

POLÍTICA INSTITUCIONAL DE PRIVACIDAD DE LA UNIVERSIDAD METROPOLITANA



CONSEJO ACADÉMICO SUPERIOR

RESOLUCION No. 58-UMET-CAS-SO-07-2026

31 de julio de 2026

RESOLUCIÓN No. 58-UMET-CAS-SO-07-2026**EL CONSEJO ACADÉMICO SUPERIOR DE LA UNIVERSIDAD
METROPOLITANA****CONSIDERANDO:**

- Que, la Constitución de la República del Ecuador reconoce los derechos a la protección de datos personales, a la intimidad personal y familiar, al honor, al buen nombre, a la inviolabilidad y secreto de la correspondencia física y virtual y a la protección de la imagen, derechos que deben ser observados por la Universidad Metropolitana en el desarrollo de sus actividades académicas, administrativas, investigativas, comunicacionales, documentales y tecnológicas;
- Que, el artículo 17 de la Ley Orgánica de Educación Superior reconoce el principio de autonomía responsable de las instituciones de educación superior, en virtud del cual las universidades pueden expedir sus estatutos, reglamentos y demás normativa interna, en armonía con la Constitución y la Ley;
- Que, el artículo 18 letra e) de la Ley Orgánica de Educación Superior reconoce a las instituciones de educación superior la libertad para gestionar sus procesos internos, conforme al principio de autonomía responsable;
- Que, la Ley Orgánica de Protección de Datos Personales, su Reglamento General y la normativa secundaria aplicable establecen principios, derechos, deberes y obligaciones orientados a garantizar el tratamiento lícito, leal, transparente, seguro, proporcional y responsable de los datos personales;
- Que, la Universidad Metropolitana cuenta con normativa interna relacionada con la protección de datos personales, la privacidad, la información institucional, la inteligencia artificial, los flujos de información y comunicación y la gestión documental y de archivos, cuya aplicación requiere una política institucional específica que articule criterios generales de privacidad en los ámbitos físico, digital, académico, laboral, administrativo, investigativo, comunicacional, documental y tecnológico;
- Que, resulta institucionalmente necesario aprobar la Política Institucional de Privacidad de la Universidad Metropolitana, como instrumento complementario a la Política de Protección de Datos Personales y a los reglamentos internos vigentes, con el objeto de establecer directrices generales para la protección de la privacidad, la intimidad, la imagen, las comunicaciones, los espacios físicos y digitales, la

información personal, la trazabilidad, la confidencialidad y los límites al monitoreo institucional;

En ejercicio de las atribuciones conferidas por la Ley Orgánica de Educación Superior, el Estatuto Institucional y el Reglamento General al Estatuto de la Universidad Metropolitana, el Consejo Académico Superior,

RESUELVE:

Artículo 1.- Aprobar la **POLÍTICA INSTITUCIONAL DE PRIVACIDAD DE LA UNIVERSIDAD METROPOLITANA**, que forma parte integrante de la presente Resolución como **ANEXO 1**, comprensivo de la Matriz Técnica de Cobertura y Articulación y del texto de la Política, y disponer su aplicación obligatoria en la matriz, sedes, extensiones, centros, entornos virtuales, repositorios, plataformas, sistemas, canales oficiales, archivos físicos y digitales y demás espacios institucionales en los que la Universidad desarrolle sus funciones sustantivas, procesos gobernantes y procesos habilitantes de asesoría y apoyo.

Artículo 2.- Aprobar el **TEXTO PÚBLICO DE PRIVACIDAD, PROTECCIÓN DE DATOS PERSONALES Y COOKIES PARA PUBLICACIÓN EN EL SITIO WEB INSTITUCIONAL**, que forma parte integrante de la presente Resolución como **ANEXO 2**, y disponer que el Departamento de Comunicación, Promoción, Relaciones Públicas y Atención al Estudiante, en coordinación con la Dirección de Tecnologías Informáticas, el Delegado de Protección de Datos Personales, la Secretaría General Técnica y la Procuraduría Nacional, elimine el contenido actualmente publicado en el enlace institucional de políticas de privacidad (<https://umet.edu.ec/politicas-de-privacidad/>) y lo sustituya por el texto aprobado en el **ANEXO 2**.

La publicación deberá realizarse bajo un esquema de información por capas, con lenguaje claro, accesible y comprensible para estudiantes, aspirantes, personal, usuarios digitales y público en general, e incorporar enlaces visibles a la Política Institucional de Privacidad, a la Política de Protección de Datos Personales, a la Política de Cookies, a los términos y condiciones de uso de plataformas y al inventario básico de bases de datos, conforme a la normativa interna y a la Ley Orgánica de Protección de Datos Personales.

DISPOSICIÓN GENERAL ÚNICA

La Política Institucional de Privacidad se aplicará de manera armónica y complementaria con la Constitución de la República, la Ley Orgánica de Educación Superior, la Ley Orgánica de Protección de Datos Personales, su Reglamento General, la normativa secundaria aplicable, el Estatuto Institucional, el Reglamento General al Estatuto, la

Política de Protección de Datos Personales, el Reglamento para la Protección de la Privacidad, de la Información y de los Datos Personales, el Reglamento para el Uso Ético, Responsable y Seguro de la Inteligencia Artificial, el Reglamento del Flujo de Información y Comunicación, el Reglamento Interno del Sistema de Gestión Documental y de Archivos y demás normativa interna de la Universidad Metropolitana. Las autoridades, unidades académicas y administrativas, sedes, centros, direcciones, responsables funcionales y miembros de la Comunidad Universitaria deberán adoptar las acciones necesarias para su cumplimiento, implementación, difusión y observancia.

DISPOSICIÓN FINAL

La presente Resolución entrará en vigencia a partir de su aprobación por el Consejo Académico Superior, sin perjuicio de su publicación y socialización institucional.

Dada en la ciudad de Guayaquil, en sesión ordinaria del Consejo Académico Superior de la Universidad Metropolitana, 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

ANEXO 1

POLÍTICA INSTITUCIONAL DE PRIVACIDAD DE LA UNIVERSIDAD METROPOLITANA

Instrumento macro de gobernanza de la privacidad institucional

Aprobación: Consejo Académico Superior de la Universidad Metropolitana

Aplicación: Matriz, sedes, centros, entornos físicos, digitales e híbridos de la Universidad Metropolitana

I. MATRIZ TÉCNICA DE COBERTURA Y ARTICULACIÓN

La presente Política se formula como instrumento institucional macro de privacidad. No sustituye la Política de Protección de Datos Personales ni replica su régimen específico. La protección de datos personales constituye una de las dimensiones de la privacidad universitaria, junto con la intimidad, la imagen, la voz, la identidad, las comunicaciones, los espacios físicos y digitales, la navegación, las cookies y demás identificadores en línea, la reserva institucional, la confidencialidad, la seguridad de la información, la trazabilidad, los límites al monitoreo y la gestión responsable de tecnologías emergentes.

Fuente o instrumento	Contenido relevante	Incorporación en la Política
Constitución de la República	Derechos al honor y buen nombre, a la intimidad personal y familiar, a la inviolabilidad y secreto de la correspondencia física y virtual, a la protección de datos personales, a la imagen, al acceso a la información, al hábeas data, a la educación superior y a la autonomía responsable.	Fundamenta los principios de dignidad, privacidad, proporcionalidad, minimización, reserva, transparencia y garantía reforzada de derechos fundamentales.
Ley Orgánica de Educación Superior y normativa del SES	Autonomía responsable, libertad de gestión de procesos internos, registros académicos, funciones sustantivas, aseguramiento de la calidad y deberes de transparencia.	Habilita una política propia de una universidad particular autofinanciada y delimita la privacidad frente a los deberes de transparencia del Sistema de Educación Superior.
Ley Orgánica de Protección de Datos Personales, su	Principios, bases jurídicas, derechos de los titulares, responsable y encargado,	Se integra como dimensión específica cuando exista

Fuente o instrumento	Contenido relevante	Incorporación en la Política
Reglamento General y normativa secundaria	Delegado de Protección de Datos, evaluaciones de impacto, transferencias, gran escala, decisiones automatizadas, videovigilancia e identificadores en línea.	tratamiento de datos personales, sin convertir esta Política en duplicado de la política sectorial de datos.
Ley Orgánica para la Transformación Digital y Audiovisual; normativa de comercio electrónico, firmas y mensajes de datos; ciberseguridad y propiedad intelectual	Seguridad digital, firma electrónica, mensajes de datos, entornos digitales seguros, identidad corporativa, propiedad intelectual e información de acceso restringido.	Sustenta la privacidad digital, las cookies e identificadores en línea, las plataformas, los servicios en la nube, las comunicaciones electrónicas y la continuidad operativa.
Política de Protección de Datos Personales (Resolución No. 81-UMET-CAS-SO-09-2025)	Instrumento rector específico del tratamiento de datos personales: principios, bases legales, obligaciones, derechos, medidas técnicas y organizativas y Delegado de Protección de Datos Personales.	Opera de manera articulada y complementaria; gobierna la dimensión específica de datos personales dentro del espectro de privacidad regulado por esta Política.
Reglamento para la Protección de la Privacidad, de la Información y de los Datos Personales	SIPPID, gobernanza transversal, clasificación de la información por niveles de acceso, deberes, controles, seguridad de la información, ciberseguridad e incidentes.	Constituye la base reglamentaria de implementación; ordena responsabilidades, controles e indicadores.
Reglamento para el Uso Ético, Responsable y Seguro de la Inteligencia Artificial	Privacidad desde el diseño, gestión de riesgos, transparencia, supervisión humana, decisiones automatizadas, IA generativa, herramientas externas y prácticas prohibidas.	Aporta las reglas de privacidad aplicables a la inteligencia artificial en docencia, investigación, gestión, proctoring, analítica, admisión y atención.
Reglamento del Flujo de Información y Comunicación	Canales oficiales, sitio web, redes sociales, publicidad, mercadeo y admisiones, publicaciones, identidad corporativa, validación, trazabilidad y responsabilidades.	Ordena la privacidad en comunicaciones, publicaciones, imagen, identidad institucional, redes sociales,

Fuente o instrumento	Contenido relevante	Incorporación en la Política
		campañas, web, cookies y difusión.
Reglamento Interno del Sistema de Gestión Documental y de Archivos	Ciclo de vida documental, conservación, transferencias, eliminación, acceso e información reservada, confidencial o restringida.	Regula la privacidad en expedientes, repositorios, archivos, trabajos de titulación, consulta documental y eliminación segura.

II. POLÍTICA INSTITUCIONAL DE PRIVACIDAD

1. Objeto.

La presente Política tiene por objeto establecer los principios, criterios, directrices, responsabilidades y mecanismos institucionales aplicables a la protección integral de la privacidad en la Universidad Metropolitana, entendida como el ámbito de reserva, intimidad, autodeterminación informativa, confidencialidad, imagen, voz, identidad, comunicaciones, navegación e identificadores en línea, espacios físicos y digitales, información personal e información institucional no pública que debe ser respetado en las relaciones académicas, administrativas, laborales, investigativas, tecnológicas, documentales, comunicacionales, contractuales, de admisión, promoción, mercadeo y de relacionamiento institucional de la Universidad.

La Universidad Metropolitana, como institución particular autofinanciada de educación superior, desarrolla actividades académicas, investigativas, administrativas, de promoción, mercadeo, admisión, captación, fidelización, vinculación, empleabilidad, financiamiento, cobranza, contratación, tecnológicas, documentales, de bienestar universitario y relacionamiento institucional que, por su naturaleza, pueden incidir en la privacidad de estudiantes, aspirantes, postulantes, graduados, personal académico, personal de apoyo académico, personal de los procesos habilitantes de asesoría y apoyo, trabajadores, proveedores, contratistas, aliados, visitantes, participantes en investigación, usuarios digitales y terceros. Esta Política reconoce y disciplina, bajo criterios de privacidad, esas aristas propias del modelo de sostenibilidad institucional.

El régimen de protección de datos personales forma parte de la privacidad institucional, pero no la agota. Cuando una situación implique tratamiento de datos personales, se aplicarán de manera preferente y especializada la Ley Orgánica de Protección de Datos Personales, su Reglamento General, la normativa secundaria expedida por autoridad

competente y la Política de Protección de Datos Personales de la Universidad Metropolitana.

2. Naturaleza y articulación normativa.

La presente Política es un instrumento institucional macro de gobernanza de la privacidad. Se articula con la Constitución de la República, la Ley Orgánica de Educación Superior, la Ley Orgánica de Protección de Datos Personales, su Reglamento General, la Ley Orgánica para la Transformación Digital y Audiovisual, la normativa sobre ciberseguridad, comercio electrónico, propiedad intelectual, gestión documental, archivo, relaciones laborales y educación superior, así como con el Estatuto Institucional, el Reglamento General al Estatuto, la Política de Protección de Datos Personales, el Reglamento para la Protección de la Privacidad, de la Información y de los Datos Personales, el Reglamento para el Uso Ético, Responsable y Seguro de la Inteligencia Artificial, el Reglamento del Flujo de Información y Comunicación, el Reglamento Interno del Sistema de Gestión Documental y de Archivos, el Código de Ética Institucional, de la Investigación y el Aprendizaje, el Reglamento Interno de Trabajo, el Reglamento de Régimen Académico Institucional, el Manual de Titulación, el Manual de Identidad Corporativa y demás normativa interna aplicable.

La presente Política se aplicará de manera armónica y complementaria con el Reglamento para la Protección de la Privacidad, de la Información y de los Datos Personales, el Reglamento para el Uso Ético, Responsable y Seguro de la Inteligencia Artificial y el Reglamento del Flujo de Información y Comunicación, que constituyen instrumentos internos de implementación especializada en materia de privacidad, información, datos personales, inteligencia artificial, comunicación institucional, canales oficiales, publicaciones, plataformas, trazabilidad y controles. Esta Política no sustituye los procedimientos especiales previstos en dichos instrumentos, sino que establece criterios transversales aplicables cuando existan comunicaciones, publicaciones, accesos, monitoreos, registros, archivos, soportes tecnológicos, sistemas de información, sistemas de inteligencia artificial, cookies o identificadores en línea, repositorios, expedientes, investigaciones, campañas, espacios físicos o interacciones institucionales que puedan afectar la vida privada, la intimidad, la imagen, la voz, la identidad, las comunicaciones, los datos, la reputación o la esfera personal de integrantes de la Comunidad Universitaria o de terceros.

En caso de concurrencia normativa, se aplicarán los principios de jerarquía, especialidad, complementariedad, competencia funcional, finalidad, necesidad, proporcionalidad, minimización y protección más favorable de los derechos fundamentales, sin afectar los intereses institucionales legítimos de la Universidad.

3. Ámbito de aplicación.

La presente Política es de cumplimiento obligatorio para las primeras autoridades, autoridades académicas y administrativas, miembros del Consejo Académico Superior y del Consejo de Regentes, promotores, personal académico, personal de apoyo académico, personal de procesos habilitantes, estudiantes, aspirantes, postulantes, participantes de educación continua, graduados, exestudiantes, pasantes, practicantes, becarios, investigadores invitados, proveedores, contratistas, aliados estratégicos, consultores, visitantes y toda persona natural o jurídica que acceda, use, trate, publique, comuniqué, custodie o conozca información institucional o participe en actividades auspiciadas, financiadas, autorizadas o reconocidas por la Universidad.

Será aplicable en la matriz, sedes, extensiones, centros, escenarios académicos, entornos virtuales, plataformas institucionales, canales digitales, sistemas de información, repositorios, bibliotecas físicas o digitales, redes sociales, espacios físicos, espacios híbridos, actividades académicas, investigativas, administrativas, laborales, de vinculación, promoción, admisión, comunicación, contratación, archivo, bienestar, seguridad, auditoría, aseguramiento de la calidad y gestión documental.

4. Definiciones operativas.

Término	Definición
Privacidad institucional	Condiciones jurídicas, técnicas, organizativas, éticas y culturales que protegen intimidad, reserva, comunicaciones, imagen, voz, identidad, reputación, espacios físicos y digitales, información personal e institucional no pública frente a accesos, usos, controles, tratamientos, monitoreos o divulgaciones indebidas.
Vida privada e intimidad	Ámbitos personales, familiares, académicos, laborales, médicos, psicológicos, patrimoniales, comunicacionales o relacionales que no deben ser conocidos, registrados, difundidos o intervenidos sin habilitación jurídica suficiente.
Datos personales	Información que identifica o hace identificable a una persona natural, sujeta al régimen específico de protección de datos personales.

Término	Definición
Identificadores en línea	Datos como direcciones IP, identificadores de cookies, identificadores de dispositivo, sesión o publicidad y huellas digitales de navegador o dispositivo que, por sí solos o combinados con otra información, pueden hacer identificable a una persona. Cuando permitan identificar o hacer identificable a una persona natural, se sujetarán al régimen de protección de datos personales.
Cookies y tecnologías de seguimiento	Archivos, etiquetas, píxeles, balizas web, mecanismos de almacenamiento local, kits de desarrollo u otras tecnologías equivalentes que permiten almacenar o recuperar información del equipo, navegador, aplicación o dispositivo de una persona para fines técnicos, funcionales, de medición, personalización, seguridad, analítica, comunicación o publicidad.
Mecanismo de gestión de preferencias o consentimiento	Herramienta, procedimiento o funcionalidad institucional que permite informar, registrar, administrar, modificar o retirar preferencias o consentimientos relacionados con cookies, tecnologías de seguimiento o tratamientos no esenciales, cuando corresponda conforme a la normativa aplicable.
Información institucional no pública	Información académica, administrativa, financiera, contractual, jurídica, tecnológica, estratégica, investigativa, disciplinaria, comercial, reputacional, de seguridad o de gestión no destinada a divulgación general.
Información sensible o delicada	Información que por su naturaleza puede afectar derechos, libertades, dignidad, igualdad, seguridad, salud, intimidad, reputación, trayectoria académica, situación laboral, condición socioeconómica o intereses legítimos de una persona o de la Universidad.
Monitoreo institucional	Observación, registro, revisión, trazabilidad, auditoría o supervisión de actividades, accesos, cuentas, sistemas, canales, redes, dispositivos, plataformas o espacios institucionales, dentro de límites de

Término	Definición
	finalidad, necesidad, proporcionalidad y autorización.
Canales oficiales	Medios físicos o digitales reconocidos por la Universidad para comunicar, publicar, notificar, difundir, cargar, descargar, tramitar o conservar información institucional.
Privacidad desde el diseño y por defecto	Criterio por el cual actividades, sistemas, procesos, formularios, plataformas, convenios, campañas, proyectos, investigaciones y tecnologías incorporan medidas de privacidad desde su planificación y operan con el menor acceso, exposición o tratamiento posible.

5. Principios institucionales de privacidad

Principio	Alcance institucional
Dignidad humana y centralidad de la persona	Toda actuación institucional deberá reconocer que estudiantes, personal, usuarios, participantes y terceros no son meras fuentes de información, registros, métricas, perfiles o expedientes, sino titulares de derechos.
Legalidad y autonomía responsable	La privacidad será protegida conforme a la Constitución, la ley, la normativa de educación superior y la normativa interna, en ejercicio de la autonomía responsable de la Universidad.
Finalidad determinada	Toda intervención, registro, tratamiento, publicación, monitoreo o comunicación que pueda afectar privacidad deberá responder a una finalidad institucional legítima, explícita y verificable.
Necesidad, proporcionalidad y minimización	Solo se accederá, solicitará, registrará, comunicará o conservará información estrictamente necesaria para la finalidad autorizada.
Transparencia razonable	Las personas deberán conocer, en términos adecuados, cuándo sus datos, imagen, voz, comunicaciones, navegación, actividades,

Principio	Alcance institucional
	accesos o interacciones institucionales pueden ser registrados, revisados, monitoreados, analizados, comunicados o difundidos.
Confidencialidad y reserva	La información privada, sensible, personal, académica, laboral, médica, disciplinaria, financiera, investigativa, jurídica o estratégica solo podrá ser conocida por personas autorizadas y en función de necesidad institucional.
Seguridad de la información	La Universidad adoptará medidas técnicas, organizativas, físicas, administrativas y jurídicas para preservar confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y resiliencia de la información.
Responsabilidad proactiva y demostrable	Las autoridades, unidades y responsables funcionales deberán poder demostrar cumplimiento mediante evidencias, registros, autorizaciones, controles, informes, matrices, actas o trazas institucionales.
Privacidad desde el diseño y por defecto	Todo nuevo proceso, sistema, convenio, campaña, investigación, plataforma, formulario, sitio web, repositorio, canal digital, herramienta de inteligencia artificial o tecnología de seguimiento incorporará criterios de privacidad desde su diseño y operará con la configuración más protectora por defecto, conforme a su finalidad y nivel de riesgo.
No discriminación y protección reforzada	La privacidad de niñas, niños y adolescentes, personas con discapacidad, personas en situación de vulnerabilidad, participantes de investigación, pacientes, denunciantes, víctimas, estudiantes becados o sujetos a evaluación deberá recibir protección reforzada.
Trazabilidad y auditabilidad	Las actuaciones institucionales sobre información privada o no pública deberán dejar constancia suficiente para verificación interna y control.

Principio	Alcance institucional
Equilibrio entre privacidad e intereses institucionales legítimos	La privacidad no impedirá el ejercicio de competencias legítimas de gestión académica, seguridad, auditoría, cumplimiento normativo, defensa jurídica, administración contractual, control interno, calidad o continuidad operativa, siempre que se respeten los límites legales y proporcionales, así como los deberes de transparencia, rendición de cuentas, información pública institucional y aseguramiento de la calidad propios del Sistema de Educación Superior.

6. Gobernanza y responsabilidades

La protección de la privacidad es una responsabilidad institucional transversal que no crea estructuras nuevas, sino que se ejerce a través de la organización prevista en el Estatuto Institucional, el Reglamento General al Estatuto y la normativa interna aplicable. Su cumplimiento se articula mediante 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, este último como instancia de articulación, coordinación, seguimiento y criterio técnico, sin sustituir las competencias decisorias, operativas, técnicas, jurídicas o disciplinarias de las autoridades y unidades competentes.

Instancia	Responsabilidad principal
Consejo Académico Superior	Aprobar las Políticas, conocer reformas y ejercer las competencias normativas institucionales.
Rectorado	Dirigir la implementación institucional, emitir directrices de cumplimiento y disponer revisiones o auditorías cuando existan riesgos relevantes.
Vicerrectorado Administrativo / Responsable interno del Tratamiento	Organizar internamente el cumplimiento en materia de datos personales, privacidad operativa y gestión administrativa vinculada a tratamientos institucionales.
Delegado de Protección de Datos Personales	Asesorar, supervisar, alertar y recomendar medidas en privacidad y datos personales,

Instancia	Responsabilidad principal
	sin asumir funciones operativas o decisorias que correspondan al responsable.
Dirección de Tecnologías Informáticas	Implementar medidas técnicas de seguridad, accesos, autenticación, continuidad, respaldos, monitoreo autorizado, gestión de incidentes, soporte a plataformas y controles tecnológicos.
Procuraduría Nacional	Emitir criterios jurídicos, revisar cláusulas, instrumentos, contratos, convenios, conflictos de privacidad, defensa institucional y requerimientos de autoridad competente.
Secretaría General Técnica y Unidad de Gestión Documental y de Archivos	Aplicar reglas de gestión documental, archivo, acceso, conservación, transferencia, eliminación, documentos electrónicos y trazabilidad documental.
Departamento de Comunicación, Promoción, Relaciones Públicas y Atención al Estudiante	Gestionar canales oficiales, publicaciones, imagen institucional, redes sociales, campañas, difusión y comunicación con criterios de privacidad, pertinencia y autorización.
CRAI	Implementar reglas de privacidad en repositorios, publicaciones académicas, trabajos de titulación, consulta y acceso a recursos bibliográficos físicos o digitales.
Unidades académicas, sedes y centros	Garantizar privacidad en docencia, investigación, titulación, evaluación, tutoría, bienestar, prácticas, vinculación y procesos académicos.
Talento Humano	Garantizar privacidad laboral, expedientes de personal, procesos de selección, evaluación, bienestar, medidas disciplinarias y documentación sensible.
Cada miembro de la Comunidad Universitaria	Usar, custodiar, comunicar y proteger la información conforme a sus funciones, autorizaciones, deberes de confidencialidad y normativa interna.

7. Privacidad en la actividad académica.

La Universidad protegerá la privacidad de estudiantes, docentes, tutores, investigadores, personal de apoyo académico y participantes en procesos de aprendizaje, evaluación, tutoría, titulación, movilidad, prácticas, internados, pasantías, educación continua y actividades extracurriculares.

Las calificaciones, retroalimentaciones, actas, expedientes académicos, reportes de desempeño, registros de asistencia, alertas tempranas, sanciones académicas y situaciones de vulnerabilidad tendrán acceso limitado.

La publicación de notas, listados, resultados, *rankings*, becas, sanciones o reconocimientos deberá observar finalidad, minimización, normativa académica, transparencia y privacidad.

Las grabaciones de clases, tutorías, defensas, sustentaciones, reuniones académicas o sesiones virtuales requerirán finalidad institucional legítima, información previa y límites de acceso, conservación y difusión.

Las actividades de supervisión académica, evaluación de integridad, similitud, proctoring o verificación de autoría deberán respetar proporcionalidad, transparencia, supervisión humana y reglas específicas sobre inteligencia artificial y datos personales.

En trabajos de titulación, repositorios, tesis, artículos y publicaciones académicas se eliminarán o separarán datos personales no necesarios para la finalidad pública del documento.

8. Privacidad en investigación, innovación y vinculación.

Los proyectos de investigación, innovación, desarrollo tecnológico, vinculación con la sociedad, consultoría, transferencia de conocimiento y cooperación deberán incorporar análisis de privacidad desde su diseño, especialmente cuando involucren personas, comunidades, datos personales, datos sensibles, información de salud, niñas, niños o adolescentes, poblaciones vulnerables, comunidades indígenas, afroecuatorianas, montubias o saberes ancestrales.

Antes de recolectar información sobre seres humanos deberá verificarse la necesidad de revisión ética por el órgano competente.

Los consentimientos, asentimientos, autorizaciones comunitarias y documentos equivalentes deberán ser claros, específicos, comprensibles, separados de la versión publicable y conservados en expediente reservado.

Los datos de participantes, informantes, encuestados, entrevistados, comunidades o terceros deberán anonimizarse, pseudonimizarse o separarse cuando no sean necesarios para la publicación.

Las bases de datos de investigación deberán contar con responsables funcionales, controles de acceso, medidas de seguridad, reglas de conservación y criterios de eliminación o archivo.

La transferencia de información de investigación a patrocinadores, aliados, revistas, repositorios, proveedores o instituciones externas deberá contar con habilitación jurídica, revisión ética o contractual y control de confidencialidad.

9. Privacidad laboral y del personal.

La Universidad protegerá la privacidad del personal académico, de apoyo académico, administrativo y demás trabajadores en procesos de selección, contratación, inducción, evaluación, capacitación, nómina, seguridad social, bienestar, salud ocupacional, acciones disciplinarias, desvinculación y archivo laboral.

Los expedientes laborales, evaluaciones de desempeño, justificativos médicos, discapacidades, medidas disciplinarias, información familiar, remuneraciones, cuentas bancarias y reportes de asistencia son de acceso restringido.

El monitoreo de cuentas institucionales, accesos, dispositivos, sistemas, redes o productividad solo procederá con finalidad legítima, información previa, proporcionalidad y autorización funcional.

No se revisarán contenidos personales ajenos a la actividad institucional en dispositivos personales, salvo habilitación expresa, orden de autoridad competente o riesgo de seguridad debidamente justificado y limitado.

Las investigaciones internas deberán respetar debido proceso, confidencialidad, reserva, presunción de inocencia y protección de denunciantes, víctimas, testigos y terceros involucrados.

10. Privacidad en admisiones, promoción, mercadeo y relacionamiento comercial.

Como universidad particular autofinanciada, la UMET desarrolla actividades de admisión, promoción, mercadeo, atención a aspirantes, educación continua, relacionamiento con graduados, alianzas, eventos, campañas y comunicación comercial. Estas actividades deberán ejecutarse con respeto a la privacidad de aspirantes, postulantes, familias, empresas, instituciones, colegios, usuarios digitales y contactos comerciales.

Los formularios, campañas, CRM, ferias, webinars, llamadas, mensajes, redes sociales, sitios *web*, *landing pages*, *chats* y canales de admisión deberán informar finalidad, responsable, canales de contacto y reglas de privacidad aplicables.

Las comunicaciones promocionales deberán permitir mecanismos razonables de oposición, baja o actualización de datos cuando corresponda.

Los leads, bases de aspirantes, contactos empresariales, bases de colegios, listas de interesados y registros de eventos son información institucional no pública y deberán protegerse contra accesos, descargas, copias o transferencias no autorizadas.

El uso de segmentación, analítica, perfiles, *scoring*, automatización comercial o inteligencia artificial deberá respetar transparencia, no discriminación, control humano y normativa de datos personales.

No se publicarán testimonios, imagen, voz, historias personales, casos de éxito o trayectorias de estudiantes, graduados o familias sin habilitación suficiente o autorización cuando corresponda.

11. Privacidad financiera, becas, cobranzas y servicios administrativos.

La información financiera, contable, contractual, patrimonial, de pagos, becas, descuentos, deudas, convenios de pago, procesos de cobranza, ayudas económicas, aranceles individuales, cuentas por cobrar, proveedores y situación socioeconómica es de circulación restringida.

La comunicación sobre valores pendientes, becas, ayudas económicas, convenios de pago o medidas administrativas se realizará por canales autorizados y procurando evitar exposición pública o indebida de la situación financiera de una persona.

Los procesos de becas, descuentos o evaluación socioeconómica deberán limitar la información solicitada a la necesaria y custodiar respaldos familiares, tributarios, bancarios o laborales con acceso restringido.

La información financiera individual no podrá comunicarse a terceros sin habilitación jurídica, autorización del titular, representación válida, mandato de autoridad competente o relación contractual aplicable.

La interacción con proveedores de cobranza, pagos electrónicos, pasarelas, bancos, aseguradoras o plataformas externas deberá sujetarse a cláusulas de confidencialidad, seguridad, protección de datos y finalidad limitada.

12. Privacidad, bienestar universitario, salud y apoyos razonables.

La información relacionada con salud física o mental, discapacidad, necesidades educativas específicas, situaciones familiares, violencia, acoso, discriminación, embarazo, lactancia, orientación, identidad, condición socioeconómica, medidas de protección o apoyos razonables será tratada bajo reserva reforzada.

Solo conocerán esta información las unidades funcionalmente autorizadas y en la medida necesaria para adoptar medidas de apoyo, prevención, protección, adaptación académica o gestión institucional legítima.

Los informes psicológicos, médicos, sociales o de bienestar no podrán circular por canales abiertos ni incorporarse a documentos públicos.

La comunicación de medidas de apoyo a docentes o unidades académicas deberá limitarse a la información estrictamente necesaria para implementar la medida, sin revelar diagnósticos o detalles privados innecesarios.

Los casos de violencia, acoso, discriminación, riesgo, autolesión o emergencia se manejarán con confidencialidad, prioridad de protección, debida diligencia y coordinación con autoridades competentes cuando corresponda.

13. Espacios físicos, *campus*, videovigilancia y control de accesos.

La Universidad podrá implementar mecanismos de seguridad física, control de accesos, identificación, registro de visitantes, videovigilancia, supervisión de espacios y respuesta a emergencias para proteger personas, bienes, infraestructura, continuidad operativa y convivencia institucional.

La videovigilancia deberá tener finalidad legítima, señalética visible, zonas delimitadas, acceso restringido, plazos de conservación definidos y controles de extracción o entrega de grabaciones.

No se instalarán cámaras o dispositivos de registro en espacios donde exista expectativa reforzada de privacidad, como baños, vestidores, lactarios, espacios de atención psicológica o médica y otros equivalentes.

Las grabaciones solo serán consultadas por personal autorizado para seguridad, investigación interna, defensa jurídica, cumplimiento normativo o requerimiento de autoridad competente.

El uso de biometría, reconocimiento facial, geolocalización, controles automatizados o tecnologías de vigilancia avanzada requerirá análisis previo de necesidad, proporcionalidad, riesgos, base jurídica, impacto y medidas reforzadas.

Los eventos, ceremonias, clases abiertas, actividades deportivas, ferias, graduaciones y actos institucionales podrán ser fotografiados o grabados para fines institucionales, siempre observando información previa, respeto a la dignidad y mecanismos de oposición cuando proceda.

14. Privacidad digital, plataformas, cuentas institucionales y dispositivos.

La privacidad digital comprende el uso responsable de cuentas institucionales, correo electrónico, chats, videoconferencias, plataformas académicas, sistemas administrativos, LMS, repositorios, redes, aplicaciones, servicios en la nube, dispositivos institucionales y dispositivos personales utilizados para acceder a recursos de la Universidad.

Las cuentas institucionales, dominios, plataformas, redes y sistemas son recursos de la Universidad destinados a fines académicos, administrativos, investigativos o institucionales.

La Universidad podrá aplicar controles de seguridad, autenticación, registros de acceso, trazabilidad, monitoreo técnico, prevención de malware, respaldo, auditoría y respuesta a incidentes sobre sus recursos tecnológicos.

El monitoreo se limitará a finalidades institucionales legítimas, seguridad, continuidad, cumplimiento, prevención de incidentes, investigación interna autorizada o defensa jurídica.

Los dispositivos personales utilizados para acceder a recursos institucionales podrán estar sujetos a requisitos de seguridad. La verificación, cuando proceda, se limitará al entorno, cuenta, aplicación, perfil o contenedor institucional, sin acceso indiscriminado a contenidos privados.

El uso de servicios en la nube, aplicaciones externas, cuentas personales, repositorios no autorizados o herramientas gratuitas para información institucional estará sujeto a autorización, evaluación de riesgos, confidencialidad, seguridad y protección de datos.

15. Comunicaciones institucionales, imagen, voz y reputación.

La comunicación institucional deberá proteger la privacidad, imagen, voz, honor, buen nombre, identidad y reputación de estudiantes, personal, graduados, autoridades, terceros, participantes de investigación y aliados.

Los canales oficiales, sitio *web*, blogs, redes sociales, correos, chats, boletines, comunicados, publicaciones, campañas, materiales audiovisuales y eventos deberán observar veracidad, pertinencia, autorización, identidad institucional, no discriminación, confidencialidad y protección de datos.

La publicación de fotografías, videos, testimonios, entrevistas, historias de vida, resultados académicos, casos disciplinarios, información médica, financiera o familiar requerirá habilitación institucional y, cuando corresponda, autorización de la persona titular.

Las crisis reputacionales, incidentes, controversias, procesos judiciales, investigaciones disciplinarias, auditorías o asuntos jurídicos sensibles serán comunicados únicamente por autoridades o voceros autorizados.

Los grupos de mensajería, chats institucionales y canales informales autorizados no podrán utilizarse para difundir información privada, rumores, documentos reservados, datos personales, claves, capturas de sistemas, decisiones no aprobadas o información no verificada.

16. Gestión documental, archivos, repositorios y trabajos de titulación.

La gestión documental y archivística de la Universidad deberá proteger la privacidad durante todo el ciclo de vida documental: producción, recepción, registro, clasificación, organización, descripción, trámite, consulta, conservación, transferencia, valoración, disposición final, eliminación y preservación.

Los expedientes académicos, laborales, disciplinarios, financieros, contractuales, jurídicos, investigativos, médicos, psicológicos y administrativos tendrán niveles de acceso acordes con su naturaleza.

La clasificación de información reservada, confidencial o restringida se aplicará conforme a la normativa institucional y deberá constar de manera motivada cuando corresponda.

La eliminación documental que contenga información privada o datos personales deberá ser segura, irreversible, documentada y conforme a la Tabla de Plazos de Conservación Documental y a los procedimientos institucionales.

Los trabajos de titulación, tesis, proyectos, artículos, estudios de caso, informes de investigación y documentos equivalentes publicados en repositorios no deberán contener cédulas, pasaportes, direcciones, teléfonos, correos personales, firmas manuscritas, datos

bancarios, información de salud, datos biométricos, información socioeconómica, datos familiares, documentos de identidad u otros datos innecesarios.

Los datos requeridos para validación administrativa, registro o titulación se entregarán en hoja, formulario o anexo separado, no publicable, destinado al expediente académico-administrativo.

El CRAI implementará controles de revisión formal y privacidad en recepción, carga, publicación, custodia y consulta de trabajos de titulación y repositorios, en coordinación con unidades académicas, Secretaría General Técnica, DTI y Delegado de Protección de Datos Personales.

17. Inteligencia artificial, analítica, automatización y tecnologías emergentes.

El uso de inteligencia artificial, analítica avanzada, sistemas predictivos, automatización, *proctoring*, reconocimiento, clasificación, generación de contenidos, *chatbots*, asistentes virtuales, herramientas de detección, plataformas adaptativas o sistemas externos deberá realizarse bajo privacidad desde el diseño, gestión de riesgos, supervisión humana y trazabilidad.

Todo sistema de IA que pueda tratar información personal, académica, laboral, financiera, sensible, estratégica o no pública deberá evaluarse antes de su adquisición, contratación, desarrollo, despliegue o uso institucional.

No se utilizará IA para vigilancia, perfilamiento, decisiones automatizadas significativas, evaluación académica o laboral, admisión, becas, sanciones o asignación de beneficios sin base jurídica, transparencia, control humano, proporcionalidad y medidas de mitigación.

Los resultados generados por IA no podrán publicarse o utilizarse como información institucional definitiva sin revisión humana competente.

No se ingresará información confidencial, datos sensibles, expedientes, claves, contratos, información jurídica, financiera, disciplinaria, académica no pública o datos personales en herramientas externas no autorizadas.

Las herramientas de detección de similitud, autoría o uso de IA deberán tratarse como instrumentos auxiliares, no como prueba única o automática de infracción.

18. Terceros, proveedores, aliados y transferencias.

La Universidad podrá contratar o relacionarse con proveedores tecnológicos, plataformas educativas, servicios de nube, pasarelas de pago, servicios de seguridad, agencias de

comunicación, consultores, aliados académicos, instituciones públicas o privadas, redes de investigación, organismos internacionales y otros terceros. Toda relación que implique acceso a información institucional, privacidad o datos personales deberá documentarse adecuadamente.

Los contratos, convenios, órdenes de compra, términos de referencia, anexos o acuerdos deberán incluir cláusulas de confidencialidad, privacidad, protección de datos, seguridad de la información, subcontratación, transferencias, retorno o eliminación de información, auditoría, incidentes y responsabilidad.

Las transferencias nacionales o internacionales de datos o información deberán cumplir la normativa aplicable, la Política de Protección de Datos Personales y los controles institucionales.

Los terceros solo podrán usar información institucional para las finalidades autorizadas y no podrán reutilizarla para entrenamiento de modelos, mercadeo propio, análisis, cesión, publicación o fines distintos sin autorización expresa.

Los proveedores deberán notificar incidentes de seguridad, accesos no autorizados, vulnerabilidades o afectaciones a la privacidad en los términos contractuales e institucionales.

19. Privacidad en disciplina, auditoría, cumplimiento y defensa jurídica.

La privacidad no impedirá a la Universidad ejercer funciones de control, auditoría, cumplimiento, investigación interna, régimen disciplinario, defensa judicial, gestión contractual, seguridad o atención de requerimientos de autoridad competente. Estas actuaciones deberán respetar legalidad, competencia, necesidad, proporcionalidad, reserva, debido proceso y trazabilidad.

Los expedientes disciplinarios, denuncias, informes de auditoría, investigaciones internas, criterios jurídicos, estrategias procesales, comunicaciones con abogados, contratos, convenios y documentos de defensa institucional tendrán acceso restringido.

La información de denunciantes, víctimas, testigos, investigados y terceros se protegerá conforme al nivel de riesgo y a la normativa aplicable.

La Procuraduría Nacional coordinará la gestión jurídica de información sensible en asuntos judiciales, administrativos, arbitrales, constitucionales, contractuales y extrajudiciales.

La comunicación externa sobre controversias, litigios, investigaciones o asuntos jurídicos sensibles requerirá autorización de la autoridad competente y coordinación con Procuraduría Nacional y Comunicación institucional.

20. Gestión de riesgos, incidentes y medidas de protección.

La Universidad gestionará los riesgos de privacidad de forma preventiva, documentada y proporcional. Se consideran riesgos de privacidad, entre otros, el acceso no autorizado, pérdida, destrucción, modificación, divulgación, publicación indebida, monitoreo desproporcionado, perfilamiento no autorizado, suplantación, filtración, uso de herramientas externas, transferencias no controladas, tratamiento excesivo, fallas de seguridad, error humano, ingeniería social, uso indebido de IA y exposición de información en repositorios o redes sociales.

Las unidades deberán reportar incidentes o sospechas de incidentes a través de los canales institucionales establecidos.

DTI, el Delegado de Protección de Datos Personales, el Responsable interno del Tratamiento, Procuraduría Nacional, Comunicación, Secretaría General Técnica y las unidades competentes actuarán según la naturaleza del incidente.

Las medidas de contención podrán incluir bloqueo de accesos, retiro de publicaciones, cambio de credenciales, preservación de evidencias, comunicación a afectados, notificación a autoridades, medidas disciplinarias, revisión contractual o acciones legales.

Los incidentes se documentarán para asegurar trazabilidad, análisis de causa, medidas correctivas, prevención y mejora continua.

21. Lineamientos de implementación.

Línea de implementación	Criterio operativo
Diseño y revisión previa	Todo nuevo proceso, formulario, plataforma, campaña, convenio, investigación, sistema de IA o canal de comunicación deberá incorporar análisis de privacidad desde su planificación.
Clasificación y acceso	La información deberá clasificarse y accederse por necesidad funcional, rol autorizado, finalidad y nivel de riesgo.
Autorizaciones y validaciones	Las publicaciones o tratamientos sensibles requerirán validación de autoridad

Línea de implementación	Criterio operativo
	competente y criterio de unidades especializadas cuando corresponda.
Capacitación	La Universidad desarrollará capacitaciones periódicas sobre privacidad, datos personales, seguridad, IA, comunicación responsable y gestión documental.
Evidencia de cumplimiento	Las unidades conservarán registros, matrices, actas, autorizaciones, informes, trazas o respaldos que demuestren cumplimiento.
Mejora continua	Las Políticas serán revisadas periódicamente y actualizada ante cambios legales, tecnológicos, institucionales, regulatorios o de riesgo.

22. Relación con la Política de Protección de Datos Personales.

La Política de Protección de Datos Personales de la Universidad Metropolitana constituye el instrumento rector específico para el tratamiento de datos personales. La presente Política opera como instrumento macro de privacidad institucional y se aplica a escenarios más amplios, incluyendo aquellos en los que no necesariamente existe tratamiento de datos personales, pero sí afectación posible a la intimidad, imagen, comunicaciones, espacios físicos o digitales, confidencialidad, reputación, reserva institucional, seguridad de la información o esfera privada de las personas.

Cuando exista tratamiento de datos personales, se aplicará la Política de Protección de Datos Personales. Cuando el caso involucre además privacidad institucional amplia, comunicación, archivo, IA, monitoreo, publicación, imagen, voz, espacios o seguridad, se aplicarán de forma complementaria ambos instrumentos y los reglamentos específicos correspondientes.

23. Revisión, interpretación y actualización.

La interpretación técnica de esta Política corresponderá a las instancias competentes según la materia: Delegado de Protección de Datos Personales, Dirección de Tecnologías Informáticas, Secretaría General Técnica, Unidad de Gestión Documental y de Archivos, Comunicación institucional, CRAI, Talento Humano, unidades académicas y demás responsables funcionales. La interpretación jurídica corresponderá a la Procuraduría

Nacional, sin perjuicio de la facultad normativa e interpretativa general del Consejo Académico Superior.

La Política será revisada cuando existan reformas constitucionales, legales, reglamentarias, estatutarias o institucionales; nuevas normas de la Superintendencia de Protección de Datos Personales; cambios relevantes en IA, ciberseguridad o transformación digital; incidentes significativos; auditorías; recomendaciones de órganos internos; o necesidades derivadas de la gestión universitaria.

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

Elaborado por: Mauricio López Ochoa
Procurador Nacional

ANEXO 2

TEXTO PÚBLICO DE PRIVACIDAD, PROTECCIÓN DE DATOS PERSONALES Y COOKIES PARA PUBLICACIÓN EN EL SITIO WEB INSTITUCIONAL

1. Instrucción técnica de publicación

El contenido del enlace institucional <https://umet.edu.ec/politicas-de-privacidad/> deberá ser sustituido íntegramente por el presente Anexo. La publicación deberá organizarse mediante un modelo de información por capas, de la siguiente manera:

Capa	Contenido	Forma de publicación
Primera capa	Mensaje breve y principal sobre privacidad, datos personales y cookies	Visible al abrir la página
Segunda capa	Secciones desplegables sobre qué protege la UMET, qué datos trata, para qué los usa, cookies, derechos y contacto	Formato acordeón o bloques diferenciados
Tercera capa	Enlaces a documentos completos	Botones o enlaces visibles a documentos institucionales
Gestión de cookies	Controles visibles para aceptar, rechazar o configurar cookies no necesarias	Banner o panel de preferencias
Actualización	Fecha de última actualización y versión vigente	Parte final de la página

El texto deberá publicarse en lenguaje claro, sin eliminar su rigor jurídico. No deberán usarse expresiones ajenas al giro institucional universitario ni referencias a autoridades extranjeras o no competentes en el Ecuador.

2. Texto público para publicación.

Privacidad, protección de datos personales y cookies

La Universidad Metropolitana, UMET, respeta y protege la privacidad de las personas que integran o se relacionan con su Comunidad Universitaria.

Esta página explica, de forma clara, cómo la Universidad protege la privacidad, cómo trata los datos personales y cómo utiliza cookies y tecnologías similares en sus sitios web, plataformas y canales digitales.

La privacidad no se limita a los datos personales. También comprende la intimidad, imagen, voz, identidad, comunicaciones, navegación web, espacios físicos y digitales, información académica, laboral, financiera, investigativa, documental y demás información institucional no pública.

La protección de datos personales es una parte específica de la privacidad y se rige por la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales, su Reglamento General, la normativa secundaria aplicable y la Política de Protección de Datos Personales de la UMET.

3. ¿A quién aplica esta información?

Esta información aplica a:

- a) Estudiantes, aspirantes, postulantes, graduados y exestudiantes;
- b) Personal académico, personal de apoyo académico, personal administrativo y trabajadores;
- c) Participantes de educación continua, cursos, eventos, congresos, ferias, actividades académicas, investigativas o de vinculación;

- d) Proveedores, contratistas, aliados estratégicos, visitantes y terceros relacionados con la Universidad;
- e) Usuarios que navegan en el sitio web institucional, completan formularios, usan plataformas, redes sociales, chats, correos, servicios digitales o canales de atención de la UMET.

4. ¿Qué protege la UMET?

La UMET protege la privacidad en sus actividades académicas, administrativas, laborales, investigativas, tecnológicas, comunicacionales, documentales, de admisión, promoción, mercadeo, cobranza, bienestar universitario, seguridad, archivo y gestión institucional.

Esto incluye, entre otros aspectos:

- a) Datos personales e información de contacto;
- b) Información académica, calificaciones, expedientes, titulaciones, becas, prácticas y movilidad;
- c) Información laboral, contractual, financiera, contable y administrativa;
- d) Información de salud, discapacidad, bienestar universitario o situaciones de vulnerabilidad, cuando corresponda;
- e) Imagen, voz, fotografías, videos, testimonios y grabaciones;
- f) Información de navegación, cookies, identificadores en línea, direcciones IP y registros de acceso;
- g) Comunicaciones institucionales, correos, chats, plataformas académicas, sistemas administrativos y entornos virtuales;
- h) Información contenida en archivos físicos, archivos digitales, repositorios, trabajos de titulación y documentos institucionales;

i) Información usada en sistemas de inteligencia artificial, analítica, automatización o tecnologías emergentes, cuando corresponda.

5. ¿Qué datos personales puede tratar la Universidad?

La UMET puede tratar datos personales necesarios para cumplir sus funciones académicas, administrativas, contractuales, legales, tecnológicas, comerciales, investigativas y de gestión institucional.

Entre ellos pueden encontrarse:

- a) Nombres, apellidos, número de identificación, nacionalidad, fecha de nacimiento y datos de contacto;
- b) Información académica, historial estudiantil, calificaciones, asistencia, certificados, títulos y documentos de titulación;
- c) Información laboral, profesional, contractual, financiera, de pagos, becas, descuentos, convenios, cobranza y facturación;
- d) Datos de representantes legales, padres, madres o contactos de emergencia, cuando corresponda;
- e) Información necesaria para bienestar universitario, inclusión, apoyos razonables, salud ocupacional o atención de situaciones de vulnerabilidad;
- f) Imágenes, voz, fotografías, videos y grabaciones de actividades institucionales;
- g) Datos de acceso a plataformas, registros de sesión, dirección IP, cookies, identificadores de dispositivo, navegación y uso de servicios digitales;
- h) Datos necesarios para seguridad física, control de accesos, videovigilancia y protección de personas, bienes e infraestructura;

i) Datos tratados por sistemas académicos, administrativos, bibliotecas digitales, repositorios, aulas virtuales, plataformas de educación continua, sistemas de atención, canales web o redes sociales institucionales.

La UMET no solicitará ni tratará datos que no sean necesarios para una finalidad legítima, salvo habilitación legal o autorización válida cuando corresponda.

6. ¿Para qué utiliza la UMET los datos personales?

La UMET puede utilizar datos personales para finalidades legítimas relacionadas con:

- a) Admisión, postulación, inscripción, matrícula y gestión académica;
- b) Prestación de servicios educativos, administrativos, bibliotecarios, tecnológicos y de bienestar universitario;
- c) Gestión de carreras, programas, cursos, educación continua, prácticas, pasantías, titulación, movilidad, investigación y vinculación;
- d) Atención de solicitudes, consultas, reclamos, requerimientos, trámites y comunicaciones institucionales;
- e) Gestión financiera, facturación, pagos, becas, descuentos, convenios, cobranza y obligaciones contables o tributarias;
- f) Cumplimiento de obligaciones legales, académicas, laborales, contractuales, regulatorias y de educación superior;
- g) Seguridad física y digital, control de accesos, videovigilancia, ciberseguridad, prevención de fraude, continuidad operativa y gestión de incidentes;
- h) Promoción, admisión, mercadeo, campañas informativas, eventos, ferias, seguimiento a aspirantes, relacionamiento con graduados y comunicación institucional;

- i) Elaboración de estadísticas, reportes, indicadores, mejora de servicios, aseguramiento de la calidad y planificación institucional;
- j) Gestión documental, archivo, conservación, consulta, transferencia, eliminación segura y preservación de documentos institucionales;
- k) Uso de plataformas tecnológicas, servicios en la nube, herramientas académicas, sistemas administrativos y tecnologías emergentes;
- l) Cumplimiento de órdenes de autoridad competente o atención de requerimientos administrativos, judiciales o regulatorios.

7. ¿La UMET comparte datos personales con terceros?

La UMET puede compartir datos personales cuando exista una base jurídica válida, una finalidad legítima y garantías adecuadas.

Esto puede ocurrir con:

- a) Organismos del Sistema de Educación Superior;
- b) Autoridades públicas, judiciales, administrativas o de control, cuando corresponda;
- c) Proveedores tecnológicos, plataformas académicas, servicios en la nube, pasarelas de pago, servicios de comunicación, seguridad, soporte o gestión institucional;
- d) Aliados académicos, instituciones de investigación, redes de cooperación, convenios de movilidad o prácticas;
- e) Auditores, asesores, abogados, consultores, aseguradoras, bancos, gestores de servicios o contratistas, cuando sea necesario para la operación institucional.

Los terceros deberán cumplir obligaciones de confidencialidad, seguridad, protección de datos personales, uso limitado de la información y notificación de incidentes, conforme a la normativa aplicable y a los instrumentos contractuales correspondientes.

La UMET no venderá datos personales y únicamente lo usará para sus finalidades, sea de manera directa o por medio de encargados debidamente contratados mediante acuerdos que contengan las seguridades técnicas y jurídicas exigidas por la ley.

8. *Cookies* y tecnologías similares

La UMET puede utilizar cookies y tecnologías similares en su sitio web, plataformas, formularios, campañas, redes sociales o servicios digitales.

Las cookies son pequeños archivos o tecnologías que permiten reconocer el navegador, dispositivo o sesión de una persona usuaria. También pueden emplearse identificadores en línea, píxeles, etiquetas, almacenamiento local, herramientas de medición, analítica o tecnologías equivalentes.

La UMET podrá usar *cookies* para:

- a) Permitir el funcionamiento técnico del sitio web o plataforma;
- b) Mantener la seguridad de la navegación;
- c) Recordar preferencias de idioma, accesibilidad o configuración;
- d) Medir el uso del sitio web y mejorar sus contenidos;
- e) Analizar el rendimiento de campañas institucionales;

- f) Facilitar formularios, servicios digitales, admisiones, solicitudes de información o atención institucional;
- g) Gestionar publicidad institucional o comunicación digital, cuando corresponda y conforme a la ley.

Las *cookies* estrictamente necesarias no requieren consentimiento previo porque permiten que el sitio o plataforma funcione correctamente. Las demás cookies, como las de medición, personalización, analítica o publicidad, requerirán información previa y consentimiento cuando corresponda.

La persona usuaria podrá aceptar, rechazar o configurar cookies no necesarias mediante los controles visibles que habilite la Universidad. La desactivación de determinadas cookies puede limitar o impedir algunas funcionalidades del sitio o de los servicios digitales.

La UMET publicará y mantendrá actualizada una Política de Cookies con información sobre tipos de cookies, finalidades, base jurídica, plazos de conservación, terceros que pueden acceder a la información y mecanismos para otorgar, denegar o revocar el consentimiento.

9. Seguridad de la información

La UMET aplica medidas técnicas, organizativas, físicas, administrativas y jurídicas para proteger la información contra pérdida, alteración, acceso no autorizado, uso indebido, divulgación no autorizada, destrucción, incidentes de seguridad o afectaciones a la privacidad.

Estas medidas pueden incluir controles de acceso, autenticación, gestión de permisos, respaldo, cifrado, trazabilidad, monitoreo de seguridad, gestión de incidentes, revisión de proveedores, capacitación y controles documentales.

Ningún sistema es absolutamente infalible, porque la humanidad conectó todo a internet y luego se sorprendió de que existieran riesgos. Aun así, la UMET implementará medidas razonables y proporcionales al nivel de riesgo de la información tratada.

10. Privacidad en publicaciones, fotografías, videos y redes sociales

La UMET puede publicar información institucional, fotografías, videos, entrevistas, testimonios, noticias, actividades académicas, eventos, ceremonias, logros, campañas o contenidos de interés universitario en sus canales oficiales.

Cuando dichas publicaciones involucren imagen, voz, datos personales, testimonios, información sensible o situaciones particulares de personas, la Universidad aplicará criterios de finalidad, pertinencia, proporcionalidad, minimización, autorización cuando corresponda, protección reforzada y respeto a la dignidad.

No se publicará información académica, financiera, médica, disciplinaria, laboral, familiar, socioeconómica o privada que no sea necesaria para una finalidad institucional legítima o que pueda afectar derechos de las personas.

11. Trabajos de titulación, repositorios y archivos

La UMET puede publicar trabajos de titulación, tesis, proyectos, artículos, estudios de caso, informes de investigación u otros documentos académicos en repositorios, bibliotecas físicas o digitales y plataformas institucionales, conforme a la normativa de educación superior y a sus procedimientos internos.

La versión publicable de estos documentos no deberá incluir datos personales innecesarios, tales como números de cédula o pasaporte, direcciones domiciliarias, teléfonos personales, correos personales, firmas manuscritas, datos bancarios, información de salud, datos biométricos, información socioeconómica, datos familiares, copias de documentos de identidad o datos de participantes de investigación que no sean necesarios para la finalidad académica.

Cuando esos datos sean necesarios para trámites administrativos, validación, archivo o titulación, deberán entregarse en documentos separados que no serán publicados en repositorios o plataformas públicas.

12. Inteligencia artificial y tecnologías emergentes

La UMET puede utilizar herramientas tecnológicas, sistemas de inteligencia artificial, analítica, automatización o plataformas digitales para mejorar sus actividades académicas, administrativas, investigativas, de admisión, atención y gestión institucional.

Cuando estas herramientas puedan incidir en la privacidad o tratar datos personales, la Universidad aplicará reglas de privacidad desde el diseño, evaluación de riesgos, transparencia, supervisión humana, seguridad, minimización y control institucional.

No se utilizarán sistemas de inteligencia artificial para tomar decisiones automatizadas relevantes sobre estudiantes, personal o terceros sin base jurídica, información suficiente, supervisión humana y garantías adecuadas.

13. Derechos de las personas titulares de datos personales

Las personas titulares de datos personales pueden ejercer los derechos reconocidos en la normativa ecuatoriana, incluyendo, según corresponda:

- a) Acceso;
- b) Rectificación y actualización;
- c) Eliminación o supresión;
- d) Oposición;
- e) Suspensión del tratamiento;
- f) Portabilidad;

- g) No ser objeto de decisiones basadas únicamente en valoraciones automatizadas, cuando corresponda;
- h) Revocatoria del consentimiento, cuando el tratamiento se base en consentimiento;
- i) Información sobre el uso, finalidad, origen, destino y plazo de conservación de sus datos.

El ejercicio de estos derechos se atenderá conforme a la Ley Orgánica de Protección de Datos Personales, su Reglamento General, la normativa secundaria aplicable y los procedimientos institucionales de la UMET.

La eliminación o supresión de datos no procederá cuando exista una obligación legal, contractual, académica, administrativa, financiera, contable, judicial, disciplinaria, documental o institucional que exija conservarlos durante un tiempo determinado.

14. Contacto para privacidad y protección de datos personales

Las solicitudes, consultas o requerimientos relacionados con privacidad y protección de datos personales podrán dirigirse a los canales institucionales que publique la Universidad Metropolitana.

La UMET informará en esta página los canales actualizados para:

- a) Ejercer derechos sobre datos personales;
- b) Consultar sobre privacidad;
- c) Reportar incidentes o posibles usos indebidos de información;
- d) Solicitar información sobre cookies o tecnologías de seguimiento;

e) Contactar al Delegado de Protección de Datos Personales, cuando corresponda, para lo cual señalará:

- **Nombre**
- **Correo institucional**
- **Teléfono y extensión**
- **Dirección física**

15. Documentos institucionales relacionados

Para mayor información, la UMET pondrá a disposición del público los siguientes documentos:

- a) Política Institucional de Privacidad;
- b) Políticas de Protección de Datos Personales;
- c) Términos y condiciones de uso de plataformas institucionales;
- d) Inventario básico de bases de datos o registro informativo de tratamientos, en la versión publicable que corresponda;
- e) Reglamento para la Protección de la Privacidad, de la Información y de los Datos Personales;
- f) Reglamento para el Uso Ético, Responsable y Seguro de la Inteligencia Artificial;
- g) Reglamento del Flujo de Información y Comunicación;
- h) Reglamento Interno del Sistema de Gestión Documental y de Archivos.

16. Aviso final

Esta página contiene una síntesis pública, clara y accesible de las reglas institucionales de privacidad, protección de datos personales y cookies de la Universidad Metropolitana.

En caso de diferencia entre esta síntesis y los instrumentos institucionales aprobados, prevalecerán la Constitución, la Ley Orgánica de Protección de Datos Personales, su Reglamento General, la normativa secundaria aplicable y los textos íntegros de las políticas y reglamentos internos de la Universidad.

Nota técnica para implementación *web*:

Bloque visible	Contenido
Encabezado	“Privacidad, protección de datos personales y cookies”
Primer párrafo	Texto breve sobre privacidad y protección de datos
Botones iniciales	“Ver Política Institucional de Privacidad”, “Ver Políticas de Protección de Datos Personales”, “Configurar cookies”
Acordeón 1	¿Qué protege la UMET?
Acordeón 2	¿Qué datos personales tratamos?
Acordeón 3	¿Para qué usamos los datos?
Acordeón 4	<i>Cookies</i> y tecnologías similares
Acordeón 5	Derechos de los titulares

Bloque visible	Contenido
Acordeón 6	Contacto
Footer	Última actualización, versión y enlaces a documentos completos

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**

**Elaborado por: Mauricio López Ochoa
Procurador Nacional**

POLÍTICA INSTITUCIONAL DE PRIVACIDAD DE LA UNIVERSIDAD METROPOLITANA



Editorial
UMET