

REGLAMENTO DEL FLUJO DE INFORMACIÓN Y COMUNICACIÓN DE LA UNIVERSIDAD METROPOLITANA

CONSEJO ACADÉMICO SUPERIOR

RESOLUCIÓN No. 57-UMET-CAS-SO-07-2026

31 de julio de 2026

RESOLUCIÓN No. 57-UMET-CAS-SO-07-2026**EL CONSEJO ACADÉMICO SUPERIOR DE LA UNIVERSIDAD METROPOLITANA
CONSIDERANDO:**

Que, en Registro Oficial Suplemento N.º 297 de 02 de agosto de 2018 fue publicada la Ley Orgánica Reformatoria a la Ley Orgánica de Educación Superior (LOES). En su Art. 12 establece que:

“El Sistema de Educación Superior se rige por los principios de autonomía responsable, cogobierno, igualdad de oportunidades, calidad, pertinencia, integralidad, autodeterminación para la producción del pensamiento y conocimiento, en el marco del diálogo de saberes, pensamiento universal y producción científica y tecnológica global.

El Sistema de Educación Superior, al ser parte del Sistema Nacional de Inclusión y Equidad Social, se rige por los principios de universalidad, igualdad, equidad, progresividad, interculturalidad, solidaridad y no discriminación; y funcionará bajo los criterios de calidad, eficiencia, eficacia, transparencia, responsabilidad y participación.

Estos principios rigen de manera integral a las instituciones, actores, procesos, normas, recursos, y demás componentes del sistema, en los términos que establece esta Ley”:

Que, el Art. 17 de la LOES dispone que:

“El Estado reconoce a las universidades y escuelas politécnicas autonomía académica, administrativa, financiera y orgánica, acorde con los principios establecidos en la Constitución de la República.

En el ejercicio de autonomía responsable, las universidades y escuelas politécnicas mantendrán relaciones de reciprocidad y cooperación entre ellas y de estas con el Estado y la sociedad; además observarán los principios de justicia, equidad, solidaridad, participación ciudadana, responsabilidad social y rendición de cuentas.

Se reconoce y garantiza la naturaleza jurídica propia y la especificidad de todas las universidades y escuelas politécnicas”;

Que, en cuanto al ejercicio de la autonomía responsable de las instituciones de educación superior la LOES dispuso la libertad para gestionar sus procesos internos (artículo 18, letra e).

Que, la Ley Orgánica para la Transformación Digital y Audiovisual, publicada en el Registro Oficial No. 245 con fecha del 7 de febrero de 2023, en su artículo 4 sobre la transformación digital, establece: *“La Transformación Digital constituye el proceso continuo de adopción multimodal de tecnologías digitales que cambian fundamentalmente la forma en que los servicios gubernamentales y del sector privado se idean, planifican, diseñan, implementan y operan, con el objeto de mejorar la eficiencia, seguridad, certeza, velocidad y calidad de los servicios, optimizando sus costos y mejorando las condiciones de transparencia de los procesos y actuaciones del Estado en su interrelación con los ciudadanos”.*

Que, la Ley Orgánica de Protección de Datos Personales, publicada en el Registro Oficial No.

459 de fecha 26 de mayo de 2021 en sus artículos 1, 10 y 47, y su Reglamento General, publicado en el Registro Oficial Tercer Suplemento 435 el 13 de noviembre de 2023, instituyen el objeto, los principios de confidencialidad y la responsabilidad proactiva que regulan las obligaciones de los responsables del tratamiento de información; marco jurídico ante el cual la Universidad Metropolitana, en ejercicio de su autonomía responsable y de su obligación de asegurar el debido proceso y la seguridad jurídica institucional, debe adoptar disposiciones internas vinculantes que garanticen el tratamiento lícito, confidencial y proporcional de los datos personales y sensibles bajo su custodia, mitigando así de manera efectiva todo riesgo legal o tecnológico que pueda comprometer los derechos fundamentales de su comunidad académica.

Que, en el Quinto Suplemento del Registro Oficial N.º 290 de 22 de mayo de 2026, se publicó la Ley Orgánica para el Fortalecimiento de la Ciberseguridad. Esta Ley reformó varios cuerpos legales con relación al fortalecimiento de la ciberseguridad nacional como condición habilitante de la transformación digital, garantizando la protección de servicios esenciales, infraestructura crítica digital, derechos fundamentales y confianza en el ecosistema digital. Esta Ley reformó de manera transversal el ordenamiento jurídico en materia de transformación digital, estableciendo un nuevo marco nacional para salvaguardar los servicios esenciales, la infraestructura crítica digital y los derechos fundamentales; marco normativo que impone a las instituciones de educación superior la obligación de robustecer sus sistemas informáticos y adecuar sus contenidos académicos en seguridad digital, haciendo indispensable que la Universidad Metropolitana incorpore estas directrices en sus procesos de gobernanza con el fin de garantizar el debido proceso y la confianza en su ecosistema, previniendo de forma proactiva incidentes o contingencias tecnológicas en su comunidad académica.

Que, el Estatuto de la Universidad Metropolitana fue aprobado mediante la Resolución No. 60-UMET- CAS-SE-06-2024 en su segundo debate, en la sexta sesión extraordinaria, realizada el 16 de diciembre de 2024, validado por el Consejo de Educación Superior mediante la RPC-SO-03-No.037-2025 de fecha 22 de enero de 2025 y reformado con fecha 8 de mayo de 2026 en su segundo debate mediante la Resolución N.º 04-2026. En la norma se señala entre los fines articulados al Modelo Educativo Pedagógico, artículo 6, letra n: “[...] *n) Consolidar la transformación digital de las mallas curriculares y de todos los procesos de gestión universitaria, así como contribuir a la transformación digital y audiovisual de la educación, de la educación superior y la sociedad ecuatoriana; [...]*”

Que, el Reglamento General al Estatuto institucional, aprobado mediante la Resolución No. 17-UMET-CAS-SE-03-2026 con fecha 24 de marzo de 2026, señala entre sus objetivos: “[...] *4) Orientar los procesos de innovación institucional, la transformación digital, la innovación educativa y su contribución a la democratización del conocimiento, la ampliación del acceso a la educación superior y la proyección social de alto impacto en la comunidad de acuerdo con la consecución de objetivos globales de desarrollo sostenible y la planificación nacional del desarrollo*”. Este reglamento establece lo referente al

patrimonio y la identidad institucional en particular sobre la identidad corporativa institucional y su uso, la denominación y logotipo. Además, las disposiciones sobre la transformación digital y audiovisual en el ámbito institucional, su planificación e invariantes, los flujos de información y comunicación, el desarrollo de la plataforma de gestión académica y administrativa, el Sistema Estructurado de Gestión del Aprendizaje Virtual de la Universidad Metropolitana (*SEGAV/UMET*), la comunicación, presencia web, redes sociales, publicidad, mercadeo y admisiones, el soporte a proyectos innovadores y alianzas estratégicas; así como la planificación de las acciones de transformación, los soportes tecnológicos y los lineamientos de innovación.

Que, el antes mencionado Reglamento General, en su artículo 21 estableció entre los contenidos invariantes de la planificación estratégica para la transformación digital y audiovisual: los flujos de información y comunicación y sus mecanismos operacionales del SGDA y SIDE; la plataforma funcional de gestión académica y administrativa; el Sistema Estructurado de Gestión del Aprendizaje Virtual de la Universidad Metropolitana (*SEGAV/UMET*); la presencia en la web, redes sociales, publicidad, mercadeo y admisiones; el soporte a proyectos innovadores y alianzas estratégicas; el desarrollo de una plataforma multilateral de aprendizaje; y, el fomento de una cultura general e integral de la transformación digital. En sus artículos 95, 96 y 97, regula lo referente al Departamento de Comunicación, Promoción, Relaciones Públicas y Atención al Estudiante, su integración y funciones del jefe departamental.

Que, la UMET, aprobó el Plan Estratégico de la Transformación Digital y Audiovisual 2026 - 2030 mediante la Resolución No.25-UMET-CAS-SO-03-2026 de fecha 31 de marzo de 2026.

Que, mediante la Resolución N°. 81-UMET-CAS-SO-09-2025 de fecha 30 de octubre de 2025, se aprobó el documento de las Políticas de Protección de Datos Personales de la Universidad Metropolitana, que estableció las regulaciones para garantizar el ejercicio del derecho a la protección de datos personales de las personas naturales titulares de datos que se encuentran en posesión, custodia o tratamiento por la Universidad Metropolitana, sean miembros de la Comunidad Universitaria actual, exestudiantes, proveedores, contratistas, visitantes y terceros que mantengan relaciones jurídicas o contractuales con la Universidad; así como establecer los principios, las bases legales, las obligaciones, los procedimientos y las medidas técnicas y organizativas mínimas para el tratamiento lícito, leal y seguro de dichos datos. En su ANEXO 1. Registro de actividades de tratamiento señaló las medidas de seguridad técnica de datos.

Que, mediante **Resolución No. 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 de la Universidad Metropolitana, instrumento institucional de carácter general, transversal e integrador que crea el Sistema Institucional de Protección de la Privacidad, la Información y los Datos Personales de la Universidad Metropolitana (SIPPID) y establece principios, deberes, mecanismos de gobernanza, responsabilidades, controles y procedimientos aplicables a la protección de la privacidad,

la información institucional, la seguridad de la información, la ciberseguridad y los datos personales;

Que, mediante **Resolución No. 56-UMET-CAS-SO-07-2026**, el Consejo Académico Superior expidió el Reglamento para el Uso Ético, Responsable y Seguro de la Inteligencia Artificial en la Universidad Metropolitana, como norma institucional especial aplicable al desarrollo, adquisición, contratación, implementación, despliegue, uso, evaluación y retiro de sistemas de inteligencia artificial, articulada de manera complementaria con el Reglamento para la Protección de la Privacidad, de la Información y de los Datos Personales, el Código de Ética Institucional, de la Investigación y el Aprendizaje, las Políticas de Protección de Datos Personales y demás normativa interna aplicable;

Que, con las premisas anteriores y como continuidad de las regulaciones derivadas del Estatuto Institucional, del Reglamento General al Estatuto, del Reglamento para la Protección de la Privacidad, de la Información y de los Datos Personales, del Reglamento para el Uso Ético, Responsable y Seguro de la Inteligencia Artificial, de las Políticas de Protección de Datos Personales, del Plan Estratégico de Transformación Digital y Audiovisual 2026-2030 y de la normativa interna relacionada, resulta necesario regular los flujos de información y comunicación interna y externa de la Universidad, el uso de sus canales oficiales, soportes tecnológicos, identidad corporativa, contenidos institucionales, responsabilidades funcionales y mecanismos de autorización, supervisión y trazabilidad, con el objeto de garantizar seguridad jurídica, eficiencia operativa, transparencia, protección de la información institucional y debido proceso en el entorno físico y digital de la comunidad universitaria;

Que, mediante **Resolución No. CR-UMET-00141-07-2026, de 24 de julio de 2026**, el Consejo de Regentes emitió informe favorable respecto del proyecto de Reglamento del Flujo de Información y Comunicación de la Universidad Metropolitana y autorizó su remisión al Consejo Académico Superior para su conocimiento y resolución, conforme a las atribuciones previstas en el Estatuto Institucional y en el Reglamento General al Estatuto;

En ejercicio de las atribuciones conferidas por la Constitución, la Ley Orgánica de Educación Superior, el Estatuto Institucional y el Reglamento General al Estatuto, resuelve aprobar y expedir el siguiente:

REGLAMENTO DEL FLUJO DE INFORMACIÓN Y COMUNICACIÓN DE LA UNIVERSIDAD METROPOLITANA

TÍTULO I

DISPOSICIONES PRELIMINARES

CAPÍTULO I

OBJETO, ÁMBITO Y FINALIDADES

Artículo 1. Objeto. - El presente Reglamento tiene por objeto establecer los principios, reglas, procedimientos, deberes, responsabilidades y mecanismos de supervisión aplicables al flujo de información y comunicación interna y externa de la Universidad Metropolitana, al uso de sus canales oficiales, soportes tecnológicos, sitio web, redes sociales, comunicados institucionales, instrumentos de comunicación, identidad e imagen institucional.

Su aplicación se realizará de manera articulada 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, las Políticas de Privacidad y las Políticas de Protección de Datos Personales, el Código de Ética Institucional, de la Investigación y el Aprendizaje y demás normativa interna aplicable, sin sustituir las competencias, procedimientos y controles específicos previstos en dichos instrumentos.

Artículo 2. Ámbito material. - Las disposiciones del presente Reglamento regulan específicamente los flujos de información y comunicación institucional. Las materias relativas a privacidad, protección de datos personales, seguridad de la información, ciberseguridad, gestión documental, archivo e inteligencia artificial se regirán por sus instrumentos especiales, sin perjuicio de la aplicación complementaria del presente Reglamento cuando dichas materias se manifiesten en procesos de comunicación, publicación, circulación, carga, descarga, transferencia o difusión de información institucional.

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 UMET, conforme la definición prevista en el Estatuto Institucional, su Reglamento General, en el Código de Ética Institucional, de la Investigación y el Aprendizaje y la normativa conexas; 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 de la Universidad Metropolitana;
- b) El personal académico y de apoyo académico, en sus distintas categorías, dedicaciones, escalafones y modalidades;
- c) El personal de procesos habilitantes de asesoría y apoyo, en todas sus denominaciones, sin distinción del régimen jurídico de su vinculación;
- d) Los estudiantes regulares, no regulares, del tercer y cuarto nivel de estudios, de educación continua, en las modalidades presencial, semipresencial, a distancia, en línea, híbrida, dual y los estudiantes en movilidad académica;
- e) Los aspirantes, postulantes y participantes en procesos de admisión, selección, becas o convocatorias institucionales;
- f) Los pasantes, practicantes, becarios, profesores e investigadores invitados, ayudantes de cátedra e investigación y los colaboradores en proyectos institucionales;
- g) 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 proyectos de desarrollo institucional, de investigación, innovación y vinculación con la sociedad; y,

- h) Toda persona que, sin estar comprendida en los literales anteriores, de acuerdo con las regulaciones de este Reglamento utilice información y se comunique en representación de la Universidad Metropolitana o en el marco de actividades auspiciadas, financiadas, autorizadas o reconocidas por ella.

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) Garantizar que el flujo de información y comunicación institucional respete la dignidad humana, los derechos fundamentales, la ética, la integridad académica, la identidad institucional y los principios constitucionales aplicables;
- b) Asegurar la calidad, oportunidad, veracidad, actualización, pertinencia y coherencia institucional de la información difundida a través del sitio web oficial, páginas web, blogs institucionales, redes sociales, comunicados, oficios, notas ejecutivas, publicaciones y demás canales oficiales;
- c) Regular el uso adecuado, ético y responsable de los soportes de comunicación institucional, incluidos correos electrónicos, comunicados, chats institucionales, foros, canales audiovisuales, videoconferencias, plataformas digitales y demás medios físicos o electrónicos utilizados por la Universidad;
- d) Establecer estándares mínimos para la elaboración, circulación, aprobación, custodia y archivo de instrumentos de comunicación institucional, tales como oficios, memorandos, circulares, notas ejecutivas, comunicados oficiales, publicaciones y documentos de similar naturaleza;
- e) Regular los accesos, roles y responsabilidades vinculados con la carga, descarga, actualización, validación y comunicación de información en plataformas institucionales y en plataformas informáticas de organismos del Sistema de Educación Superior, del Estado y de terceros relacionados con la gestión universitaria;
- f) Articular los flujos de información y comunicación institucional con el Sistema Institucional de Protección de la Privacidad, la Información y los Datos Personales (SIPPID), el régimen interno de protección de datos personales, seguridad de la información, ciberseguridad y uso responsable de tecnologías;
- g) Prevenir, identificar, mitigar y remediar riesgos jurídicos, éticos, académicos, científicos, laborales, patrimoniales, reputacionales, comunicacionales, de seguridad de la información y de protección de datos personales derivados de la gestión de información y comunicación institucional;

- h) Salvaguardar la integridad institucional, académica, investigativa, administrativa y reputacional de la Universidad frente a usos indebidos de información, comunicación, imagen institucional, identidad corporativa, canales oficiales y soportes tecnológicos;
- i) Promover la transparencia, rendición de cuentas, trazabilidad documental, auditabilidad, eficiencia operativa y seguridad jurídica en los procesos de información y comunicación institucional; y,
- j) Garantizar que la comunicación institucional contribuya al cumplimiento de la misión, visión, fines, modelo educativo, planificación estratégica, transformación digital y posicionamiento institucional de la Universidad Metropolitana.

CAPÍTULO II

PRINCIPIOS RECTORES

Artículo 6. Principios rectores. – El flujo de información y comunicación institucional de la UMET se rige por los principios establecidos en el Estatuto institucional, su Reglamento General, de acuerdo al Modelo Educativo y Pedagógico, el Código de Ética de la Investigación y el Aprendizaje, la integridad académica, de la investigación y la democratización del conocimiento que se establecen en la normativa interna; 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: el flujo de información y comunicación y sus soportes tecnológicos serán concebidos, implementados y utilizados como procesos 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: el flujo de información y comunicación institucional 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) **Protección de datos personales:** todo tratamiento de datos personales realizado mediante los flujos de información y comunicación institucional deberá observar la Ley Orgánica de Protección de Datos Personales, su Reglamento General, la normativa secundaria de la Superintendencia de Protección de Datos Personales, el Reglamento para la Protección de la Privacidad, de la Información y de los Datos Personales y las Políticas de Protección de Datos Personales de la Universidad Metropolitana;
- d) Información veraz y oportuna: la Información que se gestiona, utiliza y comunica por los distintos actores universitarios en función de sus procesos se corresponderá con la realidad y veracidad de la información documental, variables, datos y estadísticas; sin sesgos, manipulaciones y distorsiones;

- e) **Transparencia y comprensión:** los sistemas de información y comunicación 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;
- f) **Comunicación efectiva:** la comunicación efectiva en el ámbito de transmitir ideas, información y emociones tanto de forma verbal como no verbal es fundamental para el perfeccionamiento de la función directiva, de la gestión académica y administrativa, del proceso enseñanza aprendizaje, la investigación y la vinculación con la sociedad.
- g) **No discriminación y equidad:** el desarrollo y uso de los sistemas de información y comunicación 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;
- h) **Integridad académica y honestidad intelectual:** la información y comunicación institucional, la difusión de resultados académicos e investigativos y el uso de tecnologías, incluida la inteligencia artificial cuando corresponda, deberán respetar los principios de autoría, originalidad, atribución de fuentes, rigor metodológico y honestidad intelectual, sin perjuicio de las disposiciones específicas previstas en el Reglamento para el Uso Ético, Responsable y Seguro de la Inteligencia Artificial;
- i) **Seguridad de la información y resiliencia:** el flujo de información y comunicación institucional y sus soportes tecnológicos estarán protegidos por medidas técnicas y organizativas adecuadas que garanticen su confidencialidad, integridad, disponibilidad, autenticidad, seguridad y resiliencia frente a errores, fallos, ataques o usos malintencionados, conforme a este Reglamento, las políticas de la UMET sobre la gestión de seguridad de la información y la normativa interna aplicable;
- j) **Trazabilidad y auditabilidad:** el ciclo de vida de los sistemas de información y comunicación 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;
- k) **Rendición de cuentas y responsabilidad proactiva:** las autoridades, directivos, y responsables de procesos y actividades que componen el flujo de información y comunicación institucional deberán demostrar, mediante evidencia verificable, el cumplimiento de las obligaciones derivadas de este Reglamento, las políticas de la UMET sobre la gestión de seguridad de la información, el uso ético de la IA y la normativa interna aplicable;
- l) **Sostenibilidad:** se considerará el impacto ambiental, social y económico del ciclo de vida de los sistemas de información y comunicación institucional, de las aplicaciones de IA, privilegiando soluciones coherentes con los compromisos institucionales en materia de sostenibilidad y responsabilidad ambiental;
- m) **Cooperación y diálogo de saberes:** la información y la comunicación en la Universidad Metropolitana respetarán 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;

- n) Proporcionalidad: Los flujos de información y comunicación y los soportes físicos y digitales serán adecuados y proporcionales para los fines institucionales perseguidos y los datos personales tratados se reducirán al mínimo indispensable para tales fines; e,
- o) Interpretación más favorable: en caso de duda razonable sobre la aplicación de este Reglamento, prevalecerá la interpretación que brinde mayor protección a los derechos fundamentales, a la dignidad de las personas, a la integridad académica, a la seguridad de la información y a los intereses institucionales legítimos frente al uso de los sistemas de información, comunicación y tecnologías institucionales, incluidos los sistemas de inteligencia artificial cuando corresponda.

Artículo 7. Jerarquía normativa e interpretación. - Las disposiciones del presente Reglamento se interpretarán y aplicarán en consonancia con la Constitución, los instrumentos internacionales de derechos humanos ratificados por el Ecuador, 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, la Ley Orgánica para el Fortalecimiento de la Ciberseguridad, la Ley Orgánica de Educación Superior, el Estatuto Institucional, el Reglamento General al Estatuto y los demás reglamentos internos. En caso de duda interpretativa, prevalecerá 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.

TÍTULO II

GOBERNANZA DEL FLUJO DE INFORMACIÓN Y COMUNICACIÓN INSTITUCIONAL

CAPÍTULO I

COMPONENTES Y ARTICULACIÓN DEL FLUJO DE INFORMACIÓN Y COMUNICACIÓN INSTITUCIONAL

Artículo 8. Flujos de información y comunicación institucional. – En la Universidad Metropolitana, los flujos de información y comunicación institucional constituyen procesos integrados mediante los cuales las autoridades, órganos colegiados, unidades académicas, unidades administrativas, procesos gobernantes, procesos agregadores de valor y procesos habilitantes de asesoría y apoyo generan, reciben, validan, transmiten, comunican, publican, custodian, actualizan, archivan o eliminan información necesaria para el cumplimiento de sus funciones.

Estos flujos comprenden la comunicación interna y externa, física y digital, descendente, ascendente, horizontal, diagonal e interinstitucional, así como la gestión de información

académica, administrativa, investigativa, financiera, contractual, tecnológica, documental, estadística, comunicacional y de cualquier otra naturaleza vinculada con la actividad universitaria.

La gestión de los flujos de información y comunicación institucional deberá asegurar oportunidad, veracidad, trazabilidad, responsabilidad funcional, seguridad, pertinencia, calidad y coherencia con la misión, visión, planificación estratégica, identidad institucional y normativa interna de la Universidad.

Artículo 9. Componentes del flujo de información y comunicación institucional. - Los componentes del flujo de información y comunicación institucional serán objeto, partes invariantes y objetivos del Plan Estratégico de Desarrollo para la Transformación Digital y Audiovisual. Entre ellos:

- a) Gestión de comunicación, promoción, relaciones públicas y servicios al estudiante. Provee el soporte para el posicionamiento de la imagen institucional, la comunicación interna y externa, de relaciones públicas y promoción con un enfoque reputacional y estratégico a través de los canales de comunicación interna, la presencia en la web y las redes sociales;
- b) Gestión de los canales tecnológicos de difusión de información y comunicación según sus flujos interactivos descendente, ascendente, horizontal, diagonal y externo.
- c) Gestión de información para la mejora continua y progresiva de los procesos de gestión académica y administrativa a través de la elaboración, aplicación, procesamiento y comunicación de los resultados mediante instrumentos digitales de foros de discusión y encuestas;
- d) Gestión de información académica y administrativa a través de la Plataforma Sistema Nacional Académico y Administrativo (SNAA) que articula el Sistema de Gestión Documental y de Archivos (SGDA), el Sistema Institucional de Datos y Estadísticas (SIDE), el Cuadro de Mando Integral (CMI) y un conjunto de plataformas y aplicaciones informáticas para la gestión académica y de los procesos de apoyo;
- e) Flujos de información y comunicación del Sistema Estructurado de Gestión del Aprendizaje Virtual de la Universidad Metropolitana, por su denominación interna *SEGAV/UMET*, proveerá el soporte tecnológico por la Dirección de Tecnologías Informáticas, la orientación pedagógica y de recursos en entornos virtuales de aprendizaje por el Centro de Educación Semipresencial, a Distancia y en Línea (CESDEL) y los recursos bibliográficos físicos y digitales del Centro de Recursos para el Aprendizaje y la Investigación (CRAI);
- f) Socialización del conocimiento y la comunicación científica en los soportes editoriales y revistas científicas de la Universidad Metropolitana;
- g) Gestión de información de las plataformas informáticas vigentes de los organismos del Sistema de Educación Superior o de sus reformas, entre ellos: el Sistema Integral de Información de la Educación Superior (SIIES); Sistema Nacional de Información de

Educación Superior del Ecuador (SNIESE); plataformas y aplicaciones del Consejo de Aseguramiento de la Calidad del Sistema de Educación Superior (CACES); Sistema de Acompañamiento Previo para Recolección de Información (SAPPRI) del Consejo de Educación Superior (CES); Plataforma de Presentación de Carreras y Programas (PPCP) del CES;

- h) Gestión de información en las plataformas de los organismos de trabajo, seguridad social y rentas internas (MdT, IESS, SRI);
- i) Gestión documental y comunicación a través de plataformas digitales del sector público. Su principal objetivo es facilitar la creación, envío, recepción, archivo y seguimiento de documentos oficiales entre instituciones de manera completamente electrónica;

CAPÍTULO II

GOBERNANZA Y ROLES INSTITUCIONALES

Artículo 10. Gobernanza institucional. - La gobernanza del flujo de información y comunicación institucional, en soportes físicos y digitales, corresponde a las autoridades, órganos colegiados, direcciones, unidades y responsables funcionales de la Universidad Metropolitana, dentro del ámbito de sus respectivas competencias y conforme al Estatuto Institucional, al Reglamento General al Estatuto, al Manual Orgánico Funcional y a la normativa interna aplicable.

Participan en dicha gobernanza, según corresponda, el Rectorado, los Vicerrectorados, la Secretaría General Técnica, la Procuraduría Nacional, la Dirección de Tecnologías Informáticas, la Dirección General, la Dirección de Contabilidad y Finanzas, la Dirección de Bienestar Universitario, el Departamento de Comunicación, Promoción, Relaciones Públicas y Atención al Estudiante, la Unidad de Talento Humano, las unidades académicas, los centros de apoyo, las sedes, las comisiones institucionales, los responsables de plataformas, los custodios funcionales de información y los demás responsables previstos en la estructura orgánico-funcional vigente.

Cuando por reforma estatutaria, reglamentaria, orgánica o funcional se modifique la denominación, integración o dependencia de alguna unidad o cargo señalado en este Reglamento, las referencias se entenderán realizadas a la instancia que haga sus veces, siempre que no se altere el contenido sustantivo de la competencia atribuida.

La gobernanza prevista en este artículo se ejercerá de manera articulada con el Sistema Institucional de Protección de la Privacidad, la Información y los Datos Personales, con el régimen institucional de inteligencia artificial y con las políticas internas de comunicación, transformación digital, protección de datos personales, seguridad de la información e identidad institucional.

Artículo 11. Articulación funcional. – Los componentes del flujo de información y comunicación institucional y sus soportes se gestionarán como un proceso integrador, bajo los principios rectores, jerarquía normativa, jerarquía orgánica funcional, roles, atribuciones y

responsabilidades que establece este Reglamento, de manera articulada y bajo el principio de unidad e integralidad institucional del Estatuto y su Reglamento General.

Artículo 12. Roles y responsabilidades institucionales. – Las responsabilidades sobre el flujo de información y comunicación institucional se ejercerán de conformidad con las atribuciones de las primeras autoridades, autoridades académicas y administrativas, directivos de las funciones sustantivas, responsables de procesos gobernantes, agregadores de valor y habilitantes de asesoría y apoyo, previstas en el Estatuto Institucional, el Reglamento General al Estatuto, el Manual Orgánico Funcional y la normativa interna aplicable.

Cada autoridad, dirección, unidad, centro, sede, responsable funcional o usuario institucional responderá por la veracidad, oportunidad, pertinencia, actualización, legalidad, trazabilidad, confidencialidad, seguridad y uso adecuado de la información que genere, reciba, custodie, publique, comunique, cargue, descargue o transmita en el ámbito de sus funciones.

La responsabilidad sobre la información institucional comprenderá, según corresponda, la provisión de contenidos, validación técnica, aprobación jerárquica, publicación, custodia, archivo, actualización, rectificación, eliminación, protección de datos personales, preservación de evidencias y reporte de incidentes.

Las responsabilidades específicas previstas en este Reglamento se ejercerán sin perjuicio de las atribuciones establecidas en 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, las Políticas de Protección de Datos Personales, el Código de Ética Institucional, de la Investigación y el Aprendizaje y demás normativa interna aplicable.

TÍTULO III

SOPORTES DE LA INFORMACIÓN Y COMUNICACIÓN INSTITUCIONAL

CAPÍTULO I

CANALES OFICIALES DE COMUNICACIÓN INSTITUCIONAL

Sección 1

Sitio, páginas web y redes sociales institucionales

Artículo 13. Sitio web institucional. - El sitio o portal *web* institucional de la Universidad Metropolitana es el conjunto de páginas de contenidos e interacciones bajo un mismo dominio específico y accesibles en internet que conecta la comunidad universitaria y el público para brindar información relevante sobre la institución, las facilidades y servicios universitarios, la promoción de su oferta académica, de productos y servicios a la comunidad; orientados a la democratización del conocimiento y la universalización de la educación superior.

Artículo 14. Calidad de la web institucional. – El sitio *web* institucional de la Universidad Metropolitana deberá observar criterios de calidad, seguridad, accesibilidad, funcionalidad,

actualización, pertinencia, coherencia institucional, rendimiento, experiencia de usuario y protección de la información.

El sitio web institucional deberá cumplir, al menos, con los siguientes atributos:

- a) Diseño gráfico coherente con la identidad corporativa institucional establecida en su normativa interna, con respeto a la integridad de la Universidad Metropolitana, la inclusión, la no discriminación, la diversidad y la interculturalidad.
- b) Diseño WEB que garantiza una “navegación intuitiva” a través de sus menús y páginas;
- c) Diseño “responsive” adaptable a diferentes dispositivos y tamaños de pantalla;
- d) Alta calidad de la información atendiendo a su relevancia, presentación, objetividad y correspondencia con los elementos constitutivos de la misión y visión institucional;
- e) Se integra a redes sociales institucionales y presenta vínculos a la información, los soportes automatizados, páginas y aplicaciones de procesos de gestión académica y administrativa;
- f) Garantiza un proceso continuo de mantenimiento y optimización para garantizar el rendimiento, la funcionalidad y la seguridad;
- g) Utiliza un Sistema de Gestión de Contenidos (CMS) que garantiza actualización, rendimiento, funcionalidad, seguridad, visibilidad, métrica, experiencia y satisfacción de usuarios. Como línea base de desarrollo se utilizará el CMS WordPress y sus actualizaciones;
- h) Utiliza una estrategia de contenido inteligente que se planifica y enfoca en la creación, publicación y gestión de contenido a lo largo del tiempo, que garantice su actualización, relevancia;
- i) Está optimizado para motores de búsqueda (SEO). Esto incluye la integración del SEO a la estrategia de contenido para mejorar la posición en los resultados de los motores de búsqueda y la visibilidad;
- j) Garantiza el monitoreo del rendimiento para la mejora continua en términos de velocidad, capacidad de respuesta y confiabilidad durante las interacciones del usuario a través del uso de una métrica confiable y efectiva; y,
- k) Utiliza métricas de analítica como volumen de tráfico: cantidad de visitantes, popularidad y alcance; fuente de tráfico: procedencia de visitantes, motores de búsqueda, visitas directas, referencias de otros sitios y plataformas de redes sociales; tasa de rebote, que indica el porcentaje de visitantes que abandonan el sitio después de ver solo una página; tiempo en la página para evaluar la efectividad del contenido; y la tasa de conversión, como la medida en que los visitantes se integran;

Artículo 15. Redes sociales institucionales. – Las redes sociales institucionales de la Universidad Metropolitana son canales digitales oficiales destinados a la difusión de información, noticias, avisos, campañas, actividades, contenidos académicos, investigativos, de

vinculación, institucionales y de interés público relacionados con el quehacer universitario.

Las redes sociales institucionales serán administradas por el Departamento de Comunicación, Promoción, Relaciones Públicas y Atención al Estudiante, o la instancia que haga sus veces, conforme a los lineamientos aprobados por las autoridades competentes, la normativa de identidad institucional, las políticas de comunicación y las reglas de seguridad de la información y protección de datos personales.

La Universidad utilizará redes sociales y plataformas digitales confiables, de alcance institucional, nacional o internacional y compatibles con sus fines. La apertura, cierre, sustitución o incorporación de nuevas redes sociales o plataformas oficiales será autorizada por el Rectorado o por el Vicerrectorado Administrativo, según corresponda, previo criterio del Departamento de Comunicación, Promoción, Relaciones Públicas y Atención al Estudiante y de la Dirección de Tecnologías Informáticas. Cuando la decisión tenga impacto institucional relevante, será puesta en conocimiento del Consejo Académico Superior.

El jefe del Departamento de Comunicación, Promoción, Relaciones Públicas y Atención al Estudiante será responsable de la gestión comunicacional de las redes sociales institucionales, sin perjuicio de la responsabilidad técnica de la Dirección de Tecnologías Informáticas sobre los aspectos que correspondan a seguridad, accesos, recuperación de cuentas, soporte e integración tecnológica.

Toda publicación en redes sociales institucionales deberá observar criterios de veracidad, oportunidad, pertinencia, respeto, no discriminación, identidad institucional, protección de datos personales, propiedad intelectual, confidencialidad, integridad académica y reputación institucional.

Artículo 16. Gestión de los contenidos del sitio *web* y redes sociales institucionales. – La gestión de los contenidos del sitio web y redes sociales institucionales estará a cargo de la Unidad de Comunicación del Departamento de Comunicación, Promoción, Relaciones Públicas y Atención al Estudiante (CPRPAE). La Unidad contará con un *web master* y equipo proveedor del diseño gráfico.

La gestión de contenidos será distribuida contando como fuentes de información aquellas que se soliciten por las autoridades y los directivos de áreas funcionales académicas y de procesos de apoyo, quienes serán los responsables de la actualización, veracidad y relevancia de estos.

Sin perjuicio de lo dispuesto en el artículo 18 de este Reglamento, cuando la publicación o difusión de información institucional pueda involucrar datos personales, información sensible, confidencial, reservada, estratégica, jurídica, financiera, disciplinaria, contractual, investigativa no publicada o susceptible de afectar derechos de terceros, la unidad requirente deberá obtener la validación previa de la autoridad competente y, cuando corresponda, el criterio del Delegado de Protección de Datos Personales, de la Procuraduría Nacional, de la Dirección de Tecnologías Informáticas o de la instancia técnica competente.

La publicación de esta información deberá observar los principios de finalidad, necesidad, proporcionalidad, minimización, seguridad, confidencialidad, trazabilidad y responsabilidad

funcional. En ningún caso podrá difundirse información cuya publicación se encuentre prohibida por la Constitución, la ley, la normativa de protección de datos personales, la normativa interna o una disposición de autoridad competente.

Artículo 17. Cobertura de actividades. – La cobertura de actividades por la unidad de comunicación para difusión en la *web* y las redes sociales será planificada mensualmente y en el caso necesario operativamente para cuando ellas sean actividades de eventos por invitación o involucramiento de organismos y organizaciones externas. Se solicitará por las primeras autoridades, directivos de funciones sustantivas, centros y de procesos de apoyo, decanos y directores de sedes al Departamento de Comunicación, Promoción, Relaciones Públicas y Atención al Estudiante (CPRPAE), con el plazo de antelación que se disponga por las primeras autoridades ejecutivas.

Artículo 18. Publicación de contenidos del sitio *web* y redes sociales institucionales. – La publicación de la información en el sitio *web* y de él, la que corresponda a las redes sociales institucionales por la Unidad de Comunicación tendrá el siguiente nivel de provisión de información actualizada, supervisión y/o aprobación por las distintas instancias universitarias responsables:

a) Del ámbito del Rectorado

1. El SGT brindará la información actualizada de las páginas del Consejo de Regentes, el Consejo Académico Superior, las definiciones estratégicas, misión y visión institucional y dispondrá la publicación y/o sustitución de los reglamentos, manuales, instructivos, protocolos y guías metodológicas una vez autorizado por el Rector y Presidente del Consejo Académico Superior.
2. La Comisión Institucional de Planificación Estratégica (CIPE) brindará la información actualizada de las páginas de la CIPE, PEDI, Informes de cumplimiento de Objetivos Estratégicos, POA, Plan Estratégico de la Transformación Digital y Calendario Académico.
3. La Comisión Institucional de Aseguramiento de la Calidad (CIAC) brindará la información actualizada de las páginas de la CIAC, Informes de Autoevaluación y Planes de Mejora Institucional.
4. El Rector, su asesor o delegado brindará la información actualizada las páginas y blog del rectorado y las acciones de rectoría, noticias, avisos y artículos.
5. El Rector supervisará la información proporcionada y alojada en el ámbito del rectorado y la función de rectoría.

b) Del ámbito del Vicerrectorado Académico

1. El Director de Formación del Profesional brindará la información actualizada sobre el Modelo Educativo y Pedagógico, el sistema de evaluación del desempeño, los instructivos para los Programas de Estudios de las Asignaturas, Cursos y Equivalentes y las políticas y estrategias didácticas institucionales.

2. Los directores de los centros de apoyo de las funciones sustantivas brindarán la información actualizada de sus respectivos centros: Centro de Educación Semipresencial, a Distancia y en Línea (CESDEL); Centro de Recursos para el Aprendizaje y la Investigación (CRAI); y, Centro de Formación en Docencia Universitaria (CEFDU).
3. La directora de Investigación e Innovación brindará y actualizará sistemáticamente la información *web*, convocatorias, avisos y noticias sobre la Política Científica institucional, los centros de I+D+i, las publicaciones institucionales, revistas científicas, artículos, libros y capítulos de libros, Comité Científico, los manuales de procedimientos y buenas prácticas de IDi y sobre eventos científicos.
4. El director de Vinculación con la Sociedad brindará y actualizará sistemáticamente la información *web*, convocatorias, avisos y noticias sobre la estructura de programas y proyectos, resultados e impactos, seguimiento a graduados desde acciones de vinculación, los manuales de procedimientos y buenas prácticas de vinculación y las alianzas estratégicas con organismos, organizaciones, centros educativos, empresas, GAP, GADs y comunidades.
5. Los decanos y la dirección de la Unidad de Formación Técnica y Tecnológica (UAFTT) brindarán y actualizarán sistemáticamente la información *web*, convocatorias, avisos y noticias del ámbito de sus facultades y unidades académicas en la matriz y las sedes.
6. Los decanos y la dirección de la UAFTT supervisarán que toda la información que se publique en la *web* sobre la oferta académica de sus facultades y unidades académicas se correspondan con los Planes de Estudio de carreras y programas de posgrados según las resoluciones aprobatorias del CES.
7. El Vicerrector Académico supervisará la información proporcionada y alojada en el ámbito del Vicerrectorado.

c) Del ámbito del Vicerrectorado Administrativo

1. El Departamento de Comunicación, Promoción, Relaciones Públicas y Atención al Estudiante (CPRPAE) garantizará la actualización y funcionalidad del sitio *web* en todos sus criterios y atributos de calidad, la actualización y publicación oportuna de la información de su competencia y aquellas proporcionada por los ámbitos de gestión del rectorado y los vicerrectorados.
2. El Departamento de CPRPAE actualizará sistemáticamente la información de la página de inicio, páginas de menú de cabecera sobre servicios al estudiantado, profesorado y personal administrativo, de la oferta académica, admisiones y noticias y eventos.
3. La Unidad de Relaciones Interinstitucionales e Internacionales actualizará sistemáticamente la información en la *web*, convocatorias, avisos y noticias, sobre las páginas de internacionalización, convenios, auspicios, colaboración y redes.
4. La Dirección General brindará información actualizada y supervisará lo referente a las páginas de transparencia institucional, información sobre la gestión del TTHH y de las

infraestructuras físicas y digitales.

5. La Dirección de Bienestar Universitario brindará y actualizará sistemáticamente la información *web*, convocatorias, avisos y noticias sobre actividades de sus programas, proyectos y eventos extensionistas. La información *web* sobre becas y ayudas económicas, testimonios, servicios de salud y bienestar; así como supervisará en toda la información del sitio *web* el cumplimiento de los principios de la igualdad de todos los actores.
6. El Vicerrector Administrativo supervisará la información proporcionada y alojada en el ámbito del Vicerrectorado y sus dependencias.
7. El Vicerrector Administrativo garantizará que toda la información del sitio *web* cumpla con la Política Institucional de Protección de Datos Personales.

El plazo de publicación, sustitución o actualización de contenidos en el sitio *web* una vez proporcionada la información e insumos por las áreas funcionales no excederá el plazo mayor a un día hábil para las disposiciones del SGT correspondientes a información resultante de resoluciones del CAS, no mayor al plazo que soliciten las primeras autoridades, autoridades y directivos académicos y administrativos.

Las noticias cubiertas por la Unidad de Comunicación tendrán la inmediatez suficiente de publicación en el sitio *web* para garantizar su impacto no debiendo exceder el plazo que se solicite.

El resto de las solicitudes o el cumplimiento de requerimientos del Departamento de CPRPAE se realizará en un plazo que dependerá de la complejidad y tratamiento de la información.

Artículo 19. Publicación de contenido en redes sociales institucionales. – La publicación de contenidos en redes sociales que se genera por la Unidad de Comunicación tendrá la inmediatez necesaria previa revisión y autorización del Jefe del Departamento de CPRPAE.

El Jefe del Departamento de CPRPAE gestionará y garantizará el ambiente de la transmisión en vivo de actividades de actos y eventos, previa autorización del Vicerrector Administrativo.

Sección 2

Plataformas de comunicación audiovisual

Artículo 20. Plataformas de comunicación audiovisual. – La institución para los fines de gestión académica y administrativa, del proceso enseñanza – aprendizaje y otros procesos, utilizará las aplicaciones de base de *Microsoft Office Teams*, *Zoom*, sus sustitutivas homólogas o actualizaciones, entre otras nativas de las plataformas LMS o las que ocasionalmente puedan emplearse para el soporte a clases, reuniones, eventos y otras actividades que requieran realizar teleconferencias y sus grabaciones.

Artículo 21. Buenas prácticas de la participación en teleconferencias. – Para la participación de la comunidad universitaria en teleconferencias, ya sean clases sincrónicas, talleres, seminarios, reuniones, eventos u otras actividades, se deberán seguir las siguientes buenas prácticas:

- a) Puntualidad de los participantes, quienes deberán conectarse con al menos 10 minutos de antelación para solucionar imprevistos y garantizar el inicio oportuno de la sesión virtual sincrónica.
- b) Uso de vestimenta formal, acorde con el carácter institucional de la sesión.
- c) Activación de la cámara durante la sesión según las regulaciones específicas de este Reglamento.
- d) Uso del micrófono exclusivamente cuando el participante tenga la palabra o al momento de emitir un voto o intervención solicitada.
- e) Proyección de una imagen adecuada en el auditorio virtual, asegurando un correcto encuadre del rostro y un fondo apropiado en pantalla con atención a las regulaciones específicas de este Reglamento.
- f) Minimización del uso de accesorios innecesarios, como audífonos, salvo en entornos con ruido externo.
- g) Respeto absoluto a la organización de la actividad, concesión de la palabra, disciplina, lenguaje apropiado y consideraciones éticas.
- h) Participación desde un espacio con la privacidad necesaria, asegurando que la sesión transcurra sin interrupciones y acceso exclusivo.
- i) Las buenas prácticas de teleconferencia en sesiones del Consejo Académico Superior (CAS) se establecen en el Reglamento de Funcionamiento de este órgano colegiado superior.

Artículo 22. Sobre la activación de la cámara durante la sesión de teleconferencias. – La activación de la cámara será requerida cuando sea indispensable para verificar identidad, participación efectiva, solemnidad del acto, control académico, registro de asistencia o desarrollo adecuado de la sesión. Para mitigar riesgos de privacidad, será obligatorio que los participantes utilicen, cuando sea posible, fondos virtuales, filtros de desenfoque o encuadres que impidan visualizar información, personas, bienes, documentos o espacios privados ubicados detrás del usuario.

Cada participante procurará conectarse desde un ambiente adecuado, silencioso y reservado, que reduzca interrupciones de terceras personas durante los enlaces, preserve la confidencialidad de la sesión y evite la exposición incidental de datos personales de familiares, compañeros de vivienda, usuarios, pacientes, estudiantes u otras personas ajenas a la reunión o actividad.

Los responsables de la sesión, moderadores o conductores preverán las excepciones justificadas por conectividad, discapacidad, condiciones técnicas, seguridad personal, fuerza mayor o razones de privacidad debidamente informadas.

Las teleconferencias en el marco de las sesiones del CAS cumplirán las buenas prácticas que establece el Reglamento de ese órgano; las teleconferencias del Comité Científico y las actividades de dirección del Ápice Estratégico de dirección institucional seguirán las buenas prácticas que determinen las primeras autoridades para sus sesiones.

Artículo 23. Imagen e identidad corporativa en teleconferencias. – La imagen y el uso de la identidad corporativa en fondos de pantalla en las teleconferencias será obligatoria para los

responsables de las sesiones, los participantes en sesiones del rectorado y los vicerrectorados, de la función directiva, así como la participación en teleconferencias en calidad de representación institucional, entornos de aprendizaje colaborativo internacional e interinstitucional. Los responsables y participantes en estas actividades deberán garantizar con la debida antelación estos requerimientos y en el caso de ser necesario solicitar el espacio y el soporte técnico a los asistentes de la Dirección de Tecnologías en las instalaciones y los campus. Las excepciones circunstanciales para el cumplimiento deberán ser motivadas e informadas.

Sección 3

Otros soportes de información y comunicación institucional

Artículo 24. Comunicaciones auxiliares o contingentes. – Las comunicaciones auxiliares o contingentes entre miembros de la comunidad universitaria mediante el uso de plataformas de chats utilizando canales no institucionales serán responsabilidad de los interlocutores debiendo priorizarse los canales institucionales que garanticen la seguridad, trazabilidad, confidencialidad y responsabilidad demostrada.

Artículo 25. Plataformas de comunicación y chats externos de los organismos rectores de Educación Superior. – El Rector en representación de la institución podrá integrar grupos en plataformas administradas por autoridades de organismos externos cuando sea convocado a participar en ellas o lo solicite en interés de la institución, lo cual será de conocimiento del SGT.

Artículo 26. Páginas web y blogs personales de autoridades. – Las autoridades de la institución que cuenten con páginas web y blog personales a título institucional autorizados por el CAS.

Artículo 27. Páginas web y blogs institucionales del ápice estratégico de dirección. – Las páginas web y blog institucional para la gestión de información de las autoridades ejecutivas serán una atribución exclusiva del rectorado y los vicerrectorados. Los blogs de esas instancias ejecutivas serán alojados con el soporte de la Dirección de Tecnologías Informáticas. Los administradores serán el Rector, los Vicerrectores o en quienes deleguen y compartirán la cuenta de administración con el Director de Tecnologías Informáticas. La publicación de noticias, avisos, artículos y comentarios serán autorizados y moderados por las primeras autoridades según su ámbito de dirección.

Artículo 28. – Plataformas, páginas web y aplicaciones específicas de procesos académicos y administrativos. - La institución contará con plataformas, páginas web y aplicaciones específicas de procesos de gestión académica y administrativa, entre ellas:

- a) Plataforma para el seguimiento a graduados. – La plataforma, según las disposiciones de los instructivos del seguimiento a graduados, denominada *Alumni/UMET*, promoverá la comunicación con los graduados y será el soporte de los Comités Consultivos de Graduados.
- b) Aplicación *Administrativo/UMET*, que proveerá la calendarización de actividades académicas y de bienestar universitario, tanto institucional como por facultades y la UAFTT; el servicio de actualización de datos de hoja de vida del personal; la descarga de roles de pagos; formularios de solicitudes, entre otras facilidades que deberán ser

desarrollados progresivamente hasta automatizar todos los procesos.

Sección 4

Soportes de comunicación académica y científica institucional

Artículo 29. Editorial Universitaria como soporte de comunicación. – La Editorial UMET estará orientada a contribuir al acceso a información, la difusión y la democratización del conocimiento como parte de la misión y la visión estratégica del Centro de Recursos para el Aprendizaje y la Investigación (CRAI). La editorial tendrá presencia en la web institucional y conformará alianzas estratégicas y colaboración con otras editoriales nacionales e internacionales.

La dirección del CRAI, a través del director ejecutivo editorial fomentarán el fortalecimiento de sus productos impresos y en formato digital cumpliendo los requisitos de rigor y calidad por los cuales le fue otorgado el sello editorial el 1 de agosto de 2023, reconocido por la Cámara Ecuatoriana del Libro. Los servicios editoriales tendrán un componente de gestión interna y de colaboración externa.

La Editorial UMET, de la Universidad Metropolitana del Ecuador, publicará y difundirá los resultados de la producción científica en acceso abierto bajo una licencia de *Creative Commons Attribution 4.0 International*, que permite el uso, intercambio, adaptación, distribución y transmisión en cualquier medio o formato, siempre que dé el crédito apropiado al autor, origen y fuente del material gráfico. Si el uso del material gráfico excede el uso permitido por la normativa legal deberá tener permiso directamente del titular de los derechos de autor.

Artículo 30. Calidad de la imagen y la información editorial. – La calidad de la imagen y la información editorial se regirá por el Reglamento del CRAI, el Manual de Estilos, el Manual de Identidad Corporativa y la normativa interna relacionada con las funciones sustantivas. La dirección editorial, la dirección del CRAI y la dirección de Investigación e Innovación velarán por la calidad de la imagen y de los productos editoriales.

Artículo 31. Mecanismos de comunicación científica. – Los mecanismos de comunicación científica serán aquellos inherentes a la comunicación de los autores con la comunidad y el intercambio académico en redes, colectivos y el entorno. Entre ellos se incluirá la presentación de obras relevantes, libros, artículos científicos, ponencias y otros a la comunidad. La dirección de IDi planificará actividades de presentación de las obras relevantes producidas por la comunidad universitaria en actos públicos presenciales y en entornos virtuales de lanzamiento y difusión con la más amplia participación, así como procederá a su publicación en la web institucional como parte del acervo bibliográfico de la UMET. Para ello la Dirección General brindará las facilidades logísticas y financieras como parte del presupuesto operativo anual.

Artículo 32. Revistas científicas como fuentes de información y comunicación. – Las revistas científicas que aloja la UMET tendrán un soporte tecnológico permanente e ininterrumpido en el dominio umet.edu.ec.

Cada revista cumplirá con requisitos de calidad de la información y la comunicación contando con un equipo editorial conformado por un director, un director ejecutivo y un editor; un consejo

científico y un consejo internacional de revisores; tendrá un soporte de software de gestión de revistas de código abierto *Open Journal Systems* (OJS) desarrollado, impulsado y distribuido de forma gratuita por el *Public Knowledge Project* (PKP) bajo una licencia pública general (GNU). La dirección del CRAI, la dirección editorial y la dirección de IDi son corresponsables del cumplimiento de los estándares de calidad nacional, regional e internacional y del cumplimiento de los requisitos de las bases de datos en que se registran.

La indexación de las revistas buscará el registro creciente en bases de datos nacionales, regionales y globales, el incremento de su visibilidad y calidad de acuerdo con los más altos estándares mundiales de integridad de la investigación y la publicación. Las revistas proveerán información sobre: indexaciones, métricas, periodicidad, enfoque y alcance; normas; proceso editorial; proceso de revisión por pares; política antiplagio, buenas prácticas y responsabilidades; política sobre el uso de la IA; política de acceso abierto y cargos por procesamiento de artículos; autoarchivo; declaración de privacidad y contactos.

Sección 5

Plataformas y redes sociales del conocimiento

Artículo 33. Plataformas y redes sociales del conocimiento y la investigación. - Las plataformas y redes sociales especializadas en conocimiento e investigación resultarán fundamentales para facilitar la colaboración y la divulgación en el ámbito académico de la Universidad Metropolitana. Gracias a ellas, los investigadores pueden difundir sus trabajos, conectar con colegas y acceder fácilmente a recursos relevantes. La UMET reconocerá la participación del personal académico en plataformas nacionales e internacionales. Entre ellas de alcance internacional, como línea base, *Research Gate*, *Academia.edu*, *Google Scholar*, entre otras que en el tiempo se actualicen o puedan surgir para el fortalecimiento de la comunicación académica y científica.

Artículo 34. Filiación e identidad en la información y la comunicación científica. - De acuerdo con el RGE / UMET, para los efectos de la internacionalización, la visibilidad internacional, el registro en bases de datos de rankings internacionales, los identificadores de los docentes y los estudiantes en su filiación con la UMET en bases de datos y registros, redes sociales del conocimiento, entre otros, se utilizará la denominación “Universidad Metropolitana del Ecuador”.

Para la preservación de la filiación institucional y la identidad de los autores, para las publicaciones en las revistas que aloja y patrocina la UMET y aquellas que lo exijan, será obligatorio el uso de identificadores digitales según lo establece el Reglamento General al Estatuto.

Sección 6

Correo electrónico institucional y aplicaciones de Office 365

Artículo 35. Cuenta institucional de Microsoft Office 365. - Cada miembro del personal de dirección, personal académico, de apoyo académico, de los procesos habilitantes de asesoría y apoyo y los estudiantes tendrán acceso a una cuenta de Microsoft Office 365 provista por la

UMET cuyas prestaciones estarán determinadas por el Director de Tecnologías Informáticas, que podrán ser ampliadas a solicitud de las primeras autoridades ejecutivas.

La cuenta incluirá invariablemente el correo electrónico institucional; el almacenamiento de información en la nube, el cual puede ser compartido entre usuarios; la aplicación Microsoft Teams, como espacio de trabajo pensado para la colaboración en tiempo real y la comunicación, clases sincrónicas, reuniones, uso compartido de archivos, visualización de videos, videoconferencias y chats. Estas cuentas deberán tener el uso para el cual son habilitadas respetando las disposiciones del Código de Ética Institucional, de la Investigación y el Aprendizaje.

Artículo 36. Correo electrónico institucional. – Las cuentas de correo electrónico institucional serán el medio oficial de comunicación para la gestión académica y administrativa. Así mismo para la comunicación de los estudiantes. Son para el uso del titular y no transferibles, serán de su responsabilidad y podrán ser suspendidas por causa de su mal uso sin perjuicio de las demás regulaciones que establecen el Código de Ética Institucional, de la Investigación y la Investigación, así como las otras normativas conexas y la Ley.

El Director de Tecnologías Informáticas podrá crear cuentas para las unidades funcionales de los procesos habilitantes de asesoría y apoyo adicionales a la cuenta personal del directivo, cuya denominación corresponda a sus áreas, con el fin de garantizar la identidad de dichas áreas y la continuidad de la gestión de sus procesos. La creación de estas cuentas será autorizada a la dirección de tecnologías por el Rector o los Vicerrectores y asignadas a un responsable, quien tomará las medidas de seguridad informática.

Artículo 37. Activación y desactivación de las cuentas. - Las cuentas de MS Office 365 asignadas a los miembros de la comunidad universitaria deberán ser activadas a sus usuarios una vez que se incorporan a la institución en el ámbito laboral o de estudios y desactivadas previo aviso con al menos 5 días hábiles de antelación. Con excepción de aquellas que por disposición motivada sean indicadas con inmediatez por el Rector, el Consejo Académico Superior o los Vicerrectores.

Las cuentas de correo de las unidades funcionales, una vez que el directivo o funcionario a cargo cese en sus funciones deberán ser recibidas por el Director de Tecnologías Informáticas y una vez cambiadas sus claves, entregadas a los directivos o funcionarios entrantes.

En el caso extraordinario de la extinción de una cuenta, cuya referencia exista registrada en entidades externas para el flujo de información, de manera temporal, se podrá configurar por el Director de Tecnologías la transferencia de la información que se reciba a otra cuenta debidamente autorizada por el Rector.

El cumplimiento de estas regulaciones será de carácter obligatorio y la responsabilidad del director de Tecnologías Informáticas.

Artículo 38. Comunicados oficiales vía el correo electrónico institucional. - La circulación de comunicados en los correos electrónicos institucionales que sean de alcance institucional para la comunidad universitaria, para una o todas las facultades o sedes, para objetivos específicos de

difusión, deberán cumplir con los requisitos de rigor de forma, contenidos y uso de la identidad corporativa institucional. Serán solicitados al Departamento de CPRPAE por los directivos de áreas funcionales autorizadas para publicar los comunicados. El Departamento podrá establecer vínculos directos de las áreas con el *webmaster* a fin de garantizar la inmediatez.

La aprobación y autorización del contenido de comunicados corresponderá a las siguientes áreas funcionales:

- a) Comunicados generales de alta relevancia o trascendencia. – Serán aprobados por el Rector y los Vicerrectores.
- b) Comunicados de gestión del Talento Humano. - Serán aprobados por el Jefe de Departamento de Talento Humano.
- c) Comunicados de la gestión del Bienestar Universitario. – Serán aprobados por el Director de Bienestar Universitario.
- d) Comunicados de publicidad, mercadeo educativo y admisiones. – Serán aprobados por la Dirección General institucional.
- e) Comunicados del proceso de internacionalización y movilidad. – Serán aprobados por la Unidad de Relaciones Internacionales e Interinstitucionales (URII).
- f) Comunicados específicos del PCD, cursos, talleres, talleres metodológicos. – Serán aprobados por el Vicerrectorado Académico o en su delegación a las autoridades de las funciones sustantivas.

Los comunicados que impliquen emitir juicios de valor, distinciones o reconocimientos a miembros de la comunidad o áreas funcionales estarán en correspondencia con resoluciones del CAS o aquellas que las primeras autoridades ejecutivas autoricen formalmente.

Artículo 39. - Mensajes grupales de plataformas educativas LMS. – Como recurso, las aulas o salas virtuales creadas en las plataformas LMS institucionales podrán enviar mensajes de avisos y notificaciones a los estudiantes o participantes matriculados o habilitados en actividades docentes de asignaturas, cursos, talleres, entre otras. La funcionalidad de este recurso será responsabilidad del administrador designado de la plataforma, la dirección del CESDEL y de la dirección de Tecnologías Informáticas.

Artículo 40. – Buenas prácticas de uso del correo electrónico. – Las buenas prácticas del uso del correo electrónico institucional son responsabilidad del proveedor y de los usuarios.

a) Responsabilidades del proveedor:

- 1. Garantizar la funcionalidad, la autenticación y contraseñas seguras, cifrado de datos y ciberseguridad;
- 2. Dar seguimiento al buen uso de cuentas, activación y desactivación según las regulaciones de este instructivo y las restantes normas internas;
- 3. Implementación de políticas y directivas generales que faciliten y no obstaculicen el flujo de información entre los usuarios;

4. Los registros y etiquetas de usuarios deberán contener los nombres y apellidos completos y la información correcta del usuario que previo consentimiento determine la dirección de tecnologías Informáticas; y,
5. Garantizar la institucionalidad de firmas y notas de advertencia de uso.

b) Buenas prácticas de los usuarios:

1. Uso estrictamente institucional. - La cuenta debe usarse exclusivamente para los fines, proyectos y actividades vinculadas a las funciones de dirección, funciones sustantivas de docencia, investigación, vinculación con la sociedad y de procesos habilitantes de asesoría y apoyo. No se deberá utilizar para suscripciones personales, promociones o actividades ajenas a la institución;
2. No participación en el reenvío o cadenas, ni difundir material ajeno a los fines institucionales, de carácter ofensivo o discriminatorio;
3. Revisión periódica de la bandeja de entrada que garantice el flujo de información de procesos internos o externos;
4. Acusar recibo de correos que contienen avisos, indicaciones, solicitudes y otras prerrogativas institucionales. El acuse de recibo deberá realizarse exclusivamente al remitente;
5. Cumplimiento de políticas y directivas de la Dirección de Tecnologías, en cuanto al uso de adjuntos y vínculos de almacenamiento en la nube;
6. Redactar correos bajo criterios que permitan la lectura y comprensión eficaz considerando lo siguiente:
 - Asunto claro y directo. – El asunto deberá resumir el contenido del correo.
 - Estructura profesional. - Utilizar saludos y despedidas formales. Emplear párrafos cortos, viñetas o listas estructuradas para que la lectura sea rápida y eficaz.
 - Tono adecuado. - Mantener siempre un lenguaje respetuoso, objetivo y enfocado en el entorno laboral o académico.
 - Gestión de destinatarios. - Enviar el correo o responderlo solo a quienes realmente necesitan recibirlo. Utilice el campo CC (Copia) para quienes solo requieren estar informados y CCO (Copia oculta) para proteger la privacidad de las direcciones al enviar correos masivos.
 - Utilizar pies de firmas y etiquetas adecuadas.
 - Uso de asistentes de IA. – El uso de asistentes de IA deberá garantizar una estructura adecuada, no repetitiva del texto, sin extensiones innecesarias, elementos repetitivos, ni elementos que desvirtúen el propósito de la comunicación ni contrarios a la ética institucional.

Sección 7

Pertinencia y calidad de la información y los soportes de comunicación

Artículo 41. Pertinencia de la información. – La información contenida en los canales de comunicación institucional pública será pertinente cuando sea auténtica, aborde de los temas relevantes a la proyección social y de impacto de la universidad, exprese el buen desempeño de las funciones sustantivas de la educación superior, cuya profundidad y alcance del contenido sean accesibles a la comunidad, sea intercultural y no discriminatoria, esté actualizada, sea adecuada al contexto geográfico y cultural y en general cumpla con los principios rectores del flujo de información y comunicación que se indican en este Reglamento.

Artículo 42.- Requisitos de calidad de la información y comunicación institucional. La información y comunicación difundida a través de los canales oficiales de la Universidad Metropolitana deberá cumplir requisitos de calidad, veracidad, oportunidad, pertinencia, actualización, claridad, coherencia institucional, accesibilidad, trazabilidad y seguridad, conforme a la naturaleza del canal utilizado y al público destinatario.

Estos requisitos serán aplicables, según corresponda, al sitio *web* institucional, redes sociales, plataformas audiovisuales, plataformas de comunicación con organismos del Sistema de Educación Superior y del Estado, páginas *web* y *blogs* institucionales, aplicaciones académicas y administrativas, soportes de comunicación académica y científica, plataformas de conocimiento, correo electrónico institucional y demás herramientas de comunicación física o digital autorizadas por la Universidad.

La información y comunicación institucional deberá observar, además, los lineamientos de imagen, identidad y filiación institucional previstos en el Reglamento General al Estatuto, el Manual de Identidad Corporativa y la normativa interna aplicable. De igual manera, deberá respetar las reglas sobre protección de datos personales, privacidad, seguridad de la información, ciberseguridad, ética institucional, integridad académica y uso ético, responsable y seguro de la inteligencia artificial, cuando corresponda.

El Rector, por iniciativa propia o a pedido de las autoridades competentes, podrá disponer revisiones, verificaciones o auditorías sobre los canales oficiales de comunicación institucional, incluidas las redes sociales, con el objeto de evaluar su calidad, pertinencia, seguridad, cumplimiento normativo, coherencia con la identidad institucional, trazabilidad, métricas de desempeño y eventuales riesgos reputacionales, jurídicos, tecnológicos o de protección de datos personales.

Artículo 43. Ciclo de vida de los soportes de información y comunicación institucional. – La Universidad definirá la línea base de sus soportes tecnológicos, plataformas propias, plataformas *web* y aplicaciones de *software*, considerando su alcance institucional, accesibilidad, adecuación a las necesidades de la gestión académica y administrativa, sostenibilidad, costos, interoperabilidad, seguridad y atributos de calidad.

Para estos efectos, se observarán como referentes metodológicos los atributos de funcionalidad, fiabilidad, usabilidad, eficiencia del rendimiento, compatibilidad, seguridad, mantenibilidad y

portabilidad previstos en la Norma ISO/IEC 25010, así como las normas ISO 9001 e ISO/IEC 27001, sus reformas, modificaciones, actualizaciones o las normas que las sustituyan, en cuanto faciliten la implementación de sistemas de mejora continua, aseguramiento de la calidad y seguridad de la información.

El ciclo de vida de los soportes tecnológicos de información y comunicación institucional comprenderá el conjunto de fases por las que atraviesa un activo tecnológico y la información asociada a este durante su existencia, incluidas la planificación, evaluación, adquisición, contratación, desarrollo, implementación, configuración, uso, administración, actualización, mantenimiento, monitoreo, respaldo, sustitución, retiro, disposición final o reciclaje responsable, según corresponda.

Los ciclos de vida de la información documental, archivos, expedientes, registros y datos institucionales se gestionarán conforme al Reglamento del Sistema de Gestión Documental y de Archivos, al Reglamento para la Protección de la Privacidad, de la Información y de los Datos Personales, a las Políticas de Protección de Datos Personales y a la normativa interna aplicable.

CAPÍTULO II

INSTRUMENTOS PARA OBTENER Y PROCESAR INFORMACIÓN INSTITUCIONAL

Artículo 44. Instrumentos para obtener y procesar información institucional. - El uso de instrumentos para obtener y procesar información de interés institucional para la mejora continua y progresiva de los procesos de gestión académica y administrativa, entre ellos la realización de foros de discusión y las encuestas a través de aplicaciones en línea, será centralizada ejecutivamente por el área correspondiente de la función directiva, deberá realizarse en soporte informático de *MS Office 365* del dominio www.umet.edu.ec u otra que resultara autorizada por la dirección de Tecnologías.

Artículo 45. Elaboración de encuestas. - La elaboración de los instrumentos considerará la definición del tipo de encuesta, cuestionarios, preguntas y aseveraciones a consulta, objetos y sujetos de aplicación, alcance, tamaño de muestras, población y consultas del tratamiento de privacidad y protección de datos personales.

Artículo 46. – Foros de discusión. – Los foros de discusión podrán ser utilizados para obtener información útil para los objetivos de la mejora de procesos a partir de espacios digitales en los que se sigan hilos de discusión por los cuales se intercambian ideas sobre temas de interés institucional. Los foros de discusión serán diseñados con base en la definición de temas o preguntas para la retroalimentación de la gestión de procesos institucionales. Según el objeto del foro, el moderador o gestor abre el foro para que sobre un tema cualquier participante pueda iniciar una nueva discusión, una única discusión o un foro de preguntas elaboradas por el moderador. Los espacios de foro podrán programarse en fechas, permitir carga y descarga de archivos, inicio y fin de subscripción, entre otras utilidades que faciliten sus objetivos.

Artículo 47. Gestor del instrumento. - El gestor del instrumento será el directivo cuyas funciones se relacionen con el objeto de aplicación del instrumento o aquel que designen las

primeras autoridades para su elaboración, aplicación, procesamiento e informe de resultados.

Artículo 48. Tratamiento de la información. – Todo instrumento, formulario, encuesta, entrevista, registro, ficha, base, aplicativo, plataforma o mecanismo institucional destinado a recabar, tratar, analizar, comunicar o conservar información o datos personales deberá identificar previamente, de forma clara y documentada, al menos: la finalidad del tratamiento, las categorías de información o datos a recabar, la base jurídica aplicable, el responsable interno del tratamiento, la unidad gestora, los destinatarios o usuarios autorizados, el plazo de conservación, las medidas de seguridad, las condiciones de confidencialidad y el procedimiento para el ejercicio de derechos de los titulares, cuando corresponda.

Cuando el tratamiento se sustente en el consentimiento del titular, este deberá ser libre, específico, informado e inequívoco, conforme a la Ley Orgánica de Protección de Datos Personales, su Reglamento General, la normativa secundaria aplicable y las Políticas de Protección de Datos Personales de la Universidad. No serán válidos los consentimientos genéricos, tácitos, ambiguos, incorporados en cláusulas amplias o desvinculados de una finalidad determinada.

Cuando los instrumentos de levantamiento de información se vinculen con investigación, proyectos académicos, estudios institucionales, innovación, vinculación con la sociedad o cualquier actividad que implique recolección de información sobre seres humanos, deberá verificarse previamente si corresponde revisión ética por el Comité Universitario de Ética, el Comité de Ética de la Investigación con Seres Humanos o la instancia competente, según la naturaleza del proyecto. Esta revisión será especialmente necesaria cuando se recaben datos sensibles, información de salud, datos de niñas, niños o adolescentes, información socioeconómica, opiniones, hábitos, desempeño académico, datos laborales, información biométrica o cualquier otra información que pueda generar riesgos para los titulares.

Antes de la aplicación del instrumento, la unidad gestora deberá realizar el análisis preliminar de finalidad, necesidad, proporcionalidad, base jurídica, minimización, confidencialidad, seguridad y riesgos del tratamiento. Cuando el instrumento involucre datos personales, datos sensibles, tratamientos a gran escala, transferencias, uso de plataformas externas, inteligencia artificial, menores de edad o riesgos relevantes para los titulares, deberá solicitarse criterio del Delegado de Protección de Datos Personales y, de ser necesario, de la Dirección de Tecnologías Informáticas, del Comité competente y de la Procuraduría Nacional, sin perjuicio de la autorización de la autoridad académica o administrativa que corresponda conforme a la normativa interna.

Artículo 49. Consultas del tratamiento de datos personales. – La unidad gestora o responsable del instrumento, antes de elaborar, aplicar, procesar o generar informes que impliquen tratamiento de datos personales, deberá verificar si el tratamiento se encuentra previsto en las Políticas de Protección de Datos Personales de la Universidad Metropolitana y en el Registro de Actividades de Tratamiento, RAT.

Cuando el tratamiento no conste en el RAT, modifique una finalidad previamente registrada, incorpore nuevas categorías de datos, implique nuevos destinatarios, transferencias, uso de

plataformas externas, tratamiento de datos sensibles, datos de menores de edad, decisiones automatizadas, uso de inteligencia artificial o cualquier otro supuesto de riesgo relevante, la unidad gestora deberá solicitar criterio previo al Delegado de Protección de Datos Personales y al responsable interno del tratamiento, sin perjuicio de la intervención de la Dirección de Tecnologías Informáticas, de la Procuraduría Nacional o del Comité competente cuando la naturaleza del caso lo requiera.

El Delegado de Protección de Datos Personales emitirá las recomendaciones técnicas y jurídicas que correspondan en materia de licitud, finalidad, minimización, proporcionalidad, transparencia, confidencialidad, seguridad, conservación, ejercicio de derechos y necesidad de evaluación de impacto. El responsable interno del tratamiento dispondrá, cuando corresponda, la aprobación interna, actualización o incorporación del tratamiento en el RAT, con apoyo de la unidad gestora y de las unidades competentes.

Ningún instrumento, encuesta, formulario, aplicativo, base de datos, plataforma o mecanismo institucional que implique un nuevo tratamiento de datos personales, o una modificación sustancial de uno existente, podrá aplicarse sin que previamente se haya verificado su base jurídica, finalidad, medidas de seguridad, responsabilidades funcionales y registro o actualización en el RAT, cuando corresponda.

Artículo 50. Autorización para la aplicación de los instrumentos. – Una vez elaborada la encuesta o los temas para el caso del foro, la supervisión de calidad y la consulta del tratamiento de privacidad y protección de datos de los participantes, la autorización de su aplicación se realizará por las autoridades según el siguiente alcance:

a) El Rector o en quien delegue:

1. Instrumentos para gestionar información relevante de múltiples actores, para toda la institución, o de alcance limitado a una o varias de sus facultades o sedes; y,
2. Instrumentos a aplicar para recabar información institucional por actores externos, pasantes nacionales e internacionales, en el marco de investigaciones en colaboración, redes y otros actores externos. En este caso deberá existir un convenio interinstitucional que regule lo necesario sobre la gestión de información, la propiedad intelectual y el uso de la identidad corporativa institucional.

b) El Vicerrector Administrativo:

1. Instrumentos para gestionar información relevante para toda la institución, una o varias de sus facultades o sedes, de los estudiantes para la gestión del bienestar universitario,
2. Instrumentos de aplicación al personal directivo o trabajadores de los procesos habilitantes de apoyo;

c) El Vicerrector Académico:

1. Instrumentos para gestionar información del personal académico y de apoyo académico;
2. Instrumentos para el seguimiento a graduados, graduados, empleadores, organismos, organizaciones o empresas para toda la institución;

3. Seguimiento a prácticas preprofesionales, tareas de investigación o de servicios a la comunidad; ambos con presentación previa de los decanos para las facultades y sedes;
 4. Evaluación del desempeño y satisfacción del personal según los instrumentos regulados en el Manual de Planificación del Trabajo Individual y Evaluación del Desempeño;
- d) Los decanos autorizarán, cuando corresponda, encuestas a estudiantes en el marco de asignaturas, cursos, talleres y otras actividades en entornos virtuales de las plataformas LMS institucionales; y,
- e) Coordinadores de carreras y programas de posgrados los foros en el marco de cursos, talleres y otras actividades en entornos virtuales de las plataformas LMS institucionales.

Artículo 51. Requisitos de calidad del instrumento y validación estadística. – Los instrumentos deberán cumplir con requisitos de utilidad, viabilidad, objetividad y criterios de calidad según el propósito. Los resultados deberán ser objeto de validación estadística utilizando las herramientas de software y estadígrafos apropiados de confiabilidad. Aquellos instrumentos que no demuestren su validez estadística deberán ser analizados para su rediseño y los resultados no podrán ser tomados en cuenta para la toma de decisiones.

Artículo 52. – Confidencialidad y difusión de resultados. – El gestor del instrumento aplicado garantizará los elementos de confidencialidad y privacidad según el propósito y el uso de la información que fueren aprobados en cuanto al tratamiento de datos. La difusión de resultados como parte de informes académicos o administrativos, tesis, trabajos de titulación, artículos, libros, capítulos de libros, ponencias o alguna otra forma de publicación deberá ser aprobada por la autoridad o directivo inmediato del gestor. Para ello se tendrá en cuenta lo establecido en cuanto a los requisitos de calidad, validación estadística y las consideraciones éticas de este Reglamento y la normativa interna.

Artículo 53. Participación de la comunidad universitaria en la aplicación de instrumentos por otras organizaciones. – Se prohíbe la participación de miembros de la comunidad universitaria en encuestas sobre aspectos de la actividad institucional que no sean debidamente analizadas y autorizadas por el CAS cuya información pueda ser utilizada en perjuicio de ella.

Artículo 54. – Instrumentos de investigación educativa. – La aplicación de instrumentos para recabar información en el marco del trabajo científico metodológico institucional, según lo establece el Reglamento Interno de Régimen Académico, será parte de proyectos de IDi aprobados institucionalmente para la mejora continua y la innovación institucional.

La aplicación de instrumentos en el marco de proyectos interinstitucionales de investigación e innovación deberá estar aprobada en el marco de estos, previo establecimiento de las condiciones de tratamiento de información y datos, propiedad intelectual debidamente establecidas y convenientes.

TÍTULO IV

PLATAFORMAS INSTITUCIONALES DE GESTIÓN ACADÉMICA Y ADMINISTRATIVA

Artículo 55. Plataforma Sistema Nacional Académico y Administrativo (SNAA). – El SNAA es la plataforma de gestión académica y administrativa de la UMET. La plataforma será administrada por el Director de Tecnologías Informáticas quien es el responsable de su funcionalidad, actualizaciones y nuevos desarrollos según el Plan Estratégico de la Transformación Digital de la Universidad.

El SNAA deberá integrar aplicaciones de soporte a los procesos de dirección, funciones sustantivas y procesos habilitantes de asesoría y apoyo.

La plataforma de gestión académica y administrativa deben proveer igual información que la requerida en el Sistema Integral de Información de la Educación Superior (SIIES) y adaptar las aplicaciones internas a este objetivo.

La responsabilidad de los accesos, las seguridades, respaldos y ciberseguridad son de entera responsabilidad del Director de Tecnologías Informáticas.

a) Información de entrada. – La información de entrada a la plataforma SNAA será provista por las áreas funcionales de gestión del TTHH, SGT, DG, Bienestar Universitario, direcciones de funciones sustantivas, unidad de planificación docente y el profesorado para la carga de las calificaciones. La veracidad y calidad en general de la información y datos será responsabilidad del personal directivo o en general por los usuarios designados.

b) Información de salida para la gestión universitaria y el SIIES:

1. Información de sedes y extensiones
2. Información de instalaciones e infraestructuras
3. Información de recursos de aprendizaje
4. Ejecución financiera
5. Períodos académicos
6. Unidades académicas
7. Carreras o programas
8. Asignaturas / cursos / equivalentes
9. Información personal de estudiantes
10. Trayectoria académica de los estudiantes
11. Información financiera, becas y ayudas económicas
12. Mallas curriculares, prerrequisitos y correquisitos
13. Información documental de soporte del portafolio del estudiante
14. Información de egresados y seguimiento
15. Evaluaciones del estudiante
16. Información personal de profesores

17. Planificación docente
18. Distribuciones horarias
19. Trayectoria de contratos laborales
20. Formación del claustro
21. Información documental de soporte de la carpeta del docente
22. Evaluación del desempeño
23. Líneas, programas y proyectos de IDi y vinculación
24. Matriz de publicaciones, producción artística y registros
25. Matriz de eventos
26. Repositorio documental de proyectos, publicaciones y otras salidas.
27. Parametrización y recuperación de reportes de información
28. Recuperación de documentos de archivo

c) Sistema Institucional de Datos y Estadísticas (SIDE)

El SIDE será parte integrada al SNAA como la aplicación que provee las variables cuantitativas, datos, información estadística, indicadores e índices del seguimiento al PEDI, POA y PMI. Será el proveedor de los indicadores del Cuadro de Mando Integral (CMI).

El CMI es la herramienta de gestión académica y administrativa para el seguimiento a la planificación estratégica y operativa institucional y de sus áreas funcionales, la mejora continua y todos los procesos que requieren evaluación, retroalimentación y seguimiento. Proveerá la información de indicadores e índices formalizados, que permitan recuperar información en series históricas por períodos, niveles de gestión, facultades, sedes, carreras, programas de posgrados y el cumplimiento de las metas de las áreas funcionales académicas y administrativas.

La formalización de los indicadores establecerá la denominación y descripción del indicador, variables, períodos, unidades funcionales, fórmula de cálculo, representaciones gráficas definición, responsabilidades, umbrales y objetivos; de acuerdo con la planificación estratégica, operativa y de mejora continua. Deberá sustentarse en herramientas informáticas avanzadas, que permitan la integración de la IA, la agregación y consolidación de indicadores en los tres niveles de gestión: 1. Nivel de los impactos de la misión y visión y las grandes metas estratégicas institucionales; 2. Nivel de la estrategia y táctica. Incluyen los indicadores e índices referentes de la evaluación externa, acreditación y mejora continua institucional; y 3. Nivel operativo. Gestión de los procesos de las unidades funcionales de base, los escenarios de actuación y los equipos de trabajo de profesores y estudiantes.

Los escenarios de seguimiento y control, los procedimientos, informes y la caracterización general de indicadores y estándares estarán definidos en los capítulos respectivos del PEDI y el PMI.

Artículo 56. Sistema Estructurado de Gestión del Aprendizaje Virtual. – El Sistema

Estructurado de Gestión del Aprendizaje Virtual de la Universidad Metropolitana (SEGAV/UMET) es el sistema institucional que integra las plataformas LMS (*Learning Management System* / Sistema de Gestión del Aprendizaje), los servicios digitales y los procesos destinados a la gestión académica en entornos virtuales y mixtos de enseñanza y aprendizaje. Las regulaciones relacionadas con el sistema serán las contenidas en el Reglamento del Centro de Educación Semipresencial, a Distancia y en Línea (CESDEL).

Las plataformas LMS de la UMET, sus centros, la Plataforma Multilateral CEC y toda aquella plataforma que aloje oferta académica institucional y de servicios fuera del dominio umet.edu.ec deberá cumplir con los términos y condiciones del uso de la identidad corporativa institucional, principios éticos y valores que promueve la institución, la protección de datos, propiedad intelectual y ciberseguridad.

TÍTULO V

PLATAFORMAS DE GESTIÓN ACADÉMICA Y ADMINISTRATIVA DE ORGANISMOS PÚBLICOS

Artículo 57. Plataformas digitales de comunicación del gobierno y los organismos públicos.

- El Rector y el Secretario General Técnico administrarán los correos electrónicos institucionales y plataformas digitales establecidas para recibir comunicación externa de los organismos de la administración del estado y sus dependencias, que requieran la atención de las primeras autoridades. La información oficial en contestación a requerimientos de esas instancias será únicamente remitida por el SGT.

Artículo 58.- Patrocinio de procesos judiciales, administrativos y contractuales.

El Procurador Nacional de la Universidad Metropolitana, en el ámbito de las competencias previstas en el Estatuto Institucional, el Reglamento General al Estatuto y la normativa interna aplicable, tendrá a su cargo la gestión jurídica, patrocinio, seguimiento, custodia y coordinación de la información y comunicación relacionada con los procesos judiciales, administrativos, arbitrales, constitucionales, contractuales, extrajudiciales y demás asuntos jurídicos en los que intervenga o tenga interés la Universidad.

La información generada, recibida o custodiada en el marco de dichos procesos tendrá el nivel de reserva, confidencialidad o acceso que corresponda conforme a su naturaleza, al estado procesal, a la estrategia jurídica institucional, a las disposiciones de autoridad competente y a la normativa sobre protección de datos personales, privacidad, seguridad de la información y gestión documental.

La Procuraduría Nacional podrá requerir información, documentos, informes técnicos, certificaciones, antecedentes, respaldos y criterios a las autoridades, unidades académicas, unidades administrativas, sedes, centros, direcciones y demás dependencias institucionales, cuando sean necesarios para la defensa de los intereses de la Universidad, la emisión de criterios jurídicos, la elaboración de contratos, la atención de requerimientos oficiales o el cumplimiento de actuaciones procesales.

La comunicación externa sobre procesos judiciales, administrativos, contractuales o asuntos jurídicos sensibles deberá ser previamente coordinada con la Procuraduría Nacional y autorizada por la autoridad competente, sin perjuicio de las obligaciones de comparecencia, respuesta, entrega de información o actuación procesal que deban cumplirse dentro de los plazos legales.

La Procuraduría Nacional mantendrá la trazabilidad documental de sus actuaciones y coordinará con la Secretaría General Técnica, la Dirección de Tecnologías Informáticas, la Dirección Financiera, Talento Humano, las sedes y demás unidades competentes, según la naturaleza del asunto, para asegurar la conservación, seguridad, integridad, disponibilidad y uso legítimo de la información jurídica institucional.

Artículo 59. Plataformas del Consejo de Educación Superior (CES). - El Secretario General Técnico será el único directivo con acceso al Sistema Nacional de Información de Educación Superior del Ecuador (SNIESE) y al Sistema de Acompañamiento Previo para Recolección de Información (SAPPRI) del CES, cuya función será indelegable y en su caso por causa de fuerza mayor autorizada por el Rector.

Artículo 60. Sistema Integral de Información de la Educación Superior (SIIES). Este sistema tendrá como usuario para el control de seguridades y supervisión del primer nivel al Rector, así como usuarios habilitados en un segundo nivel para la gestión de la información, uno el Especialista Principal de la CIAC y otro Especialista Informático, como soporte a procesos específicos como interfaz con las autoridades y directivos proveedores de la información.

Artículo 61. Plataformas o aplicativos informáticos del sistema de aseguramiento de la calidad del CACES. – Para la gestión de información en este tipo de aplicativos el Rector tendrá el usuario de control de seguridades y supervisión general de los procesos abiertos, seguido del usuario de procesos, el Especialista Principal de la CIAC y otro Especialista Informático, como soporte a procesos específicos como interfaz con las autoridades y directivos proveedores de la información.

Artículo 62. Plataformas informáticas del MdT, el SUT y el IESS. – El acceso a estas plataformas u otras relacionadas con la gestión del personal, el cumplimiento de obligaciones y nóminas de la institución, son de entera responsabilidad, control y seguimiento de la Jefatura de Talento Humano, lo mismo que las comunicaciones recibidas, enviadas y sus registros, incluyendo de los accesos y las claves asignadas a los RUC de todas las sedes.

Los usuarios y claves estarán bajo la custodia de esa dirección y serán entregadas con copia en sobre sellado para su custodia al SGT. La delegación a asistentes es de su entera responsabilidad y deberá ser aprobada por el Vicerrector Administrativo tomando en cuenta las funciones desconcentradas del director de la sede Machala.

El jefe del Departamento de TTHH tendrá acceso en cualquier momento a todas las plataformas de las sedes. Cualquier cambio en las claves mencionadas deberán ser autorizadas por la jefe de TTHH y entregadas en sobre sellado al SGT.

Artículo 63. Servicio de Rentas Internas. - El acceso a las cuentas del SRI es de entera responsabilidad de la Dirección de Contabilidad y Finanzas, lo mismo que la información de

cuentas bancarias operativas de toda la institución, las comunicaciones recibidas, enviadas y sus registros, incluyendo de los accesos y las claves asignadas a los RUC de todas las sedes.

Los usuarios y claves estarán bajo la custodia de esa dirección y serán entregadas con copia en sobre sellado para su custodia al SGT. El Director de Contabilidad y Finanzas considerará lo que corresponda bajo autorización del Vicerrector Administrativo sobre la función desconcentrada del director de la sede Machala y tendrá acceso en cualquier momento a todas las plataformas de las sedes. Cualquier cambio en las claves mencionadas deberá ser autorizado por el Director de Contabilidad y Finanzas y entregado en sobre sellado al SGT.

Artículo 64. – Plataforma de Presentación de Carreras y Programas (PPCP). - El acceso a la PPCP, del Consejo de Educación Superior (CES), cambios de claves y otras actividades de administración es exclusivo del Rector y el SGT. En el caso de la carga de información y seguimiento de proyectos de carreras y programas, previa firma de responsabilidad es responsabilidad del decano, lo mismo que la carga de información de respuestas observaciones y otras solicitudes, que realice directamente o por el profesor responsable del proyecto que haya designado, también es responsable de la comunicación directa o a través de consultas técnicas con las comisiones del CES relacionadas con los proyectos de su ámbito.

TÍTULO VI

REPOSITORIOS DE INFORMACIÓN INSTITUCIONAL

Artículo 65. Repositorios digitales de información institucional. – Los repositorios digitales de información documental de la Universidad Metropolitana serán parte del Sistema de Gestión Documental y de Archivos (SGDA). Este sistema de registrará por el Reglamento Interno del Sistema de Gestión Documental y de Archivos, que establece las normas, principios, procedimientos, instrumentos técnicos y responsabilidades aplicables a la producción, recepción, registro, organización, descripción, trámite, conservación, transferencia, acceso, disposición final y preservación de los documentos institucionales, en cualquier soporte o formato. La información institucional estará compuesta además por archivos digitales asociados a las fuentes documentales en distintos formatos de textos, tabulación electrónica, imágenes, audios y videos.

Serán repositorios articulados y estructurados para los propósitos institucionales con soporte de aplicaciones de software estandarizados y de uso universal que satisfagan las necesidades de alojamiento, almacenamiento, gestión colaborativa, trazabilidad y recuperación de la información.

Artículo 66. Plataforma integral de gestión de contenidos de la organización. – La plataforma de línea base para la gestión de contenidos (documentos, recursos digitales entre otros) de los procesos de la UMET es la plataforma *ALFRESCO*. Esta plataforma, sus versiones, actualizaciones o sustitución por otra proporcionarán un sistema de gestión de los contenidos de la institución para capturar, almacenar, gestionar y colaborar sobre documentos e información digital de manera centralizada y segura, contenidos web, flujos de trabajo, colaboración en tiempo real y administración de registros conforme a estándares internacionales. El desarrollo de las funcionalidades de la plataforma será brindado y administrado por la Dirección de Tecnologías Informáticas.

Artículo 67. Repositorio Digital UMET. – El Repositorio Digital de la UMET tendrá una gestión distribuida, lo que significa la estructura por perfiles de usuarios, actividades, tareas, sitios, ficheros, ficheros compartidos, documentos, calendario, entre otras funciones.

El repositorio se organizará por procesos, entre ellos los siguientes:

- a) Procesos de gestión de información en el Repositorio Digital de la UMET:
 - 1. Sistema de Aseguramiento de la Calidad. – Alojará las fuentes documentales y de contenidos del Plan de Mejoras Institucional (PMI) y su seguimiento. Este proceso se gestiona por el Especialista Principal de la CIAC.
 - 2. Planificación Estratégica y Operativa Anual. – Alojará la información de los procesos de planificación estratégica y operativa anual y su seguimiento. Este proceso se gestiona por el Especialista Principal de la CIPE.
 - 3. Información de las Unidades Académicas. – Información estructurada del nivel del Vicerrectorado, funciones sustantivas, centros de apoyo a las funciones sustantivas, facultades y UAFTT, sedes, carreras y programas. Este proceso se gestiona por los usuarios de las unidades académicas y se supervisa por el Vicerrectorado Académico.
 - 4. Información de los procesos de apoyo. – Información estructurada del nivel del Vicerrectorado Administrativo, direcciones y dependencias departamentales. Este proceso se gestiona por los usuarios de las unidades funcionales de los procesos de apoyo y se supervisa por el Vicerrectorado Administrativo. La Dirección General habilitará un repositorio de Contratos de servicios y el Departamento de Talento Humano para los contratos de personal cumpliendo las disposiciones de la Resolución No. UMET-REC-2025-005 aprobatoria del “*Instructivo para la Gestión de Contratos de la Universidad Metropolitana*”. Todos los contratos serán de acceso cuando lo solicite el Procurador Nacional.
- b) Procesos de certificación de formación continua. – La emisión y formalización de certificados de formación continua y formación continua avanzada se establecerán según las disposiciones de la Resolución No. UMET-REC-2025-002 aprobatoria del “*Instructivo para la Certificación de Actividades de Formación Continua y Formación Continua Avanzada*”, Los certificados digitales serán válidos solamente cuando cuenten con un código alfanumérico único y un código QR para verificación.
- c) Proceso de gestión de información científico – tecnológica. – Los repositorios de ICT como recursos de aprendizaje e investigación serán gestionados por el CRAI en sus páginas web institucionales de conformidad con el reglamento del centro. La dirección de Investigación e Innovación actualizará al menos al final de cada semestre las páginas de publicaciones de artículos y libros que son el resultado de los proyectos de IDi y vinculación con la sociedad.
- d) Procesos de gestión de información de procesos del Rectorado. – Información del Rectorado, repositorios específicos del Consejo Académico Superior (CAS) y de Procuraduría. Estos procesos se gestionan por el Rector, el Secretario del CAS y el

Procurador respectivamente. Se supervisan por el Rector.

Los repositorios específicos tendrán la información sobre:

1. Repositorio del Consejo de Regentes. - Documentos de convocatoria, actas de la sesión, resoluciones, acuerdos, insumos documentales, grabaciones de las sesiones, etc. Este repositorio se gestiona por el Secretario Ejecutivo del CR. Cumplirá las disposiciones del Reglamento del Consejo de Regentes.
2. Repositorio del Consejo Académico Superior. – Documentos de convocatoria, actas de la sesión, resoluciones, acuerdos, informes e insumos documentales, grabaciones de las sesiones. Este repositorio se gestiona por el Secretario General Técnico. Cumplirá las disposiciones del Reglamento de Funcionamiento del Consejo Académico Superior.
3. Convenios interinstitucionales. – Documentos de convenios según las disposiciones de la Resolución No. UMET-REC-2025-004, aprobatoria del *“Instructivo para la Gestión de Convenios Interinstitucionales de la Universidad Metropolitana”*. La Secretaría General Técnica dispondrá y actualizará sistemáticamente la base de datos de convenios interinstitucionales y su repositorio institucional.

Artículo 68. Flujo y formalización documental del rectorado. – El flujo ordenado de documentos que requieren la firma del Rector como representante legal de la institución se establece en la Resolución No. UMET-REC-2024-006 de fecha 12 de noviembre de 2024, aprobatoria del *“Protocolo para la Solicitud, Revisión y Registro de Documentos que Requieren la Firma del Rector”*, en el cual se regula el procedimiento para la solicitud, revisión, aprobación, suscripción, registro y archivo de los documentos que requieren la firma del Rector. Con referencia a los oficios, informes, contratos, certificaciones y otros de cualquier índole con la finalidad de garantizar la responsabilidad, corresponsabilidad, veracidad, legalidad, cumplimiento de estándares, transparencia, confidencialidad y protección de la información;

Artículo 69. Calidad de las fuentes documentales. – La información documental en el Repositorio Institucional cumplirá los siguientes criterios de calidad:

- a) Cumplir las especificaciones según el tipo de documento en cuanto a encabezados, número de oficios o resoluciones, cortesías, etc.;
- b) Cumplimiento de los requisitos del Manual de Estilos de la UMET para el uso de pautas, tamaño de hojas, márgenes, formatos de párrafos, letras, tamaño de letras, sangrías, paginación, números de página, identificadores, citas y referencias, entre otros parámetros. El estilo podrá tener especificaciones para oficios, actas, informes, resoluciones, memorándums, documentos jurídicos de procuraduría, u otros documentos siendo la aprobación de estos una atribución de las primeras autoridades para sus dependencias correspondientes;
- c) Registrar información veraz y significar las fuentes de elaboración u obtención de datos;
- d) Contar con una calidad y estética adecuadas cuando se insertan imágenes, gráficas, tablas u otras representaciones gráficas;

- e) Cumplir la estructura de contenidos de los documentos señalada en reglamentos, manuales, instructivos y protocolos, así como la que se oriente por indicaciones o solicitudes específicas de información documental por las autoridades o aquellas solicitudes de organismos externos;
- f) Redacción precisa, profesional y apropiada al lenguaje técnico del proceso, inclusiva, no ofensiva, no discriminatoria y propia de los valores que proclama la institución;
- g) Formalidad institucional de créditos, firmas de responsabilidad y fechas. Los documentos deberán estar debidamente firmados. Las firmas físicas de las primeras autoridades deberán ser acompañadas de los correspondientes sellos de tinta; las firmas digitales de autoridades, directivos o personal académico y administrativo deberá corresponder a una firma digital válida en Ecuador.

Los pies de firma tendrán nombres y apellidos completos, títulos del firmante (ej: Ing., Lic., Ab., Eco., etc. / Nombres y apellidos completos / ej: Mgs., Mgtr., Espec., PhD.); el cargo o denominación del puesto, según el RGE/UMET o el Manual Orgánico Funcional.

Los pies de firmas podrán incluir varios firmantes según el tipo de documento con alcance a elaborado, revisado y aprobado;

- h) Otros criterios específicos con relación a la seguridad de la información que sean requeridos.

Artículo 70. Responsabilidad de la gestión del Repositorio Digital Institucional. – La debida información documental, disponibilidad y calidad, así como el nivel de actualización será responsabilidad de los usuarios en sus distintos niveles de dirección y ámbitos de gestión.

Artículo 71. Responsabilidad con las fuentes documentales. – La calidad, veracidad de la información y formalidades serán responsabilidad de quienes elaboran el documento y lo firman. No se podrá cargar en el Repositorio Institucional ninguna fuente documental sin la calidad y formalidades descritas en este Reglamento.

TÍTULO VII

SEGURIDAD DEL FLUJO DE INFORMACIÓN Y COMUNICACIÓN INSTITUCIONAL

Artículo 72. Políticas, tecnologías y procedimientos. – La seguridad del flujo de información y comunicación institucional en la Universidad Metropolitana estará conformada por el conjunto de políticas, normativas, tecnologías y procedimientos que garantizan que la información y los datos, correos, documentos y mensajes no sean interceptados, alterados o destruidos por personas no autorizadas.

Artículo 73. Principios básicos de seguridad y riesgos. – La seguridad del flujo de información y comunicación institucional que se oriente y regule en este Reglamento y la normativa interna

será objeto de control por la Dirección de Tecnologías Informáticas atendiendo a los principios básicos de confidencialidad, integridad, disponibilidad y autenticidad para garantizar la prevención y respuesta a las amenazas y riesgos de ciberseguridad, de interceptación, filtración accidental, ingeniería social y suplantación. En particular la vulneración a la privacidad, la protección de datos personales para usos diversos y la seguridad informática.

Artículo 74. Riesgos reforzados por la Inteligencia Artificial. – La institución, mediante la gestión de riesgos de sus sistemas informáticos prestará atención especial a los flujos de información que puedan ser vulnerados por aplicaciones de Inteligencia Artificial (IA) comprometedores de la confidencialidad, integridad y veracidad de las comunicaciones digitales, que a partir de su alta capacidad y potencial para manipular la información pueden producir los siguientes impactos indeseables:

- a) Desinformación: Los generadores de texto crean noticias falsas y propaganda a gran escala que pueden ser lesivos a la integridad institucional, la ética institucional, de la investigación y el aprendizaje;
- b) *Deepfakes*: Los atacantes pueden falsificar videos y clonar voces para engañar a los usuarios, afectar la imagen institucional y de los miembros de la comunidad universitaria;
- c) Phishing persuasivo: La IA redacta correos electrónicos personalizados y libres de errores gramaticales que hacen difícil su identificación y pueden traspasar barreras de contención de los sistemas de seguridad informática;
- d) Ataques de voz (*vishing*): Los estafadores usan clonación de voz en tiempo real para extorsionar suplantando identidades;
- e) Robo de datos: El uso de herramientas de IA no supervisadas puede provocar filtraciones de información corporativa y confidencial; y,
- f) Otros utilizados por la ciberdelincuencia para alterar las respuestas de los modelos de IA, inserción de comandos maliciosos en documentos y modificar registros sin supervisión humana.

Artículo 75. Prevención y mitigación de riesgos. – La prevención y mitigación de riesgos será una función institucional con alcance a todos los flujos de comunicación: descendente, ascendente, horizontal, diagonal y externa. Por lo tanto, participan del proceso todos los miembros de la comunidad universitaria quienes deberán cumplir las indicaciones del Sistema Institucional de Protección de la Privacidad, la Información y los Datos Personales de la Universidad Metropolitana, la política institucional y su normativa conexas; las indicaciones y mecanismos de Ciberseguridad que establece la normativa interna e implementa la Dirección de Tecnologías Informáticas para la adquisición de software y hardware, licencias y su utilización.

Artículo 76. Mecanismos básicos de protección y control. – Para asegurar el flujo de información y comunicación, además de las seguridades nativas de los sistemas digitales debidamente habilitadas y funcionales, la Dirección de Tecnologías Informáticas implementará acciones de seguridad de los activos digitales o informáticos, las aplicaciones, seguridad en la nube, seguridad de datos y de la infraestructura de red; el cifrado de extremo a extremo mediante

la codificación de correos y mensajería interna; controles de acceso mediante el otorgamiento de permisos estrictos basados en los roles del personal; las redes privadas virtuales (VPN) mediante el cifrado del tráfico para personal que labora de forma remota; y los acuerdos de confidencialidad (NDA) mediante las firmas de responsabilidad legal para empleados y proveedores.

DISPOSICIONES GENERALES

PRIMERA. - Sin perjuicio de las definiciones previstas en los reglamentos de Protección de la Privacidad, de la Información y de los Datos Personales y del Uso ético, Responsable y Seguro de la Inteligencia Artificial, para la interpretación y aplicación del presente Reglamento se entenderá por:

Activo digital o informático: todo recurso digital, tangible o intangible, incluidos datos, información, sistemas, aplicaciones o plataformas, que tenga valor para una persona, organización o institución y que requiera medidas de protección frente a incidentes de ciberseguridad.

Comunicación científica: conjunto de prácticas, herramientas y estrategias orientadas a compartir conocimiento científico de forma rigurosa, comprensible y contextualizada, con distintos públicos y en diversos formatos que implica destrezas, medios, actividades y diálogos apropiados para producir resultados como la concienciación, el disfrute, el interés, la formación de opinión y la comprensión de la ciencia.

Comunicación institucional: empero los flujos de comunicación interna y externa en la organización, la comunicación institucional es la forma en que una organización construye y transmite mensajes formales para representar su identidad, sus valores, su función y su relación con distintos públicos. No se trata solo de informar, sino de proyectar claridad, coherencia y legitimidad a través de la comunicación. Su propósito es transmitir mensajes formales sobre identidad, principios, valores, misión y visión estratégica, estructura, postura institucional, mensajes oficiales y relación con públicos clave.

Filiación institucional: en la información y la comunicación científica es la identificación formal de la institución con la que un autor está vinculado al momento de publicar trabajos científicos o académicos. Esta filiación actúa como respaldo institucional de la producción del autor y permite que las publicaciones sean correctamente asociadas a la institución en bases de datos, repositorios y métricas académicas.

Flujo de información y comunicación: el movimiento, intercambio y transmisión de información, datos, instrucciones o conocimientos entre personas, sistemas y procesos dentro de una organización o entorno operativo y aquella que conecta con su entorno. Conecta diferentes áreas y niveles jerárquicos internos y externos, para asegurar la visibilidad, la imagen, la proyección social y que la información relevante llegue al lugar y a las personas adecuadas de manera segura y en el momento oportuno.

Identificadores digitales: conjuntos de datos, credenciales o códigos únicos que permiten reconocer a una persona, entidad u objeto en el entorno virtual. En el ámbito de la comunicación

científica los identificadores digitales son utilizados para identificar las personas; acreditación de documentos; codificación alfanumérica para enlazar permanentemente a artículos científicos, libros u otros documentos digitales.

Norma ISO 25010: estándar internacional que define un modelo de calidad para software y sistemas, estableciendo características y sub características para evaluar su desempeño, fiabilidad, seguridad y usabilidad. La ISO/IEC 25010 forma parte de la serie SQuaRE (*Software Quality Requirements and Evaluation*) y proporciona un marco para especificar, medir y evaluar la calidad del software y sistemas informáticos. Su objetivo principal es garantizar que los productos digitales cumplan con altos estándares de calidad, ofreciendo valor a los usuarios y evitando errores o fallos que puedan afectar a las partes interesadas.

Normas ISO 9001: marco de referencia internacionalmente reconocido para implementar un sistema de gestión de la calidad efectivo. Estas normas, en constante evolución, ofrecen una guía práctica para mejorar los procesos, aumentar la satisfacción del cliente y fomentar la mejora continua.

Norma ISO 27001: estándar internacional que establece un marco para la gestión de la seguridad de la información en las organizaciones. Su objetivo principal es ayudar a las empresas a proteger la confidencialidad, integridad y disponibilidad de la información que manejan. Esta norma proporciona un conjunto de buenas prácticas y controles que permiten a las organizaciones identificar y gestionar los riesgos asociados a la seguridad de la información, incluyendo accesos no autorizados y ciberataques.

Redes sociales del conocimiento: espacios interactivos en que los productores, gestores y beneficiarios del conocimiento acceden, distribuyen y utilizan la información de manera colaborativa y abierta con participación colectiva a través de la conexión y la interacción entre individuos o recursos. Las redes sociales del conocimiento utilizan plataformas digitales de amplio acceso y facilidades de interacción, discusión, intercambio de ideas y acceso a recursos.

Riesgo de ciberseguridad: probabilidad de ocurrencia de un incidente de ciberseguridad y la magnitud de sus consecuencias, cuantificada en función de la probabilidad y del impacto sobre las personas, las instituciones, la economía o la seguridad nacional.

SEGUNDA. - El presente Reglamento 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, las Políticas de Protección de Datos Personales, el Código de Ética Institucional, de la Investigación y el Aprendizaje, el Reglamento General al Estatuto y demás normativa interna aplicable.

Las materias específicas de protección de datos personales, privacidad, seguridad de la información, ciberseguridad e inteligencia artificial se regirán por sus instrumentos especiales, sin perjuicio de la aplicación de las reglas del presente Reglamento en lo relativo a los flujos de información y comunicación institucional.

TERCERA. - El presente Reglamento tiene carácter obligatorio, orientado al perfeccionamiento y la mejora continua del flujo de información y comunicación de la Universidad Metropolitana

que incluye los espacios físicos y digitales y con ello su orientación a las autoridades, directivos, personal y estudiantes.

CUARTA. – Este Reglamento forma parte de las regulaciones del ecosistema institucional del aseguramiento de la calidad, de las regulaciones de la ética institucional, de la investigación y el aprendizaje; articulándose con toda la normativa interna que se relaciona con la gestión de información y comunicación, uso de las plataformas y sistemas tecnológicos digitales, privacidad y protección de datos personales, ciberseguridad, el Plan Estratégico de Desarrollo Institucional 2024 – 2034, la planificación operativa y el Plan de Mejoras Institucional.

QUINTA. – La seguridad de la información y la ciberseguridad son elementos transversales tratados en este Reglamento, en todo lo relacionado con el Sistema de Gestión Documental y de Archivos, el Sistema Institucional de Datos y Estadísticas, el Sistema Estructurado de Gestión del Aprendizaje Virtual y el Sistema Institucional de Protección de la Privacidad, la Información y los Datos Personales, aplicable a todas las sedes, unidades académicas y dependencias administrativas, que incluya, al menos políticas y procedimientos de clasificación, custodia, acceso y trazabilidad de la información, medidas técnicas y organizativas de seguridad, control de usuarios y credenciales, gestión de incidentes, y mecanismos de actualización y mejora continua, conforme la Ley Orgánica de Protección de Datos Personales, su Reglamento y normativa conexas, así como la Ley Orgánica para el Fortalecimiento de la Ciberseguridad. Y en consecuencia la normativa interna aplicable.

SEXTA. - Cuando por reforma estatutaria, reglamentaria, orgánica o funcional se modifique la denominación, integración, dependencia o adscripción de una autoridad, dirección, unidad, departamento, centro, comisión, cargo o responsable mencionado en el presente Reglamento, las referencias se entenderán efectuadas a la instancia que haga sus veces conforme a la normativa vigente, siempre que no se altere el contenido sustantivo de la competencia atribuida.

Las modificaciones materiales de competencias, procedimientos, responsabilidades o niveles de aprobación requerirán la correspondiente reforma o armonización normativa.

SÉPTIMA.- La información y comunicación institucional deberá realizarse a través de canales oficiales, plataformas autorizadas, cuentas institucionales, sistemas habilitados o medios expresamente aprobados por la autoridad competente.

El uso de canales personales, cuentas no institucionales, plataformas no autorizadas o aplicaciones externas para comunicar, cargar, descargar, transferir, publicar o custodiar información institucional solo procederá cuando exista autorización expresa, necesidad justificada y cumplimiento de las medidas de seguridad, confidencialidad y protección de datos personales aplicables.

La Universidad podrá restringir, suspender o retirar el uso de canales, plataformas o cuentas cuando se adviertan riesgos de seguridad, suplantación, pérdida de control, uso indebido, afectación reputacional, vulneración de datos personales o incumplimiento de la normativa interna.

OCTAVA.- Para la publicación, difusión, depósito, consulta o incorporación de trabajos de titulación, tesis, proyectos de titulación, artículos académicos, estudios de caso, exámenes complexivos documentados, informes de investigación o cualquier otro documento equivalente en repositorios institucionales, bibliotecas físicas o digitales, plataformas académicas, bases de datos o sistemas de consulta de acceso a la Comunidad Universitaria o al público en general, la Universidad Metropolitana observará la Ley Orgánica de Educación Superior, el Reglamento de Régimen Académico, la normativa de protección de datos personales, el Reglamento Interno de Régimen Académico, el Manual de Titulación de la Universidad y demás normativa interna aplicable.

Cuando el trabajo incluya anexos, instrumentos de investigación, matrices, encuestas, entrevistas, consentimientos informados, bases de datos, fotografías, capturas de pantalla o documentos de respaldo, estos deberán ser revisados previamente para eliminar, anonimizar, pseudonimizar o separar los datos personales que no sean necesarios para la versión publicable.

Los datos personales identificativos, sensibles, privados o innecesarios para la finalidad académica y pública del trabajo no deberán constar en el cuerpo del documento destinado a publicación. En particular, deberán excluirse números de cédula o pasaporte, direcciones domiciliarias, correos electrónicos personales, números telefónicos, firmas manuscritas, códigos personales de acceso, datos bancarios, certificados médicos, información de salud, datos biométricos, información socioeconómica, datos familiares, copias de documentos de identidad y cualquier otro dato personal del autor, tutor, miembros del tribunal, participantes en la investigación, informantes, encuestados, entrevistados o terceros que no resulte estrictamente necesario para la identificación académica del trabajo y su trazabilidad institucional.

Cuando por razones administrativas, académicas, de archivo, validación, registro o titulación sea necesario recabar alguno de estos datos, el estudiante deberá entregarlos en una hoja, formulario o anexo separado, destinado exclusivamente al expediente académico-administrativo correspondiente. Dicho documento no formará parte de la versión publicable del trabajo de titulación ni podrá ser incorporado al repositorio, biblioteca digital, plataforma pública o medio de difusión institucional.

La versión publicable del trabajo de titulación deberá contener únicamente los datos académicos necesarios, tales como nombres y apellidos del autor, carrera o programa, sede, modalidad, título del trabajo, nombre del tutor o director, fecha de aprobación y demás elementos exigidos por la normativa académica, siempre bajo criterios de minimización, pertinencia, proporcionalidad y finalidad.

Esta disposición se entenderá incorporada al Reglamento Interno de Régimen Académico, al Manual de Titulación de la Universidad Metropolitana y a los procedimientos internos de biblioteca, repositorio institucional, archivo académico y gestión documental, sin necesidad de reforma expresa inmediata, hasta que dichos instrumentos sean actualizados formalmente.

El Centro de Recursos para el Aprendizaje y la Investigación, CRAI, será responsable de implementar esta disposición en los procesos de recepción, revisión formal, carga, publicación, custodia y consulta de trabajos de titulación, en coordinación con las unidades académicas, la

Secretaría General Técnica, la Dirección de Tecnologías Informáticas, el Delegado de Protección de Datos Personales y las demás instancias competentes.

DISPOSICIONES TRANSITORIAS

PRIMERA. – En el plazo máximo de seis (6) meses contados desde la entrada en vigor del presente Reglamento, el Departamento de Talento Humano, en coordinación con la Procuraduría Nacional, elaborará y tramitará la reforma del Reglamento Interno de Trabajo de la Universidad Metropolitana, a fin de incorporar las infracciones a las disposiciones de este Reglamento. La reforma deberá establecer las consecuencias disciplinarias aplicables de acuerdo con la gravedad de la conducta, el daño causado, el riesgo generado, la intencionalidad, la reincidencia y la afectación institucional, incluida la posibilidad de solicitar el visto bueno cuando concurran las causales y presupuestos previstos en el Código del Trabajo, sin perjuicio de las responsabilidades civiles, administrativas o penales que correspondan.

SEGUNDA. - En el plazo máximo de seis (6) meses contados desde la entrada en vigor del presente Reglamento, la Dirección de Tecnologías de la Información, en coordinación con la Procuraduría Nacional, elaborará y tramitará la reforma del Reglamento que regula el Procedimiento Disciplinario para los Estudiantes, Profesores e Investigadores de la Universidad Metropolitana. Esta reforma deberá establecer consecuencias disciplinarias aplicables de acuerdo con la gravedad de la conducta, el daño causado, el riesgo generado, la intencionalidad, la reincidencia y la afectación institucional.

TERCERA. – En el plazo máximo de ciento veinte (120) días contados desde la entrada en vigor del presente Reglamento, el Departamento de Comunicación, Promoción, Relaciones Públicas y Atención al Estudiante presentará al Rectorado una propuesta de política, instructivo o manual operativo para la gestión de comunicación, promoción, relaciones públicas y atención al estudiante, con el objeto de desarrollar los procedimientos internos, flujos de aprobación, criterios editoriales, lineamientos de imagen institucional, administración de redes sociales, presencia web y comunicación interna y externa previstos en este Reglamento.

CUARTA. - A partir de la aprobación de este Reglamento, el director de Tecnologías Informáticas presentará los manuales de usuario o memorias descriptivas de las plataformas y aplicaciones informáticas relacionadas con los flujos de información y comunicación institucional descritos como procesos en este Reglamento de conformidad con los objetivos y plazos de revisión, evaluación, actualización, entregas e implementación del Plan Estratégico de la Transformación Digital y Audiovisual de la UMET.

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 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, 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, a los 31 días del mes de julio de 2026

Ing. Alejandro Rafael Socorro Castro, Ph.D.

RECTOR Y PRESIDENTE DEL CONSEJO ACADÉMICO SUPERIOR

En mi calidad de Secretario General Técnico, **CERTIFICO** que la presente Resolución fue aprobada por el Consejo Académico Superior de la Universidad Metropolitana, a los 31 días del mes de julio de 2026.

Abg. Augusto Andrés Cueva Gaibor, Mgs.

SECRETARIO GENERAL TÉCNICO

REGLAMENTO DEL FLUJO DE INFORMACION Y COMUNICACION DE LA
UNIVERSIDAD METROPOLITANA



Editorial
UMET