; el área requirente asume la responsabilidad funcional de la necesidad institucional; y las demás instancias intervienen como controles de legalidad, cumplimiento y gestión de riesgos, sin paralizar indebidamente la contratación.

La calificación de un sistema como de alto riesgo no constituirá, por sí sola, causal automática de rechazo o de no adquisición. En estos casos, la unidad requirente y las instancias competentes deberán determinar si los riesgos pueden ser razonablemente mitigados mediante controles reforzados, supervisión humana, restricciones de uso, medidas contractuales, mecanismos de trazabilidad, pruebas previas, implementación progresiva o cualquier otra salvaguarda adecuada.

Artículo 67.- Diligencia debida en la selección de proveedores. Previo a la contratación de proveedores externos, se verificará, al menos:

- a) La existencia y solvencia jurídica del proveedor, así como su régimen de cumplimiento normativo;
- b) La existencia de mecanismos suficientes de protección de datos personales y de seguridad de la información;
- c) Las certificaciones, auditorías o reconocimientos profesionales relevantes, incluidas las certificaciones bajo normas técnicas internacionales aplicables;
- d) El régimen jurídico aplicable al alojamiento, procesamiento y almacenamiento de datos, incluyendo la jurisdicción y las garantías para transferencias internacionales;
- e) La política del proveedor respecto del uso de los datos cargados o procesados para fines de entrenamiento de modelos o para finalidades distintas de las contractualmente pactadas;
- f) Las cláusulas relativas a propiedad intelectual sobre los datos, los modelos, los resultados y los productos generados; y,
- g) Los antecedentes de incidentes, sanciones o controversias relevantes.

Artículo 68.- Cláusulas contractuales mínimas. Los contratos celebrados con proveedores, desarrolladores, distribuidores, desplegados o implementadores externos de sistemas de inteligencia artificial deberán contener, al menos, cláusulas relativas a:

1. La identificación de la calidad jurídica de cada parte respecto del tratamiento de datos personales;
2. Las finalidades, instrucciones, alcance, ubicaciones y plazos del tratamiento;
3. Las medidas técnicas, organizativas y de seguridad de la información aplicables;
4. La prohibición de usar los datos cargados, procesados o generados para fines distintos de los contractualmente autorizados, en particular para entrenamiento de modelos;
5. El régimen de transferencias internacionales y las garantías adecuadas;
6. Los derechos del titular y los mecanismos para su atención;
7. El régimen de propiedad intelectual sobre datos, modelos, resultados y productos derivados;
8. Las obligaciones de notificación de incidentes y vulneraciones, con plazos compatibles con el régimen ecuatoriano de protección de datos personales;
9. Las obligaciones de auditoría y de cooperación con la Universidad y con la Superintendencia de Protección de Datos Personales;
10. Los mecanismos de salida y portabilidad al término del contrato, incluida la devolución y eliminación de datos;
11. El régimen de responsabilidad por incumplimientos contractuales, daños patrimoniales y sanciones derivadas de la actuación del proveedor;
12. Las cláusulas de confidencialidad, no competencia y protección de la información institucional, según corresponda; y,
13. La cláusula expresa de deber perpetuo de protección de los datos personales, conforme al Reglamento de Privacidad.

Artículo 69.- Desarrollo interno. Cuando la Universidad Metropolitana desarrolle sistemas de inteligencia artificial con recursos propios o en colaboración con terceros, observará los principios y obligaciones del presente Reglamento y del Reglamento de Privacidad durante todo el ciclo de vida del sistema, incluida la fase de diseño, recolección y curado de datos, entrenamiento, validación, prueba, despliegue, monitoreo, actualización y retiro. La documentación técnica, los conjuntos de datos y los modelos se conservarán bajo medidas de seguridad apropiadas y conforme a las políticas institucionales.

TÍTULO VIII

TRANSPARENCIA, EXPLICABILIDAD Y SUPERVISIÓN HUMANA

Artículo 70.- Transparencia institucional. La Universidad Metropolitana publicará y mantendrá actualizada información clara, accesible y comprensible sobre los sistemas de inteligencia artificial que utilice o despliegue, en particular respecto de aquellos que interactúen con miembros de la Comunidad Universitaria o que afecten significativamente sus derechos. La información podrá presentarse de manera centralizada o vinculada a cada sistema, conforme a las directrices del Comité y al régimen general de transparencia del Reglamento de Privacidad.

Artículo 71.- Información mínima. La información de transparencia incluirá, al menos:

- a) La identificación del sistema y del proveedor o desarrollador;
- b) La finalidad y los contextos de uso;
- c) Las categorías de datos tratados, cuando corresponda;
- d) Los tipos de decisiones que pueden derivar del sistema y los efectos previsibles sobre las personas;
- e) Los mecanismos de supervisión humana y los canales de impugnación o reclamo;
- f) Las limitaciones conocidas, los riesgos identificados y las medidas de mitigación adoptadas; y,
- g) Los responsables operativos.

Artículo 72.- Identificación de contenidos sintéticos. Los contenidos generados o manipulados por sistemas de inteligencia artificial que se publiquen o difundan en contextos institucionales se identificarán de manera visible. Se prohíbe su utilización para suplantar identidades, falsear hechos, atribuir declaraciones a personas reales o generar piezas que puedan inducir razonablemente a error sobre su autoría o autenticidad.

Artículo 73.- Supervisión humana significativa. Toda autoridad o funcionario que utilice o supervise un sistema de inteligencia artificial con efectos relevantes sobre personas estará dotado de capacidad real de comprender el sistema, interpretar sus resultados, intervenir, modificar o anular sus decisiones y motivar adecuadamente la decisión final. La Universidad asegurará la formación, los recursos y las condiciones organizativas necesarias para hacer efectiva esta supervisión.

TÍTULO IX

SEGURIDAD, AUDITORÍA Y GESTIÓN DE INCIDENTES

Artículo 74.- Medidas de seguridad. La Universidad Metropolitana implementará, en relación con los sistemas de inteligencia artificial, las medidas técnicas, organizativas,

físicas, jurídicas y de seguridad de la información previstas en el Sistema de Gestión de Seguridad de la Información del Reglamento de Privacidad, proporcionales a las categorías y al volumen de datos personales, al estado de la técnica, a las mejores prácticas y al nivel de riesgo del sistema. Tales medidas comprenderán, al menos: control de accesos, autenticación robusta, cifrado de datos en tránsito y en reposo, segregación de ambientes, copias de respaldo, registros de actividad, protección frente a accesos no autorizados, gestión de vulnerabilidades, gestión de cambios y planes de continuidad.

Artículo 75.- Auditorías. Los sistemas de inteligencia artificial utilizados institucionalmente se someterán a auditorías periódicas, internas o externas, en función del nivel de riesgo y de manera articulada con el programa de auditoría del SIPPID. Las auditorías comprenderán, según corresponda, aspectos jurídicos, técnicos, éticos y de protección de datos personales. Los resultados se documentarán y los planes de remediación se ejecutarán dentro de plazos razonables.

Artículo 76.- Gestión de incidentes. La detección, gestión y notificación de incidentes asociados a sistemas de inteligencia artificial se realizará conforme al Procedimiento Institucional de Gestión de Incidentes previsto en el Reglamento de Privacidad y, en caso de afectación a datos personales, conforme a la Ley Orgánica de Protección de Datos Personales, su Reglamento General y la normativa secundaria aplicable. En particular:

1. Toda persona que detecte un incidente deberá reportarlo de inmediato a su superior jerárquico, al responsable operativo del sistema y a la Dirección de Tecnologías Informáticas;
2. Los incidentes que afecten datos personales serán puestos en conocimiento del Vicerrectorado Administrativo y del Delegado de Protección de Datos Personales. El Vicerrectorado Administrativo, con la asesoría y supervisión del Delegado, determinará la procedencia de la notificación a la Superintendencia de Protección de Datos Personales y a los titulares afectados y garantizará el cumplimiento de los plazos legalmente aplicables;
3. Los incidentes con efectos académicos, laborales, disciplinarios o reputacionales serán informados a las autoridades competentes y, cuando corresponda, al Comité; y,
4. Se conservará evidencia documental del incidente, las acciones adoptadas, los plazos de respuesta y las medidas correctivas implementadas.

Artículo 77.- Continuidad y desactivación. Cuando se detecten riesgos graves, vulnerabilidades críticas, incumplimientos sustanciales del presente Reglamento, del Reglamento de Privacidad o de la normativa de protección de datos personales o cuando un sistema de inteligencia artificial deje de cumplir las condiciones que justificaron su adopción, las autoridades competentes podrán suspender, restringir o desactivar el sistema, sin perjuicio de las medidas adicionales que correspondan.

TÍTULO X

CAPACITACIÓN, ALFABETIZACIÓN Y CULTURA INSTITUCIONAL

Artículo 78.- Alfabetización en inteligencia artificial. La Universidad Metropolitana promoverá la alfabetización institucional en inteligencia artificial, de modo que las autoridades, el personal académico, administrativo y los estudiantes adquieran las competencias necesarias para comprender los fundamentos, posibilidades, limitaciones y riesgos de estas tecnologías y para utilizarlas de manera ética, crítica, rigurosa y segura.

Artículo 79.- Plan institucional de capacitación. El Comité, en coordinación con el Vicerrectorado Académico, el Vicerrectorado Administrativo y las unidades responsables, integrará en el plan institucional integrado de capacitación, sensibilización y cultura previsto en el Reglamento de Privacidad los componentes específicos relativos a inteligencia artificial, los cuales serán incorporados en el Plan Operativo Anual y en el presupuesto institucional, conforme a la normativa interna aplicable.

Artículo 80.- Inclusión curricular. Los aspectos éticos, jurídicos, técnicos y sociales de la inteligencia artificial podrán ser incorporados, conforme a las directrices del Vicerrectorado Académico y a la normativa del Consejo de Educación Superior, en los planes y programas de estudio, en los procesos de inducción y en las actividades de educación continua, en cumplimiento del artículo 8 letra m) de la Ley Orgánica de Educación Superior.

TÍTULO XI

RÉGIMEN DE CUMPLIMIENTO, INFRACCIONES Y RESPONSABILIDADES

Artículo 81.- Naturaleza del régimen. El régimen de cumplimiento previsto en el presente Reglamento se aplicará sin perjuicio del régimen disciplinario establecido en la Ley Orgánica de Educación Superior, el Código del Trabajo, el Estatuto Institucional, el Reglamento Interno de Trabajo, el Reglamento que regula el Procedimiento Disciplinario para Estudiantes, Profesores e Investigadores, el Código de Ética Institucional, de la Investigación y el Aprendizaje y el Reglamento de Privacidad, así como de las responsabilidades civiles, administrativas o penales que correspondan.

Artículo 82.- Reenvío al régimen disciplinario y ético. Las infracciones a las disposiciones del presente Reglamento serán tramitadas conforme a los procedimientos disciplinarios y éticos aplicables, según la calidad del presunto infractor, la naturaleza de la conducta y el régimen jurídico al que se encuentra sujeto. Cuando la conducta constituya, simultáneamente, infracción ética y disciplinaria, prevalecerá el procedimiento disciplinario, sin perjuicio de la actuación del Comité Universitario de Ética como órgano sustanciador, conforme al Código de Ética Institucional, de la Investigación y el Aprendizaje.

Artículo 83.- Conductas constitutivas de infracción. Sin perjuicio de las infracciones tipificadas en otras normas internas y en el ordenamiento jurídico, constituyen infracción a este Reglamento:

- a) Desarrollar, adquirir, contratar, implementar, desplegar o utilizar prácticas de inteligencia artificial expresamente prohibidas en el Capítulo II del Título III;
- b) Utilizar sistemas de inteligencia artificial para fraude académico, plagio, suplantación o vulneración de la propiedad intelectual;
- c) Tratar datos personales mediante sistemas de inteligencia artificial sin observar los principios y obligaciones legales y reglamentarios aplicables;
- d) Cargar, ingresar o compartir información sometida a reserva, confidencialidad o protección institucional en sistemas externos no autorizados;
- e) Omitir la información, citación o identificación del uso de inteligencia artificial cuando ello sea exigible;
- f) Adoptar decisiones que afecten significativamente a personas basadas única o predominantemente en valoraciones automatizadas, sin supervisión humana significativa;
- g) Omitir el reporte oportuno de incidentes, vulnerabilidades o usos contrarios a la ética; y,
- h) Cualquier otra conducta que vulnere los principios, deberes o prohibiciones establecidos en este Reglamento o en el Reglamento de Privacidad.

Artículo 84.- Medidas preventivas. Sin perjuicio del régimen sancionador aplicable, las autoridades competentes y, en su caso, el Comité podrán adoptar medidas preventivas, formativas o restaurativas orientadas a corregir, mitigar o evitar el agravamiento de las situaciones detectadas, incluida la suspensión, restricción o desactivación de sistemas, la solicitud de remediación y la disposición de capacitación específica.

DISPOSICIONES GENERALES

PRIMERA. - Sin perjuicio de las definiciones previstas en el Reglamento de Privacidad, para la interpretación y aplicación del presente Reglamento se entenderá por:

Alfabetización en inteligencia artificial: conjunto de competencias, conocimientos y habilidades que permiten a las personas comprender, utilizar críticamente, supervisar y evaluar los sistemas de inteligencia artificial, así como identificar sus posibilidades, limitaciones y riesgos.

Alto riesgo: calificación aplicable a los sistemas de inteligencia artificial cuyo uso, por su finalidad, alcance, datos tratados o efectos potenciales, pueda producir consecuencias jurídicas, académicas, laborales, disciplinarias, financieras, sanitarias o reputacionales relevantes sobre los derechos, libertades, intereses o bienes jurídicos protegidos.

Alucinación: resultado generado por inteligencia artificial que contiene información falsa, inventada, inexacta, inconsistente o no sustentada, aunque sea presentada con apariencia de veracidad.

Auditoría: proceso documentado de revisión, evaluación y verificación, interna o externa, del cumplimiento de obligaciones jurídicas, técnicas, éticas y organizativas aplicables a un sistema de inteligencia artificial.

Calificación de riesgo: categorización del sistema de inteligencia artificial conforme al enfoque basado en niveles de riesgo previsto en el Título III del presente Reglamento.

Capacidad de inteligencia artificial embebida: funcionalidad de inteligencia artificial incorporada por un proveedor externo en una herramienta de uso ordinario — ofimática, colaboración, videoconferencia u otro servicio tecnológico contratado—, respecto de cuyo diseño, entrenamiento, modelos, filtros o funcionamiento técnico interno la Universidad no ejerce control, sin perjuicio de la regulación del uso institucional que de ella se haga.

Categorías especiales de datos o datos sensibles: datos personales relativos a origen étnico, identidad de género, identidad cultural, estado civil, orientación sexual, salud, datos biométricos y genéticos, ideología, afiliación sindical o política, antecedentes penales, condición migratoria u otros que la ley califique como tales o cuyo tratamiento incremente significativamente el riesgo para los derechos del titular.

Ciclo de vida de la IA: etapas sucesivas de un sistema de inteligencia artificial, que comprenden el diseño, la recolección y curado de datos, el entrenamiento, la validación, la prueba, el despliegue, el monitoreo, la actualización, el mantenimiento y el retiro.

Comité o CIPPIA: Comité Institucional de Protección de la Privacidad, la Información, los Datos Personales y de Uso Ético de la Inteligencia Artificial de la Universidad Metropolitana, regulado en el Reglamento de Privacidad, al cual se remite el presente Reglamento para los efectos de naturaleza, integración, sesiones, quórum y régimen de confidencialidad.

Consentimiento: manifestación de la voluntad libre, específica, informada e inequívoca por la que el titular de datos personales autoriza el tratamiento de los datos que le conciernen, conforme a la Ley Orgánica de Protección de Datos Personales.

Contenido sintético: texto, imagen, audio, vídeo o cualquier otro contenido generado, recreado o manipulado por un sistema de inteligencia artificial.

Datos personales: datos que identifican o hacen identificable a una persona natural directa o indirectamente, conforme la Ley Orgánica de Protección de Datos Personales.

Datos de entrenamiento: información utilizada para desarrollar, ajustar o mejorar el funcionamiento de un modelo de inteligencia artificial, incluidos los datos empleados en sus fases de entrenamiento, validación y prueba.

Decisión automatizada: decisión adoptada total o parcialmente sin intervención humana significativa, mediante el tratamiento automatizado de datos personales o no personales por un sistema de inteligencia artificial.

Delegado de Protección de Datos Personales: persona designada conforme a la Ley Orgánica de Protección de Datos Personales y al Reglamento General al Estatuto Institucional para asesorar, supervisar e informar respecto del cumplimiento de las obligaciones en materia de protección de datos personales.

Desarrollador: persona natural o jurídica que genera o crea un sistema de inteligencia artificial, en los términos de la Norma General SPDP-SPD-2026-0009-R.

Desplegador: persona natural o jurídica que, mediante el uso de un sistema de inteligencia artificial, ejecuta la prestación de un servicio, salvo cuando dicho uso se enmarque en una actividad personal de carácter no profesional.

Dirección de Tecnologías Informáticas: dependencia institucional prevista en el Reglamento General al Estatuto, a cuyo titular corresponden las funciones en materia de tecnologías de la información, seguridad tecnológica, ciberseguridad y soporte técnico, incluida la administración de los sistemas de inteligencia artificial institucionalmente adoptados.

Distribuidor: persona natural o jurídica que, dentro de la cadena de suministro distinta del desarrollador, desplegador o implementador, comercializa o presta un sistema de inteligencia artificial en el mercado.

Elaboración de perfiles: tratamiento automatizado de datos personales destinado a evaluar aspectos personales relativos a una persona, en particular para analizar o predecir aspectos referidos a su rendimiento, situación económica, salud, preferencias, intereses, fiabilidad, comportamiento, ubicación o movimientos.

Encargado del tratamiento: persona natural o jurídica que, sola o conjuntamente con otras, trate datos personales por cuenta del responsable del tratamiento, conforme a la Ley Orgánica de Protección de Datos Personales.

Entrenamiento: proceso mediante el cual un sistema de inteligencia artificial ajusta sus parámetros con base en datos, con el objeto de aprender patrones, reglas o representaciones útiles para sus finalidades.

Especialista en Cumplimiento: responsable funcional previsto en el Reglamento General al Estatuto, a cuyo cargo se encuentran las funciones de cumplimiento normativo y control interno, incluido el seguimiento del cumplimiento en materia de uso de

inteligencia artificial, privacidad, protección de datos personales y seguridad de la información.

Evaluación de Impacto del Tratamiento: instrumento preventivo de análisis de riesgos previsto en la Ley Orgánica de Protección de Datos Personales y su Reglamento General, destinado a identificar afectaciones potenciales a los derechos y libertades de los titulares y a definir medidas de mitigación.

Herramienta o aplicación de inteligencia artificial: programa, plataforma, servicio digital, funcionalidad o interfaz que permite al usuario utilizar uno o varios modelos de inteligencia artificial para realizar tareas determinadas, sin que el usuario controle necesariamente su diseño, entrenamiento o funcionamiento interno.

Herramienta externa no autorizada: sistema, plataforma, aplicación o servicio de inteligencia artificial que no haya sido evaluado o habilitado institucionalmente para tratar información no pública, datos personales o contenidos protegidos de la Universidad, con independencia de que sea gratuito, de pago, propietario o de acceso abierto.

Hipertruaje o deepfake: contenido sintético, especialmente de vídeo, audio o imagen, que mediante el uso de inteligencia artificial recrea, modifica o atribuye a una persona declaraciones, hechos o conductas que no realizó, con apariencia de autenticidad.

Implementador: persona natural o jurídica que encarga el desarrollo o implementa un sistema de inteligencia artificial en procedimientos o procesos internos.

Incidente: evento que afecte o pueda afectar la confidencialidad, integridad, disponibilidad, autenticidad o resiliencia de un sistema de inteligencia artificial, sus datos o sus resultados, así como toda vulneración de la protección de datos personales asociada a tales sistemas.

Inteligencia artificial o sistema de inteligencia artificial: sistema basado en máquinas, diseñado para operar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras su despliegue y que, a partir de los datos de entrada que recibe, infiere cómo generar resultados, tales como predicciones, contenidos, recomendaciones o decisiones, capaces de influir en entornos físicos o virtuales.

Inteligencia artificial embebida o incorporada: capacidad de inteligencia artificial integrada por un proveedor dentro de una herramienta ofimática, plataforma de colaboración, sistema de videoconferencia, entorno virtual de aprendizaje, motor de búsqueda, aplicación administrativa u otro servicio tecnológico de uso ordinario.

Inteligencia artificial generativa: tipo de inteligencia artificial diseñada para producir textos, imágenes, audios, vídeos, códigos, simulaciones, diseños, datos u otros

contenidos nuevos a partir de instrucciones, ejemplos o datos proporcionados por el usuario.

Inventario Institucional de Sistemas de Inteligencia Artificial: Inventario Institucional de Sistemas de Inteligencia Artificial de la Universidad Metropolitana, previsto en el artículo 27 del presente Reglamento, articulado con el Inventario de Activos de Información del Reglamento de Privacidad.

Modelo de inteligencia artificial: componente matemático, estadístico o computacional entrenado mediante datos y algoritmos para reconocer patrones, realizar inferencias o generar resultados. El modelo podrá formar parte de uno o varios sistemas, herramientas o aplicaciones de inteligencia artificial;

Modelo Técnico de Gran Escala: instrumento técnico previsto en la normativa secundaria de la Superintendencia de Protección de Datos Personales para la calificación de tratamientos como de gran escala con base en variables como número de titulares, volumen de datos, categorías, frecuencia, permanencia y alcance geográfico.

Práctica prohibida: uso de sistemas de inteligencia artificial expresamente vedado por el Capítulo II del Título III del presente Reglamento.

Privacidad desde el diseño: principio según el cual la protección de datos personales se incorpora, desde la concepción y a lo largo del ciclo de vida del sistema, en el diseño, configuración, implementación y operación de los sistemas y procesos.

Privacidad por defecto: principio según el cual los sistemas y procesos están configurados, en su estado inicial y de manera predeterminada, para tratar únicamente los datos personales estrictamente necesarios para los fines específicos del tratamiento.

Proveedor de inteligencia artificial: persona natural o jurídica que desarrolla, comercializa, licencia, aloja, administra, integra o pone a disposición de la Universidad o de sus usuarios un sistema, modelo, herramienta o servicio de inteligencia artificial.

Proctoring: supervisión electrónica de exámenes o evaluaciones académicas mediante sistemas que pueden incluir grabación de vídeo, audio, captura de pantalla, análisis de comportamiento o reconocimiento biométrico.

Reglamento de Privacidad: es el Reglamento para la Protección de la Privacidad, de la Información y de los Datos Personales de la Universidad Metropolitana, instrumento institucional general, transversal e integrador con el cual el presente Reglamento se articula conforme a los principios de especialidad, complementariedad y aplicación armónica.

Registro de Actividades de Tratamiento o RAT: documento o sistema que recoge, de manera estructurada y actualizada, las actividades de tratamiento de datos personales

realizadas por la Universidad Metropolitana, conforme a la Ley Orgánica de Protección de Datos Personales y su Reglamento General.

Registro Nacional de Protección de Datos Personales o RNPd: registro administrado por la Superintendencia de Protección de Datos Personales en el que se inscriben las bases de datos o tratamientos conforme a la Ley Orgánica de Protección de Datos Personales y a las normas secundarias aplicables.

Responsable del tratamiento: persona que decide, sola o conjuntamente con otras, sobre los fines, medios y alcance del tratamiento de datos personales. Frente a los titulares, la sociedad y el Estado, la responsable del tratamiento es la Universidad Metropolitana.

Responsable operativo: persona o unidad encargada de la administración cotidiana, uso funcional, supervisión, documentación y reporte de incidentes relacionados con un sistema de inteligencia artificial institucionalmente autorizado.

Resultado generado por inteligencia artificial: predicción, recomendación, clasificación, decisión, respuesta, resumen, texto, imagen, audio, vídeo, código, simulación, análisis u otro producto obtenido mediante un sistema de inteligencia artificial.

Riesgo: probabilidad de ocurrencia de un evento adverso que afecte derechos, libertades, intereses o bienes jurídicos protegidos, considerando su impacto y los factores de mitigación existentes.

Sesgo algorítmico: desviación sistemática en los datos, el diseño, el entrenamiento, la configuración o el uso de un sistema de inteligencia artificial que pueda producir resultados injustificados, inexactos, discriminatorios o desproporcionados respecto de determinadas personas o grupos.

SIPPID: Sistema Institucional de Protección de la Privacidad, la Información y los Datos Personales de la Universidad Metropolitana, establecido por el Reglamento de Privacidad, dentro del cual se gobierna la dimensión de inteligencia artificial conforme al presente Reglamento.

Sistema de alto riesgo: sistema de inteligencia artificial cuyo uso, por su finalidad, alcance, datos tratados, contexto o efectos previsibles, pueda producir impactos jurídicos o significativos sobre derechos, libertades, trayectoria académica, relación laboral, situación económica, salud, seguridad o patrimonio de las personas o sobre intereses esenciales de la Universidad.

Sistema institucionalmente autorizado: sistema, herramienta, aplicación o funcionalidad de inteligencia artificial cuyo uso haya sido aprobado, habilitado o reconocido por la autoridad competente, luego de cumplirse las evaluaciones técnicas,

jurídicas, presupuestarias, éticas, de seguridad de la información y de protección de datos personales que correspondan según su finalidad y nivel de riesgo.

Supervisión humana significativa: intervención humana efectiva, oportuna, dotada de capacidad real de comprender, evaluar, modificar o anular las decisiones o resultados de un sistema de inteligencia artificial, no meramente formal o aparente.

Tratamiento a gran escala: tratamiento de datos personales que, conforme a la Norma General **SPDP-SPD-2026-0005-R**, sus reformas o sustituciones afecte a una gran cantidad de datos respecto de un elevado número de titulares, con diversidad geográfica y con potencial riesgo para derechos y libertades o que se encuentre comprendido en los supuestos de calificación directa previstos en dicha norma.

Transferencia internacional: comunicación de datos personales fuera del territorio ecuatoriano, conforme a la Ley Orgánica de Protección de Datos Personales y a la Norma General **SPDP-SPD-2026-0004-R**, sus reformas o sustituciones.

Transparencia: principio en virtud del cual la información relativa a los sistemas de inteligencia artificial y a los tratamientos de datos personales es presentada en forma clara, accesible, suficiente y comprensible para los usuarios y los afectados.

Trazabilidad: capacidad de seguir, mediante registros suficientes, el origen, procesamiento, decisiones y resultados generados por un sistema de inteligencia artificial a lo largo de su ciclo de vida.

Uso personal asociado a la actividad universitaria: utilización de inteligencia artificial realizada mediante cuentas, equipos o servicios personales, pero vinculada con actividades académicas, investigativas, laborales, administrativas, contractuales o institucionales de la Universidad.

Uso institucional de inteligencia artificial: utilización de un sistema de inteligencia artificial realizada en nombre de la Universidad, con recursos institucionales, dentro de sus procesos académicos o administrativos o para producir documentos, decisiones, servicios, investigaciones o resultados vinculados con sus funciones.

Usuario institucional: autoridad, miembro de órgano colegiado, integrante del personal académico, personal de apoyo académico, personal de los procesos habilitantes de asesoría y apoyo, estudiante, investigador, practicante, pasante, proveedor, contratista o tercero autorizado que utilice sistemas de inteligencia artificial en actividades vinculadas con la Universidad.

Las definiciones previstas en esta disposición se aplicarán de acuerdo con el contexto, la finalidad y el nivel de riesgo de cada sistema. Una herramienta de uso ordinario no será tratada de la misma manera que un sistema destinado a adoptar o apoyar decisiones con

efectos jurídicos o significativos. En caso de contradicción con una definición establecida en una norma de superior jerarquía, prevalecerá esta última.

SEGUNDA. - El presente Reglamento se encuentra articulado con el Reglamento de Privacidad. En caso de conflicto material insalvable entre ambos instrumentos, prevalecerá el Reglamento general. Las dudas interpretativas se resolverán a favor de la solución que ofrezca mayor protección a los derechos fundamentales, a la dignidad de las personas, a la integridad académica y a los intereses institucionales.

TERCERA. - Las referencias contenidas en este Reglamento a leyes, reglamentos, resoluciones u otros instrumentos normativos se entenderán hechas a las disposiciones vigentes en cada momento de aplicación. En caso de modificación de la denominación, numeración o contenido de tales instrumentos, las referencias a denominaciones o numeraciones se entenderán actualizadas cuando la modificación no altere el contenido sustantivo de la norma citada. Las reformas materiales requerirán la correspondiente armonización del presente Reglamento.

CUARTA. - Toda referencia contenida en otros instrumentos normativos internos a la regulación específica de la inteligencia artificial dentro de la Universidad Metropolitana se entenderá hecha al presente Reglamento, sin perjuicio de las disposiciones generales del Reglamento de Privacidad y de las disposiciones específicas previstas en el Código de Ética Institucional, de la Investigación y el Aprendizaje y en las Políticas de Protección de Datos Personales.

QUINTA. - El Comité realizará una revisión integral del contenido, aplicación y efectividad del presente Reglamento al menos cada dos (2) años, contados a partir de su entrada en vigencia o de su última reforma sustancial. Como resultado de dicha revisión, podrá proponer al Consejo Académico Superior, a través del Rector y previo informe favorable del Consejo de Regentes en lo que corresponda, las reformas que estime necesarias.

SEXTA. - Las disposiciones del presente Reglamento son aplicables a todos los programas, actividades de docencia, investigativas o de vinculación que la Universidad Metropolitana desarrolle en virtud de convenios, alianzas o colaboraciones con personas o instituciones nacionales y extranjeras. El Comité podrá establecer protocolos específicos para la actuación en contextos internacionales, garantizando el respeto a los principios de este Reglamento, el debido proceso y la compatibilidad normativa con las jurisdicciones extranjeras implicadas.

SÉPTIMA. - Las consultas, dudas o controversias interpretativas relativas a la aplicación de este Reglamento serán absueltas por la Procuraduría Nacional, en su calidad de órgano asesor jurídico institucional, mediante criterio no vinculante, sin perjuicio de las competencias del Comité en su ámbito técnico y del Comité Universitario de Ética en el

suyo. Cuando el caso involucre simultáneamente dimensiones jurídicas, técnicas y éticas, los respectivos órganos coordinarán la emisión de criterios articulados.

OCTAVA. - Sin perjuicio del régimen general de responsabilidad de la Universidad Metropolitana como responsable del tratamiento, los integrantes de la Comunidad Universitaria responderán personalmente, en el ámbito ético, disciplinario, civil, administrativo o penal según corresponda, por el uso indebido o contrario al presente Reglamento de los sistemas de inteligencia artificial, sin perjuicio del deber perpetuo de protección de los datos personales establecido en el Reglamento de Privacidad.

DISPOSICIONES TRANSITORIAS

PRIMERA. - Los plazos previstos en el Reglamento de Privacidad para la conformación, formalización y funcionamiento del Comité son aplicables, por extensión funcional, a las atribuciones que dicho órgano ejerce en materia de inteligencia artificial conforme al presente Reglamento, sin requerir conformación distinta, ni adicional.

SEGUNDA. - En el plazo máximo de ciento veinte (120) días contados a partir de la aprobación del presente Reglamento, el Comité, en coordinación con el Vicerrectorado Administrativo, el Vicerrectorado Académico, la Dirección de Tecnologías Informáticas y el Delegado de Protección de Datos Personales, levantará el primer Inventario Institucional de Sistemas de Inteligencia Artificial, articulándolo con el Inventario de Activos de Información del SIPPID, identificará los sistemas en uso, propondrá su calificación preliminar de riesgo y formulará un plan de regularización para los sistemas que requieran adecuación a las disposiciones del presente Reglamento.

TERCERA. - En el plazo máximo de ciento ochenta (180) días contados a partir de la aprobación del presente Reglamento, el Comité elaborará y propondrá al Rector las guías, directrices, formularios y plantillas necesarios para la implementación operativa de este Reglamento, en particular, en relación con la calificación de riesgo, las Evaluaciones de Impacto del Tratamiento, las cláusulas contractuales mínimas, la información de transparencia y el reporte de incidentes.

CUARTA. - Los componentes específicos relativos a inteligencia artificial del primer plan institucional integrado de capacitación, sensibilización y alfabetización previsto en el Reglamento de Privacidad serán elaborados por el Comité dentro de los ciento ochenta (180) días siguientes a la aprobación del presente Reglamento y se incorporarán en el Plan Operativo Anual y en el presupuesto institucional inmediatamente siguiente.

QUINTA. - Los procedimientos, procesos, contrataciones y despliegues de sistemas de inteligencia artificial que se encuentren en curso a la fecha de aprobación del presente Reglamento continuarán su trámite conforme a las disposiciones vigentes al momento de su inicio, sin perjuicio de su adecuación progresiva a las exigencias de este Reglamento dentro del plan de regularización previsto en la Disposición Transitoria Segunda.

SEXTA. - Hasta tanto se expidan las guías, directrices y demás instrumentos complementarios previstos en este Reglamento, las disposiciones generales aplicables se interpretarán y aplicarán en consonancia con la Ley Orgánica de Protección de Datos Personales, su Reglamento General, la normativa secundaria de la Superintendencia de Protección de Datos Personales, el Reglamento de Privacidad, el Código de Ética Institucional, de la Investigación y el Aprendizaje y las Políticas de Protección de Datos Personales de la Universidad Metropolitana.

SÉPTIMA. - Dentro del plazo máximo de ciento ochenta días (180) días contados a partir de la aprobación del presente Reglamento, el Vicerrectorado Administrativo, en coordinación con el Delegado de Protección de Datos Personales y la Procuraduría Nacional, revisará y, de ser el caso, complementará los contratos vigentes con proveedores de sistemas de inteligencia artificial para incorporar las cláusulas mínimas previstas en el artículo 68 de este Reglamento, incluida la cláusula expresa de deber perpetuo de protección de los datos personales.

OCTAVA. - El proceso de certificación institucional bajo la norma ISO/IEC 42001:2023 se articulará dentro del plan progresivo de certificaciones previsto en el Reglamento de Privacidad. La eventual certificación institucional bajo la norma ISO/IEC 42001 se ejecutará conforme a la planificación, alcance, disponibilidad presupuestaria y aprobación de las autoridades competentes. Mientras no se disponga su implementación formal, la Universidad adoptará dichas normas como referentes metodológicos.

DISPOSICIÓN DEROGATORIA

Quedan derogadas todas las disposiciones internas de igual o inferior jerarquía que se opongan a las contenidas en el presente Reglamento o que regulen materias que ahora se entienden comprendidas en él, sin perjuicio de las disposiciones del Reglamento de Privacidad, del Código de Ética Institucional, de la Investigación y el Aprendizaje y de las Políticas de Protección de Datos Personales de la Universidad Metropolitana, las cuales se aplicarán de manera complementaria y articulada con el presente Reglamento.

DISPOSICIÓN FINAL

El presente Reglamento entrará en vigencia a partir de su aprobación por parte del Consejo Académico Superior, sin perjuicio de su publicación en los canales institucionales oficiales para conocimiento de la Comunidad Universitaria.

Dado en la ciudad de Guayaquil, en la sesión ordinaria del Consejo Académico Superior de la Universidad Metropolitana, llevada a cabo a los 31 días del mes de julio de 2026.

Ing. Alejandro Rafael Socorro Castro, PhD.

**RECTOR Y PRESIDENTE DEL CONSEJO ACADÉMICO SUPERIOR
UNIVERSIDAD METROPOLITANA**

Lo certifico:

Abg. Augusto Andrés Cueva Gaibor, Mgs.
SECRETARIO GENERAL TÉCNICO
UNIVERSIDAD METROPOLITANA

REGLAMENTO PARA EL USO ETICO, RESPONSABLE Y SEGURO DE LA INTELIGENCIA
ARTIFICIAL EN LA UNIVERSIDAD METROPOLITANA



Editorial
UMET