UNIVERSIDAD METROPOLITANA

REGLAMENTO PARA LA PROTECCIÓN DE LA PRIVACIDAD, DE LA INFORMACIÓN Y DE LOS DATOS PERSONALES DE LA UNIVERSIDAD METROPOLITANA

CONSEJO ACADÉMICO SUPERIOR

RESOLUCION No. 55-UMET-CAS-SO-07-2026

31 de julio de 2026

RESOLUCIÓN Nº. 55-UMET-CAS-SO-07-2026

EL CONSEJO ACADÉMICO SUPERIOR DE LA UNIVERSIDAD METROPOLITANA

Considerando

Que, el artículo 18 (2) de la Constitución reconoce a todas las personas, en forma individual o colectiva, el derecho a acceder libremente a la información generada en entidades públicas o en las privadas que manejen fondos del Estado o realicen funciones públicas y a buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa, salvo las excepciones de ley;

Que, el numeral 18 del artículo 66 de la Constitución reconoce el derecho al honor y al buen nombre, así como a la rectificación de la información que afecte tales derechos y los numerales 19, 20 y 21 reconocen los derechos a la protección de datos de carácter personal, a la intimidad personal y familiar y a la inviolabilidad y al secreto de la correspondencia física y virtual;

Que, los artículos 350 y 352 de la Constitución establecen que el sistema de educación superior tiene como finalidad la formación académica y profesional con visión científica y humanista y que las instituciones que lo integran ejercerán su autonomía responsable, con sujeción a los principios constitucionales y al ordenamiento jurídico vigente;

Que, el artículo 17 de la Ley Orgánica de Educación Superior reconoce el principio de autonomía responsable, en virtud del cual las instituciones de educación superior pueden expedir sus estatutos, reglamentos y normas internas, en armonía con la Constitución y la Ley;

Que, la Ley Orgánica de Protección de Datos Personales, su Reglamento General y la normativa secundaria emitida por la Superintendencia de Protección de Datos Personales constituyen el marco vinculante para todo tratamiento de datos personales realizado en territorio ecuatoriano y respecto de titulares ecuatorianos y reconocen al titular un derecho personalísimo, inherente, inalienable, indisponible e imprescriptible sobre sus datos personales;

Que, la Ley Orgánica para la Transformación Digital y Audiovisual y su Reglamento General reconocen los principios de seguridad digital, protección de la información, confidencialidad, ciberseguridad y gobernanza de las tecnologías de la información en los sectores público y privado, así como las funciones de los órganos rectores en estas materias;

Que, el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, el régimen ecuatoriano de propiedad intelectual y la normativa aplicable reconocen y protegen los secretos empresariales, la información comercial confidencial, los conocimientos tradicionales, los saberes ancestrales y la propiedad intelectual de las personas naturales, jurídicas y de las comunidades;

Que, la **Resolución Nº SPDP-SPD-2026-0009-R**, mediante la que se expide la Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial, **la Resolución Nº SPDP-SPD-2026-0005-R**, sobre Tratamiento de Datos Personales a Gran Escala y la Resolución Nº **SPDP-SPD-2026-0004-R**, de Transferencias o Comunicaciones Nacionales e Internacionales de Datos Personales, expedidas por la Superintendencia de Protección de Datos Personales, son de aplicación obligatoria a la Universidad Metropolitana en el desarrollo de sus actividades sustantivas y adjetivas;

Que, las normas técnicas internacionales constituyen referente metodológico de buenas prácticas para el diseño, implementación y mejora continua de los sistemas institucionales de seguridad de la información y protección de la privacidad; en particular, las normas ISO/IEC 27001:2022 sobre Sistemas de Gestión de Seguridad de la Información, ISO/IEC 27002:2022 sobre controles, ISO/IEC 27701:2019 sobre Sistema de Gestión de Información de Privacidad, ISO/IEC 27017 e ISO/IEC 27018 sobre seguridad y protección de datos personales en servicios en la nube, ISO/IEC 42001:2023 sobre Sistema de Gestión de Inteligencia Artificial, ISO/IEC 23894:2023 sobre gestión de riesgos en inteligencia artificial, ISO 31000:2018 sobre gestión de riesgos e ISO 22301 sobre continuidad del negocio;

Que, la Conferencia General de la UNESCO aprobó el 23 de noviembre de 2021 la Recomendación sobre la Ética de la Inteligencia Artificial, que consagra, entre otros, los principios del derecho a la intimidad y a la protección de datos, transparencia y explicabilidad, supervisión y decisión humanas y responsabilidad y rendición de cuentas, aplicables al ecosistema de tratamientos de información sustentados en tecnologías emergentes;

Que, el artículo 25 letras p) y q) del Estatuto Institucional faculta al Consejo Académico Superior para aprobar y reformar, en una sola discusión, los reglamentos internos de las funciones sustantivas de educación superior y los reglamentos y resoluciones normativas internas de los procesos de gobierno, funcionamiento, trabajo, estudiantes y demás procesos habilitantes de asesoría y apoyo, previo informe favorable del Consejo de Regentes;

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

Que, el Reglamento General al Estatuto de la Universidad Metropolitana, aprobado mediante **Resolución Nº 17-UMET-CAS-SE-03-2026**, reconoce expresamente las figuras del Responsable del Tratamiento y del Delegado de Protección de Datos Personales y dispone que, para fines de organización y gestión interna, el Vicerrector Administrativo actuará como Responsable interno del Tratamiento de datos personales de la Universidad Metropolitana;

Que, mediante **Resolución Nº 81-UMET-CAS-SO-09-2025** el Consejo Académico Superior aprobó las Políticas de Protección de Datos Personales de la Universidad Metropolitana, las cuales reconocen a la institución como responsable del tratamiento de datos personales frente a los titulares, la sociedad y el Estado y contemplan expresamente el tratamiento de datos sensibles, biométricos, de menores de edad, decisiones automatizadas, elaboración de perfiles, videovigilancia y transferencias nacionales e internacionales de datos personales;

Que, mediante **Resolución Nº 57-UMET-CAS-SO-07-2025** el Consejo Académico Superior expidió el Código de Ética Institucional, de la Investigación y el Aprendizaje, el cual contempla, entre los valores y deberes éticos de la Comunidad Universitaria, la integridad intelectual, la confidencialidad, la protección de datos personales, el respeto a la propiedad intelectual y la honestidad académica;

Que, la información que la Universidad Metropolitana genera, custodia, procesa, comunica, transfiere, conserva y elimina, así como los datos personales y la información sensible, delicada, comercial confidencial, académica, investigativa y administrativa que se manejan en el desarrollo de sus funciones, constituyen activos institucionales que requieren protección integral, sistemática y demostrable, mediante un marco normativo, organizativo, técnico y cultural específico;

Que, resulta institucionalmente necesario consagrar de manera categórica que el deber de protección de los datos personales que pesa sobre las autoridades, el personal académico, técnico docente, administrativo, los estudiantes y los demás integrantes de la Comunidad Universitaria, así como sobre los proveedores y colaboradores externos, es un deber permanente, indelegable, intransferible y exigible a perpetuidad, sin sujeción a plazo, condición, prescripción ni caducidad, atendiendo al carácter personalísimo e inherente del derecho a la protección de datos personales;

Que, se requiere establecer un Sistema Institucional unificado de Protección de la Privacidad, la Información y los Datos Personales, que articule de modo coherente las dimensiones jurídicas, éticas, técnicas, organizativas y de cultura institucional, en armonía con los estándares técnicos internacionales aplicables;

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

Que, mediante Resolución No. CR-UMET-00139-07-2026, de 24 de julio de 2026, el Consejo de Regentes emitió informe favorable sobre el proyecto y autorizó su remisión al Consejo Académico Superior para conocimiento y aprobación;

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

REGLAMENTO PARA LA PROTECCIÓN DE LA PRIVACIDAD, DE LA INFORMACIÓN Y DE LOS DATOS PERSONALES DE LA UNIVERSIDAD METROPOLITANA

TÍTULO I

DISPOSICIONES PRELIMINARES

Capítulo I

Objeto, ámbito y finalidad

Artículo 1.- Objeto. El presente Reglamento tiene por objeto establecer los principios, deberes, prohibiciones, mecanismos institucionales, controles y procedimientos aplicables a la protección de la privacidad, de la información en general —incluida la información sensible, delicada, reservada, académica, investigativa, administrativa y de cualquier otra índole— y de los datos personales que la Universidad Metropolitana genera, recibe, custodia, trata, comunica, conserva, transfiere o elimina en el desarrollo de sus actividades sustantivas y adjetivas, así como crear el Sistema Institucional de Protección de la Privacidad, la Información y los Datos Personales (SIPPID) y articularlo con el régimen aplicable al uso ético, responsable y seguro de la inteligencia artificial.

Artículo 2.- Naturaleza y función integradora. El presente Reglamento es un reglamento institucional de carácter general, transversal e integrador, sujeto al mismo régimen de aprobación, validez, aplicación y control que los demás reglamentos de la Universidad Metropolitana. Sus disposiciones constituyen la base normativa común de la institución en materia de protección de la privacidad, de la información y de los datos personales, y operan como instrumento general de gobernanza institucional de la información, del cual se articulan, mediante técnicas de remisión, complementariedad, especialidad y no contradicción, los instrumentos específicos que regulan dimensiones particulares de la misma materia, entre ellos el Reglamento para el Uso Ético, Responsable y Seguro de la Inteligencia Artificial, las Políticas de Protección de Datos

Personales, el Reglamento Interno del Sistema de Gestión Documental y Archivos y demás normativa interna de la Universidad Metropolitana.

La Política de Protección de Datos Personales aprobada por el Consejo de Regentes y el Consejo Académico Superior constituye el instrumento rector específico en materia de tratamiento de datos personales. El presente Reglamento se aplicará de manera complementaria, armónica y sin sustitución del Código de Ética Institucional, de la Investigación y el Aprendizaje, de dichas Políticas, del Reglamento sobre Inteligencia Artificial, del Reglamento Interno de Trabajo, del Reglamento que regula el Procedimiento Disciplinario para los Estudiantes, Profesores e Investigadores y de los demás reglamentos internos.

Artículo 3.- Ámbito material. Las disposiciones de este Reglamento son de cumplimiento obligatorio respecto de toda información institucional —en cualquier soporte y formato, físico, digital, audiovisual, electrónico o de cualquier otra naturaleza— y de todo tratamiento de datos personales que la Universidad Metropolitana realice por sí o por intermedio de terceros, incluidos los flujos hacia y desde proveedores, contratistas, aliados, instituciones de educación superior nacionales o extranjeras, organismos del Estado y demás partes relacionadas.

Artículo 4.- Ámbito subjetivo. Este Reglamento se aplica, sin distinción de jerarquía, función, sede o modalidad de vinculación, a todas las personas que integran la Comunidad Universitaria de la Universidad Metropolitana, comprendiendo, en particular:

a) Las Primeras Autoridades, las autoridades académicas y administrativas, los directivos académicos y administrativos, los miembros del Consejo Académico Superior y del Consejo de Regentes, los promotores institucionales y demás autoridades;

b) El personal académico, en sus distintas categorías, dedicaciones, escalafones y modalidades, incluidos los investigadores y el personal técnico docente;

c) El personal administrativo, sin distinción del régimen jurídico de su vinculación;

d) Los estudiantes de las carreras técnico-tecnológicas, de grado, de posgrado y de educación continua, en cualquier modalidad, así como los estudiantes en movilidad académica;

e) Los aspirantes, postulantes, pasantes, practicantes, becarios, asistentes de investigación, investigadores invitados y colaboradores en proyectos institucionales;

f) Las personas naturales o jurídicas, nacionales o extranjeras, que en virtud de convenios, contratos, alianzas o relaciones de cooperación con la Universidad

Metropolitana intervengan en el tratamiento de información o datos personales vinculados a la actividad institucional; y,

g) Toda persona que, sin estar comprendida en los literales anteriores, acceda, trate o conozca información institucional o datos personales en el marco de actividades auspiciadas, financiadas, autorizadas o reconocidas por la Universidad Metropolitana.

Artículo 5.- Ámbito territorial y temporal. 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, durante todo el tiempo en que subsista el vínculo institucional y, respecto de los deberes de confidencialidad y de protección de datos personales, también con posterioridad a su terminación, conforme a las disposiciones de este Reglamento.

Artículo 6.- Finalidades. Son finalidades del presente Reglamento:

a) Garantizar la protección integral, sistemática y demostrable de la privacidad, de la información institucional y de los datos personales que se tratan en la Universidad Metropolitana;

b) Establecer un Sistema Institucional unificado de Protección de la Privacidad, la Información y los Datos Personales, articulado con el régimen aplicable al uso ético, responsable y seguro de la inteligencia artificial;

c) Asegurar el cumplimiento del régimen ecuatoriano de protección de datos personales, de seguridad de la información y de las normas relacionadas con secreto profesional, propiedad intelectual y reserva legal;

d) Adoptar como referente metodológico las normas técnicas internacionales aplicables, en particular las de la familia ISO/IEC;

e) Consagrar el carácter permanente y perpetuo del deber de protección de los datos personales y de la información sensible y delicada, sin sujeción a plazo, condición ni caducidad;

f) Promover una cultura institucional de privacidad, protección de la información, integridad académica, seguridad y uso ético de las tecnologías; y,

g) Establecer mecanismos de supervisión, auditoría, certificación, mejora continua, transparencia, rendición de cuentas y responsabilidad proactiva.

Artículo 7.- Jerarquía normativa e interpretación. Las disposiciones del presente Reglamento se interpretarán y aplicarán en consonancia con la Constitución, los

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

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 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.

Artículo 8.- Articulación con el Reglamento sobre Inteligencia Artificial. Este Reglamento se aplicará de manera articulada con el Reglamento para el Uso Ético, Responsable y Seguro de la Inteligencia Artificial de la Universidad Metropolitana. Las cuestiones específicas relativas a sistemas de inteligencia artificial se regirán por dicho instrumento, sin perjuicio de la aplicación general del presente Reglamento. La gobernanza de ambos cuerpos normativos quedará unificada en el Comité y el Sistema Institucional regulados en este Reglamento.

Capítulo II

Principios rectores

Artículo 9.- Principios rectores. El tratamiento de la información, la protección de la privacidad y la gestión de los datos personales en la Universidad Metropolitana se rigen por los siguientes principios:

a) Dignidad humana y derechos fundamentales: todo tratamiento de información y de datos personales se ordenará al respeto de la dignidad humana, la intimidad, el honor, el buen nombre, la libre autodeterminación informativa y los demás derechos fundamentales reconocidos por la Constitución y los instrumentos internacionales de derechos humanos;

b) Legalidad y legitimidad: todo tratamiento se sustentará en una base jurídica válida, conforme al ordenamiento ecuatoriano y a la normativa interna de la Universidad;

c) Lealtad, transparencia y buena fe: la información se tratará con lealtad, claridad y previa información al titular, sin engaño, ni reserva indebida;

d) Finalidad determinada y vinculada: la información se tratará para fines determinados, explícitos, legítimos e institucionalmente justificados y no se utilizará de modo incompatible con tales fines;

e) Minimización: se tratará únicamente la información estrictamente necesaria, adecuada y pertinente para los fines perseguidos;

f) Calidad y exactitud: la información se mantendrá completa, actualizada, exacta y veraz y se rectificará o suprimirá oportunamente cuando corresponda;

g) Conservación limitada y deber de eliminación: la información se conservará por el tiempo estrictamente necesario para los fines del tratamiento o por el que exija la normativa aplicable y será eliminada o anonimizada al término del plazo correspondiente, salvo deberes legales de conservación;

h) Confidencialidad y reserva: toda información tratada por la Universidad Metropolitana se sujetará al deber de reserva conforme a su clasificación y a las obligaciones legales, contractuales o éticas aplicables;

i) Integridad y disponibilidad: se garantizará que la información permanezca íntegra, exacta y accesible para los fines y a las personas autorizadas, en el momento y forma en que se requiera;

j) Seguridad y resiliencia: los activos de información se protegerán mediante medidas técnicas, organizativas, físicas y jurídicas proporcionales al riesgo, capaces de asegurar su confidencialidad, integridad, disponibilidad, autenticidad, no repudio, trazabilidad y resiliencia;

k) Privacidad desde el diseño y por defecto: los procesos, sistemas, plataformas y prácticas institucionales incorporarán, desde su concepción y por defecto, las medidas de protección de la información y de los datos personales;

l) Enfoque basado en riesgos: las obligaciones aplicables y las medidas de control serán proporcionales al nivel de riesgo identificado para los derechos, libertades, intereses y bienes jurídicos protegidos;

m) Responsabilidad proactiva y demostrada: la Universidad y los integrantes de la Comunidad Universitaria deberán cumplir las obligaciones aplicables y demostrarlo mediante evidencia verificable;

n) Mejora continua y estandarización internacional: el Sistema Institucional se diseñará, implementará, evaluará y perfeccionará atendiendo a las normas técnicas internacionales aplicables, en particular las de la familia ISO/IEC;

o) Interés superior del niño y de la adolescencia: todo tratamiento que involucre a niños o adolescentes observará, de manera reforzada, su interés superior;

p) No discriminación e inclusión: el tratamiento de información y de datos personales no podrá ser instrumento de discriminación por razón de origen étnico, género, identidad de género, orientación sexual, discapacidad, edad, nacionalidad, condición socioeconómica, convicciones religiosas, filiación política o cualquier otra condición protegida;

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

q) Protección perpetua de los datos personales: el deber de protección de los datos personales es permanente, indelegable, intransferible y exigible a perpetuidad, sin sujeción a plazo, condición o suspensión, conforme al Título II del presente Reglamento; y,

r) Cooperación, diálogo de saberes e interculturalidad: la protección de la información respetará la diversidad cultural, epistémica y lingüística y se ejercerá con especial cuidado respecto de los conocimientos colectivos, los saberes ancestrales y la propiedad intelectual de pueblos y comunidades.

TÍTULO II

DEBER GENERAL DE PROTECCIÓN Y RÉGIMEN DE PERPETUIDAD

Artículo 10.- Deber general de protección. Toda persona integrante de la Comunidad Universitaria, así como toda persona natural o jurídica vinculada a la Universidad Metropolitana por cualquier relación académica, laboral, contractual, civil, mercantil, de cooperación o de colaboración, está obligada a proteger la privacidad, la información y los datos personales a los que tenga acceso, conozca o trate en razón de tal vínculo, en los términos del presente Reglamento, la normativa interna y el ordenamiento jurídico aplicable.

Artículo 11.- Deber de protección perpetua de los datos personales. Los datos personales son inherentes a la persona del titular y forman parte de su esfera de autonomía, identidad y dignidad. En consecuencia, el deber de protección, custodia, reserva, confidencialidad y no divulgación de los datos personales de los estudiantes, aspirantes, postulantes, graduados, profesores, investigadores, personal académico, técnico docente, administrativo, autoridades, miembros de los órganos colegiados, promotores institucionales, proveedores, contratistas, clientes, aliados, visitantes y demás terceros vinculados a la Universidad Metropolitana, que pesa sobre las autoridades, el personal en sus distintas categorías, los estudiantes y los demás integrantes de la Comunidad Universitaria, así como sobre los proveedores y colaboradores externos, es un deber permanente, indelegable, intransferible y exigible a perpetuidad, sin sujeción a plazo, condición o suspensión alguna.

Este deber subsiste íntegramente con posterioridad a la terminación, por cualquier causa, del vínculo académico, laboral, contractual, de cooperación o de colaboración con la Universidad Metropolitana y no se extingue por jubilación, renuncia, separación, expulsión, conclusión de estudios, finalización del contrato ni por ninguna otra circunstancia.

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

Artículo 12.- Alcance del deber perpetuo. El deber establecido en el artículo precedente comprende, sin limitación, las obligaciones de:

a) No revelar, divulgar, comunicar, transferir, publicar, compartir o de cualquier otra forma poner a disposición de terceros no autorizados los datos personales conocidos en virtud del vínculo institucional;

b) No utilizar los datos personales para fines distintos de aquellos para los que fueron recolectados o tratados institucionalmente;

c) No conservar copias, extractos, reproducciones, respaldos, transcripciones o derivaciones de datos personales fuera de los entornos institucionales autorizados ni con posterioridad al cese del vínculo;

d) Devolver, eliminar o destruir, conforme a las directrices institucionales, los soportes físicos o digitales que contengan datos personales al término del vínculo o cuando así se le requiera;

e) Cumplir las medidas técnicas, organizativas, físicas y jurídicas que la Universidad disponga para la protección de los datos personales;

f) Reportar de inmediato cualquier vulneración, riesgo, incidente, sospecha o circunstancia que pueda afectar la protección de los datos personales; y,

g) Cooperar con la Universidad y con la autoridad de control en la atención de los derechos de los titulares y en la gestión de incidentes.

Artículo 13.- Carácter no contractual y consecuencias. El deber perpetuo de protección de los datos personales es un deber de carácter personalísimo, que no requiere pacto contractual expreso para su exigibilidad, sin perjuicio de la incorporación de cláusulas específicas en contratos, convenios, acuerdos y compromisos institucionales.

La Universidad Metropolitana podrá exigir, en sede administrativa, civil, penal o constitucional según corresponda, las acciones, indemnizaciones, sanciones y medidas conducentes ante el incumplimiento de este deber, sin perjuicio de las acciones que pertenezcan al propio titular conforme a la Ley Orgánica de Protección de Datos Personales y demás normativa aplicable.

Artículo 14.- Cláusulas de confidencialidad reforzada. Sin perjuicio del carácter no contractual del deber perpetuo, la Universidad Metropolitana incluirá en los contratos laborales, contratos de servicios profesionales, convenios, acuerdos de pasantía, contratos con proveedores y demás instrumentos jurídicos, cláusulas expresas de confidencialidad, protección de datos personales y deber perpetuo de reserva, en términos compatibles con este Reglamento. La ausencia de tales cláusulas no afectará la exigibilidad del deber, conforme al artículo precedente.

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

TÍTULO III

CLASIFICACIÓN DE LA INFORMACIÓN INSTITUCIONAL

Capítulo I

Reglas generales

Artículo 15.- Clasificación de la información. La Universidad Metropolitana clasificará la información que genera, recibe, custodia o trata según su sensibilidad, valor, riesgo y nivel de confidencialidad, en las siguientes categorías:

a) Pública: aquella cuya divulgación sea obligatoria conforme al ordenamiento jurídico, haya sido expresamente autorizada por la Universidad o no se encuentre sujeta a restricciones de acceso;

b) Información de acceso limitado o uso interno: aquella destinada al funcionamiento ordinario de la Universidad, cuyo acceso se encuentre restringido a las autoridades, unidades, servidores, trabajadores, estudiantes o terceros que la requieran para el cumplimiento de sus funciones, actividades o responsabilidades;

c) Reservada: aquella cuya divulgación, comunicación o acceso no autorizado pueda afectar derechos de las personas, obligaciones contractuales, investigaciones, procesos académicos, administrativos o disciplinarios, intereses institucionales legítimos o el normal funcionamiento de la Universidad; y,

d) Información estrictamente confidencial: aquella cuya divulgación, pérdida, alteración, acceso o uso no autorizado pueda producir una afectación grave a los derechos fundamentales, la seguridad de las personas, la continuidad institucional, el patrimonio, la estrategia, las investigaciones, la defensa jurídica, la infraestructura tecnológica o los intereses esenciales de la Universidad.

La clasificación deberá responder a criterios de necesidad, proporcionalidad, finalidad, riesgo y temporalidad y no podrá utilizarse para restringir injustificadamente el acceso a información pública ni para impedir el cumplimiento de obligaciones legales de transparencia, rendición de cuentas o control.

Artículo 16.- Inventario de activos de información. La Dirección de Tecnologías Informáticas, en coordinación con el Comité Institucional de Protección de la Privacidad, la Información, los Datos Personales y de Uso Ético de la Inteligencia Artificial (el CIPPIA) y con las unidades académicas y administrativas, mantendrá un Inventario de Activos de Información, en el que se registre, al menos, la denominación, custodio, ubicación, formato, clasificación, base jurídica de tratamiento, plazos de conservación, medidas de protección aplicables y demás información relevante.

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

Con independencia de su nivel de acceso, la información institucional podrá ser identificada, según su naturaleza, como:

a) Datos personales;
b) Datos personales sensibles;
c) Información académica;
d) Información investigativa;
e) Información administrativa
f) Información financiera o contable;
g) Información jurídica o contractual;
h) Información disciplinaria;
i) Información técnica o tecnológica;
j) Información comercial o estratégica;
k) Información de seguridad;
l) Información protegida por propiedad intelectual, secreto profesional, secreto empresarial o deber legal de reserva; y,
m) Cualquier otra categoría que, por su naturaleza, finalidad, riesgo o valor institucional, requiera tratamiento diferenciado.

La naturaleza de la información no determinará por sí sola su nivel de acceso. Una misma categoría podrá ser pública, de acceso limitado, confidencial o estrictamente confidencial, según el contexto, la finalidad, la normativa aplicable y el riesgo asociado a su divulgación.

Artículo 17.- Custodios y responsables operativos. Cada activo de información tendrá un custodio funcional —autoridad o unidad responsable de su tratamiento— y un responsable operativo —persona designada para su gestión cotidiana—, quienes responderán por el cumplimiento de las medidas de protección aplicables, sin perjuicio de la responsabilidad indelegable de la Universidad como persona jurídica.

Capítulo II

Información sensible y delicada

Artículo 18.- Información sensible. Se considera información sensible, a efectos de este Reglamento, además de los datos personales sensibles definidos por la Ley Orgánica de Protección de Datos Personales, la información sobre salud y salud mental; la información sobre violencia de género, acoso o abuso; la información disciplinaria de estudiantes, profesores, investigadores y personal administrativo; las evaluaciones académicas o laborales no comunicadas; las investigaciones en curso; los expedientes de procesos electorales internos; las denuncias y los procesos sancionadores; y, la información sobre menores de edad.

Artículo 19.- Información delicada. Se considera información delicada aquella cuya revelación, alteración o pérdida puede causar afectación significativa, sin alcanzar la categoría de sensible, tales como información sobre conflictos institucionales en curso; comunicaciones internas no destinadas a difusión externa; información sobre procesos de admisión, becas y ayudas económicas; información financiera personal; antecedentes laborales detallados; opiniones, reportes o evaluaciones aún no validadas; e información sobre auditorías internas no concluidas.

Artículo 20.- Tratamiento reforzado. La información sensible y delicada estará sometida a medidas reforzadas de protección, que comprenderán, según corresponda, limitación del acceso por necesidad de conocer; cifrado en tránsito y en reposo; segregación de ambientes; control y registro de accesos; supervisión humana significativa de su tratamiento; y atención reforzada al deber de reserva profesional. Su comunicación a terceros requerirá base jurídica explícita y autorización del custodio funcional.

Capítulo III

Información reservada, estratégica y de acceso limitado

Artículo 21.- Información estratégica institucional. Se considera información estratégica institucional aquella cuyo conocimiento, divulgación o acceso anticipado pueda afectar la toma de decisiones, la posición jurídica, financiera, académica, tecnológica, investigativa o competitiva de la Universidad Metropolitana. Comprende, entre otros, los borradores de planes estratégicos, escenarios financieros, presupuestos no aprobados, proyecciones, negociaciones contractuales en curso, proyectos de inversión en etapa preparatoria, estudios preliminares para la creación de carreras o programas, diseños curriculares en elaboración, estrategias de admisión y posicionamiento aún no publicadas, matrices de riesgo, diagnósticos internos de vulnerabilidad tecnológica, información técnica de seguridad, configuraciones y arquitectura de sistemas, metodologías institucionales propias, información académica o investigativa no publicada y aquella protegida por cláusulas de confidencialidad propias o de terceros.

La reserva se aplicará únicamente mientras subsistan las razones que la justifican y no comprenderá los instrumentos institucionales aprobados que, conforme a la Constitución, la Ley Orgánica de Educación Superior y la normativa del Sistema de Educación Superior, deban ser objeto de publicidad, transparencia o rendición de cuentas. En consecuencia, el Plan Estratégico de Desarrollo Institucional, los Planes Operativos Anuales, los presupuestos aprobados, la oferta académica autorizada, los aranceles vigentes, las resoluciones institucionales y los informes de rendición de cuentas serán difundidos en los términos y con las limitaciones previstas en el ordenamiento jurídico,

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

sin perjuicio de proteger los datos personales, secretos empresariales, información de seguridad y demás contenidos sujetos a reserva legal.

Artículo 22.- Deber de reserva. Las autoridades, el personal académico, técnico docente, el personal de los procesos habilitantes de asesoría y apoyo y los demás integrantes de la Comunidad Universitaria que, en virtud de su función, tengan acceso a información reservada, estratégica o de acceso limitado de la Universidad o de terceros, observarán los deberes de reserva, no divulgación y no aprovechamiento, los cuales subsistirán durante todo el vínculo y luego de su terminación, sin perjuicio del régimen de protección perpetua aplicable a los datos personales.

Artículo 23.- Información de terceros. La información reservada o de acceso limitado entregada a la Universidad Metropolitana por proveedores, contratistas, aliados o entidades vinculadas, así como la información derivada de convenios, acuerdos de cooperación, dictámenes en proceso o asesorías, se tratará con el mismo estándar de reserva aplicable a la información reservada y estratégica institucional propia y conforme a los términos del instrumento jurídico que la genere.

Capítulo IV

Información académica e investigativa

Artículo 24.- Información académica. La información académica de los estudiantes —incluida la relacionada con admisión, matrícula, calificaciones, evaluaciones, asistencia, sanciones, becas, ayudas económicas, expediente disciplinario, salud y bienestar, prácticas, titulación, expediente psicopedagógico y demás registros académicos— se tratará con estricta confidencialidad y conforme a los principios y deberes establecidos en este Reglamento, en la Ley Orgánica de Protección de Datos Personales y en el régimen interno de la Universidad.

Artículo 25.- Información investigativa. La información generada en proyectos de investigación, incluida la información sobre sujetos de investigación, datos de campo, resultados preliminares, manuscritos, prototipos, hallazgos, instrumentos no publicados, propiedad intelectual asociada, datos de comunidades, conocimientos colectivos y saberes ancestrales, se sujetará a las medidas de protección previstas en este Reglamento, en el Código de Ética Institucional, de la Investigación y el Aprendizaje, en el Reglamento de Investigación e Innovación, en los protocolos de los Comités de Ética y en la demás normativa interna aplicable.

Artículo 26.- Confidencialidad académica. Los profesores, investigadores, personal técnico docente, evaluadores, tutores, jurados, miembros de comités y demás personas que, en el ejercicio de funciones académicas o investigativas, tengan acceso a

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

información académica o investigativa de estudiantes o terceros, observarán el deber de confidencialidad de manera reforzada, con sujeción a las normas de ética profesional, a la propiedad intelectual y al deber perpetuo de protección de los datos personales.

TÍTULO IV

PROTECCIÓN DE DATOS PERSONALES

Capítulo I

Marco aplicable y calidad institucional

Artículo 27.- Marco normativo aplicable. Todo tratamiento de datos personales realizado por la Universidad Metropolitana se sujetará íntegramente a la Constitución, a la Ley Orgánica de Protección de Datos Personales y su Reglamento General, a la normativa secundaria expedida por la Superintendencia de Protección de Datos Personales, a las Políticas de Protección de Datos Personales de la Universidad y al presente Reglamento. En el caso de tratamientos efectuados mediante sistemas de inteligencia artificial, se aplicará adicionalmente el Reglamento sobre Inteligencia Artificial y la Norma General SPDP-SPD-2026-0009-R, sus modificaciones, reformas o sustituciones.

Artículo 28.- Calidad institucional y responsabilidad. Frente a los titulares, la sociedad y el Estado, la responsable del tratamiento es la Universidad Metropolitana en su calidad de persona jurídica. Para fines de organización y gestión interna, el Vicerrector Administrativo actuará como autoridad responsable interna del Tratamiento de Datos Personales, sin perjuicio de las atribuciones del Rector como máxima autoridad ejecutiva. Cuando, conforme a las funciones desempeñadas, una persona, unidad o proveedor actúe como encargado del tratamiento, se aplicarán las disposiciones legales y reglamentarias correspondientes a esa figura.

Artículo 29.- Determinación del tratamiento a gran escala. La Universidad determinará la existencia de tratamientos de datos personales a gran escala respecto de actividades específicas de tratamiento, conforme a los criterios previstos en la Resolución Nº SPDP-SPD-2026-0005-R, sus reformas y normas sustitutivas, de ser el caso, y demás normativa aplicable.

Cuando, como resultado del análisis técnico-jurídico correspondiente, una actividad específica de tratamiento sea calificada como tratamiento a gran escala, se activarán las obligaciones reforzadas que correspondan, incluyendo la evaluación de impacto, medidas adicionales de seguridad, documentación del análisis, registro del tratamiento y controles de supervisión institucional.

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

Capítulo II

Bases jurídicas y derechos de los titulares

Artículo 30.- Bases jurídicas del tratamiento. Todo tratamiento de datos personales que la Universidad Metropolitana realice se sustentará en una base jurídica válida conforme a la Ley Orgánica de Protección de Datos Personales y su Reglamento, entre ellas el cumplimiento de obligaciones legales o regulatorias aplicables a la educación superior, la ejecución de relaciones contractuales, académicas o laborales, el interés legítimo, el cumplimiento de fines públicos en el marco del sistema de educación superior, la satisfacción de intereses vitales o el consentimiento libre, informado, específico e inequívoco del titular, según corresponda.

Artículo 31.- Datos sensibles y categorías especiales. El tratamiento de datos personales sensibles requerirá habilitación legal expresa o consentimiento explícito del titular, en los términos de la Ley Orgánica de Protección de Datos Personales y observará medidas reforzadas de protección, segregación, control de accesos y registro. Los datos biométricos, los datos de salud, los datos de menores de edad, los datos relativos a violencia o acoso y los datos relativos a procesos disciplinarios serán tratados con estándar reforzado.

Artículo 32.- Derechos de los titulares. La Universidad Metropolitana garantizará, mediante procedimientos institucionales accesibles, oportunos y gratuitos, el ejercicio efectivo de los derechos de los titulares previstos en la Ley Orgánica de Protección de Datos Personales, en particular, los derechos de información, acceso, rectificación, eliminación, oposición, suspensión del tratamiento, portabilidad, no ser objeto de decisiones basadas única o parcialmente en valoraciones automatizadas y la consulta del Registro Nacional de Protección de Datos Personales.

Artículo 33.- Procedimientos de atención. El Vicerrectorado Administrativo, en calidad de responsable interno del tratamiento de datos personales, organizará y garantizará la atención oportuna de las solicitudes presentadas por los titulares para el ejercicio de sus derechos.

La recepción, registro, tramitación, obtención de información, preparación de respuestas y ejecución de las medidas que correspondan estarán a cargo de las unidades académicas, administrativas, tecnológicas o documentales competentes, según la naturaleza de la solicitud y conforme al procedimiento institucional aplicable.

El Delegado de Protección de Datos Personales asesorará y supervisará el procedimiento, verificará el cumplimiento de los plazos y requisitos legales, emitirá alertas y recomendaciones técnicas y podrá requerir información a las unidades

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

competentes. El Delegado no sustituirá al responsable del tratamiento, no decidirá sobre la procedencia de la solicitud ni ejecutará directamente las medidas derivadas de ella.

Las solicitudes, actuaciones, respuestas, plazos y evidencias de cumplimiento deberán conservarse en un registro institucional trazable, administrado por la unidad competente.

Capítulo III

Encargados, transferencias y servicios en la nube

Artículo 34.- Encargados del tratamiento. Cuando un proveedor, contratista, aliado o tercero actúe como encargado del tratamiento, el contrato o instrumento equivalente deberá contener cláusulas expresas de protección de datos personales, conforme a la Ley Orgánica de Protección de Datos Personales y a su Reglamento General, incluyendo finalidades, instrucciones, medidas de seguridad, confidencialidad, subcontratación, atención de derechos de titulares, notificación de incidentes, auditoría y régimen de responsabilidad. El cumplimiento se verificará periódicamente.

Artículo 35.- Transferencias y comunicaciones. Las transferencias y comunicaciones nacionales e internacionales de datos personales se sujetarán a lo dispuesto en la normativa aplicable e incluirán la documentación, garantías adecuadas, instrumentos contractuales y evaluaciones de riesgos correspondientes.

Las transferencias se registrarán en el Registro de Actividades de Tratamiento.

Artículo 36.- Servicios en la nube. La contratación y uso de servicios en la nube que impliquen tratamiento de datos personales o de información institucional confidencial o sensible se ejecutará observando, además de la normativa aplicable, los lineamientos técnicos derivados de las normas ISO/IEC y se incorporará en los contratos respectivos cláusulas sobre ubicación de los datos, condiciones de procesamiento, subencargados, terminación, devolución y eliminación de datos al término del contrato.

Artículo 37.- Registro de Actividades de Tratamiento e inscripción en el Registro Nacional. La Universidad Metropolitana mantendrá actualizado su Registro de Actividades de Tratamiento, en el que se documentarán los tratamientos de datos personales realizados por las unidades académicas, administrativas y demás áreas institucionales, conforme a la Ley Orgánica de Protección de Datos Personales, su Reglamento General, la normativa secundaria aplicable y la Política de Protección de Datos Personales de la Universidad.

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

Las unidades tratantes y los custodios funcionales deberán proporcionar y actualizar la información correspondiente a los tratamientos bajo su responsabilidad. El Vicerrectorado Administrativo consolidará y supervisará el Registro de Actividades de Tratamiento, con la asesoría y supervisión del Delegado de Protección de Datos Personales.

La inscripción de tratamientos, bases de datos, responsables, encargados o demás información en el Registro Nacional de Protección de Datos Personales se efectuará únicamente cuando corresponda y en los términos exigidos por la Ley, su Reglamento General y la normativa secundaria expedida por la Superintendencia de Protección de Datos Personales. La inclusión de una actividad en el Registro de Actividades de Tratamiento institucional no implicará, por sí sola, la obligación automática de inscribirla en el Registro Nacional.

La Universidad conservará evidencia verificable de la evaluación realizada para determinar la procedencia o improcedencia de la inscripción y actualizará la información registrada cuando se produzcan cambios sustanciales en el tratamiento, en sus finalidades, categorías de datos, destinatarios, transferencias, medidas de seguridad o nivel de riesgo.

Artículo 38.- Gestión de riesgos y Evaluación de Impacto del Tratamiento. Antes de implementar tratamientos de datos personales que, por su naturaleza, alcance, contexto, finalidad, tecnología utilizada o efectos previsibles, puedan generar un alto riesgo para los derechos y libertades de los titulares, la Universidad Metropolitana deberá realizar una gestión previa de riesgos y, cuando corresponda conforme a la Ley Orgánica de Protección de Datos Personales, su Reglamento General y la normativa secundaria aplicable, una Evaluación de Impacto del Tratamiento.

La sola utilización de datos personales sensibles, datos de niños o adolescentes, sistemas de inteligencia artificial, videovigilancia, biometría, elaboración de perfiles, decisiones automatizadas, tratamientos a gran escala o tecnologías emergentes no determinará, por sí misma y de forma automática, la obligación de efectuar una Evaluación de Impacto. No obstante, estos elementos deberán considerarse como factores relevantes para determinar el nivel de riesgo, especialmente cuando concurran varios de ellos o cuando el tratamiento pueda producir efectos jurídicos, académicos, laborales, económicos o significativos sobre los titulares.

La evaluación deberá considerar, al menos:

a) La naturaleza, categorías, volumen y procedencia de los datos personales tratados;

b) Las finalidades, bases jurídicas y medios del tratamiento;

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

c) El número y condición de los titulares afectados, incluidos grupos en situación de vulnerabilidad;

d) La existencia de decisiones automatizadas, elaboración de perfiles, monitoreo sistemático o tratamiento a gran escala;

e) Los riesgos de acceso no autorizado, pérdida, alteración, discriminación, suplantación, exposición o uso incompatible de los datos;

f) La necesidad, idoneidad y proporcionalidad del tratamiento;

g) Las medidas técnicas, organizativas, jurídicas y de seguridad previstas; y

h) El riesgo residual luego de aplicadas las medidas de mitigación.

El área requirente será responsable de iniciar y documentar la evaluación, con el apoyo técnico de la Dirección de Tecnologías Informáticas y de las unidades tratantes. El Delegado de Protección de Datos Personales asesorará y supervisará el proceso y emitirá las recomendaciones que correspondan, sin asumir la ejecución operativa ni la decisión final. La aprobación de la Evaluación de Impacto corresponderá al Vicerrectorado Administrativo, en calidad de responsable interno del tratamiento.

Cuando la evaluación determine que subsiste un riesgo alto que no pueda ser razonablemente mitigado, el tratamiento no podrá iniciarse o continuar hasta que se adopten medidas adicionales y, cuando corresponda, se realice la consulta previa a la autoridad de protección de datos personales.

TÍTULO V

PRIVACIDAD EN LA INVESTIGACIÓN ACADÉMICA

Capítulo I

Reglas generales

Artículo 39.- Privacidad en la investigación. Toda actividad de investigación desarrollada por o en nombre de la UMET respetará los derechos a la privacidad, a la intimidad, a la protección de datos personales, al secreto profesional y a la propiedad intelectual de los sujetos de investigación, de los investigadores, del personal académico colaborador y de los estudiantes participantes. Las actividades se sujetarán al Código de Ética Institucional, de la Investigación y el Aprendizaje, al Reglamento de Investigación e Innovación, al presente Reglamento, a las normas técnicas aplicables y, cuando corresponda, a los pronunciamientos del Comité de Ética en Investigación con Seres Humanos.

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

Artículo 40.- Consentimiento informado. Los sujetos de investigación recibirán información clara, completa, comprensible y oportuna sobre los fines, metodología, riesgos, beneficios, duración, tratamiento de datos personales, plazos de conservación y posibles transferencias de la información y otorgarán su consentimiento libre, informado, específico e inequívoco antes de su participación.

La Universidad deberá identificar y documentar, en cada caso, la base jurídica que legitime el tratamiento. Cuando el tratamiento resulte necesario para el cumplimiento de obligaciones legales, la prestación de servicios educativos, la ejecución de relaciones jurídicas válidamente constituidas, la protección de intereses vitales u otra base reconocida por el ordenamiento jurídico, no será obligatorio recabar el consentimiento como requisito autónomo, sin perjuicio de los deberes de información, transparencia, seguridad y minimización.

Cuando la base legitimadora sea el consentimiento, este deberá obtenerse de acuerdo con la edad, capacidad y condiciones previstas en la normativa aplicable. Cuando corresponda, será otorgado por el representante legal o por el propio titular con la asistencia o autorización requerida. La información deberá proporcionarse en lenguaje claro, accesible y adecuado a la edad y nivel de comprensión del niño o adolescente.

La Universidad adoptará medidas reforzadas de protección, que incluirán, al menos:

a) Tratar únicamente los datos estrictamente necesarios para la finalidad institucional legítima;

b) Limitar el acceso a las personas autorizadas por necesidad funcional;

c) Aplicar medidas reforzadas de seguridad, confidencialidad y control de acceso;

d) Evitar la divulgación, publicación o transferencia innecesaria de información que permita identificar al titular;

e) Garantizar supervisión humana en tratamientos automatizados que puedan producir efectos jurídicos, académicos, económicos o significativos;

f) Evitar la elaboración de perfiles, la inferencia de emociones, el reconocimiento biométrico y la videovigilancia inteligente, salvo que exista base jurídica suficiente, necesidad y proporcionalidad demostradas, evaluación previa de riesgos y garantías adecuadas; y

g) Establecer plazos de conservación limitados y mecanismos seguros de supresión, anonimización o bloqueo cuando los datos hayan dejado de ser necesarios.

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

El tratamiento de datos personales de niños, niñas y adolescentes deberá incorporarse al Registro de Actividades de Tratamiento y someterse a gestión de riesgos. Cuando, por su naturaleza, alcance, contexto, finalidad o tecnología utilizada, pueda generar un alto riesgo para sus derechos y libertades, se realizará la correspondiente Evaluación de Impacto del Tratamiento antes de su inicio.

En el caso de niños y adolescentes, se requerirá adicionalmente el consentimiento expreso de sus representantes legales y se observará el interés superior del niño.

Artículo 41.- Anonimización y pseudonimización. Salvo cuando el tratamiento identificable sea estrictamente indispensable para los fines de la investigación, los datos personales se anonimizarán o pseudonimizarán de modo que se reduzca al mínimo el riesgo de reidentificación. La elección del mecanismo se documentará en el protocolo de investigación.

Capítulo II

Investigadores y personal académico

Artículo 42.- Deberes de los investigadores. Los investigadores y el personal académico que dirigen, coordinan o participan en proyectos de investigación deberán:

a) Someter a aprobación del comité competente, cuando corresponda, los protocolos que impliquen tratamiento de datos personales o de información sensible;

b) Implementar medidas de protección de la información durante el ciclo de vida del proyecto, incluyendo el acceso, almacenamiento, procesamiento, transferencia y eliminación;

c) Custodiar los soportes físicos y digitales de los datos del proyecto y observar el deber de reserva de los hallazgos no publicados;

d) Citar adecuadamente las fuentes y respetar la propiedad intelectual y los conocimientos colectivos y saberes ancestrales utilizados; y,

e) Reportar oportunamente cualquier incidente que afecte la privacidad o la seguridad de la información del proyecto.

Artículo 43.- Confidencialidad de los datos de investigación. Los datos generados o recolectados en el curso de proyectos de investigación se considerarán información confidencial o sensible, según corresponda y serán tratados conforme a las disposiciones del Título III de este Reglamento. Los productos de investigación no autorizados para difusión se considerarán información delicada y se sujetarán a su régimen específico.

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

Capítulo III

Estudiantes investigadores

Artículo 44.- Estudiantes en actividades investigativas. Los estudiantes que participen en actividades investigativas, prácticas, pasantías, proyectos de titulación o de vinculación con la sociedad observarán los deberes establecidos en este Reglamento, en el Código de Ética Institucional, de la Investigación y el Aprendizaje y en las directrices del docente o investigador responsable. Recibirán capacitación previa apropiada en materia de privacidad, protección de datos personales, secreto profesional y manejo de la información.

Artículo 45.- Tutela académica y responsabilidad funcional. El docente o investigador responsable de la actividad académica o investigativa deberá orientar y supervisar el cumplimiento de las obligaciones de privacidad, confidencialidad, seguridad de la información y protección de datos personales por parte de los estudiantes bajo su dirección.

En el ámbito de sus funciones, tendrá la calidad de responsable académico y custodio funcional de la información del proyecto y deberá adoptar, promover y verificar la aplicación de las medidas organizativas y de protección que correspondan, de conformidad con el protocolo aprobado, las políticas institucionales y el presente Reglamento.

La responsabilidad prevista en este artículo no atribuye al docente o investigador la calidad jurídica de responsable, corresponsable o encargado del tratamiento, salvo que dicha condición se configure expresamente conforme a la Ley Orgánica de Protección de Datos Personales y al instrumento jurídico aplicable. La Universidad Metropolitana conservará, frente a los titulares, la sociedad y el Estado, su calidad de responsable del tratamiento.

Capítulo IV

Sujetos de investigación, comunidades y saberes ancestrales

Artículo 46.- Sujetos de investigación. El tratamiento de datos personales de sujetos de investigación se sujetará al consentimiento informado, a las medidas de anonimización o pseudonimización aplicables, a los plazos de conservación previstos en el protocolo y a las garantías éticas adicionales que establezcan los comités competentes. Los sujetos podrán revocar su consentimiento conforme a la Ley, sin perjuicio de los tratamientos lícitamente realizados con anterioridad.

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

Artículo 47.- Comunidades y saberes ancestrales. Toda investigación que involucre a pueblos y nacionalidades indígenas, montubios, afroecuatorianos, comunidades u otros colectivos titulares de conocimientos colectivos o saberes ancestrales requerirá su consentimiento libre, previo e informado, cuando resulte exigible por la naturaleza del proyecto, la población involucrada, el ordenamiento jurídico y los protocolos éticos aplicables, conforme a la Constitución, los instrumentos internacionales de derechos humanos y la legislación ecuatoriana.

La Universidad protegerá la propiedad intelectual colectiva y el patrimonio cultural inmaterial asociados y se abstendrá de tratamientos que puedan despojar, distorsionar o lesionar tales saberes.

TÍTULO VI

SEGURIDAD DE LA INFORMACIÓN

Capítulo I

Sistema de Gestión de Seguridad de la Información

Artículo 48.- Sistema de Gestión de Seguridad de la Información. El Sistema de Gestión de Seguridad de la Información (SGSI) constituye el componente técnico, organizativo y de gestión de riesgos del Sistema Institucional de Protección de la Privacidad, la Información y los Datos Personales (SIPPID). Su finalidad es preservar la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y resiliencia de la información institucional, con independencia de su soporte, formato o ubicación.

El SGSI será implementado, administrado y actualizado por la Dirección de Tecnologías Informáticas, bajo la coordinación del Vicerrectorado Administrativo y conforme a las políticas, lineamientos y prioridades institucionales definidas en el marco del SIPPID. Para su funcionamiento se aplicarán controles técnicos, físicos, organizativos y jurídicos proporcionales a los riesgos identificados, considerando las normas ISO/IEC aplicables como referentes metodológicos.

El SGSI comprenderá, al menos:

a) Inventario y clasificación de activos de información;
b) Gestión de riesgos;
c) Administración de accesos y privilegios;
d) Seguridad de redes, sistemas, aplicaciones, servicios en la nube y dispositivos;
e) Gestión de vulnerabilidades e incidentes;
f) Continuidad operativa, respaldo y recuperación;

g) Monitoreo y trazabilidad;
h) Gestión de proveedores tecnológicos;
i) Capacitación y concienciación; y,
j) Revisión, auditoría y mejora continua.

El SGSI no sustituye al SIPPID, ni constituye un sistema paralelo. El SIPPID mantiene la gobernanza integral de la privacidad, la protección de datos personales y la información institucional, mientras que el SGSI ejecuta y articula las medidas de seguridad de la información dentro de dicho marco general.

Artículo 49.- Componentes mínimos del SGSI. El SGSI comprenderá, al menos:

1. Una Política Institucional de Seguridad de la Información, aprobada por el Consejo de Regentes y el Consejo Académico Superior;

2. Un análisis y tratamiento institucional de riesgos de información, conforme a las normas **ISO/IEC**;

3. Un Inventario de Activos de Información permanentemente actualizado;

4. Una declaración de aplicabilidad de controles, basada en el catálogo de las normas **ISO/IEC**;

5. Procedimientos de control de accesos, gestión de identidades, gestión de cambios, gestión de vulnerabilidades, gestión de proveedores y desarrollo seguro;

6. Mecanismos de monitoreo, registro de actividad, métricas e indicadores;

7. Un Plan de Continuidad y Recuperación ante Desastres, conforme a las normas **ISO**;

8. Procedimientos de gestión de incidentes de seguridad y notificación de vulneraciones a la protección de datos personales;

9. Programas de capacitación, sensibilización y cultura institucional; y,

10. Mecanismos de auditoría interna, revisión por la dirección y mejora continua.

Artículo 50.- Política Institucional de Seguridad de la Información. La Política Institucional de Seguridad de la Información será aprobada por el Consejo de Regentes y el Consejo Académico Superior, definirá los objetivos, alcance, principios, responsabilidades y compromisos institucionales en la materia y será revisada periódicamente. Su contenido se difundirá obligatoriamente a toda la Comunidad Universitaria y será de cumplimiento obligatorio.

Capítulo II

Controles técnicos, organizativos y físicos

Artículo 51.- Controles aplicables. Se implementarán controles técnicos, organizativos, físicos y jurídicos proporcionales al riesgo, basados en las normas **ISO/IEC** y demás referentes técnicos aplicables, que comprenderán, entre otros, los siguientes:

a) Control de accesos, autenticación robusta y gestión de identidades y privilegios;

b) Cifrado de datos en tránsito y reposo, según el nivel de clasificación de la información;

c) Segregación de ambientes de desarrollo, prueba y producción;

d) Copias de respaldo, conservación y verificación de su integridad;

e) Protección contra códigos maliciosos, acceso no autorizado y exfiltración de datos;

f) Gestión de vulnerabilidades, parches y configuraciones seguras;

g) Protección física de instalaciones, áreas restringidas, equipos y soportes de información;

h) Procedimientos de gestión de proveedores y subcontratistas con acceso información o sistemas;

i) Procedimientos de desarrollo seguro de aplicaciones y sistemas;

j) Procedimientos de eliminación segura de información y de retiro o reutilización de soportes; y,

k) Otros controles que determine el Comité y la Dirección de Tecnologías Informáticas.

Artículo 52.- Cultura de seguridad. Se promoverá una cultura institucional de seguridad de la información mediante programas obligatorios de inducción, capacitación periódica, sensibilización, comunicación y participación, dirigidos a las autoridades, el personal académico, técnico docente, administrativo, los estudiantes y los terceros con vínculo institucional.

Capítulo III

Continuidad y gestión de incidentes

Artículo 53.- Continuidad y resiliencia. La Universidad adoptará un Plan Institucional de Continuidad y Recuperación ante Desastres, conforme a las normas **ISO** aplicables, que comprenda análisis de impacto, identificación de procesos críticos,

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

estrategias de recuperación, ejercicios periódicos y mecanismos de mejora continua. El Plan se articulará con el SGSI y con los planes operativos de la Dirección de Tecnologías Informáticas.

Artículo 54.- Gestión de incidentes. La Universidad implementará un Procedimiento Institucional de Gestión de Incidentes que comprenda detección, registro, clasificación, respuesta, contención, análisis de causa raíz, comunicación interna y externa y mejora. Cuando el incidente afecte datos personales, se aplicará el procedimiento de notificación a la Superintendencia de Protección de Datos Personales y, cuando corresponda, a los titulares afectados, dentro de los plazos legales. La gestión técnica corresponderá a la Dirección de Tecnologías Informáticas, en coordinación con el Delegado de Protección de Datos Personales y la Procuraduría Nacional.

Artículo 55.- Reporte y prevención de incidentes. Toda persona que detecte un incidente, vulnerabilidad, brecha de seguridad, sospecha de incidente o cualquier circunstancia que pueda afectar la seguridad de la información o la protección de datos personales deberá reportarlo de inmediato a su superior jerárquico, al responsable operativo del activo o sistema y a la Dirección de Tecnologías Informáticas. Cuando el hecho involucre datos personales deberá informarse también al Delegado de Protección de Datos Personales.

El deber de reporte comprende, entre otros, los intentos de *phishing*, suplantación de identidad, ingeniería social, acceso no autorizado, obtención fraudulenta de credenciales, envío de enlaces o archivos sospechosos, instalación de software malicioso, pérdida o exposición de dispositivos, accesos inusuales, alteración de información y cualquier otra conducta orientada a comprometer sistemas, cuentas, redes o información institucional.

La Dirección de Tecnologías Informáticas deberá capacitar periódicamente al personal y a los demás usuarios institucionales para identificar, prevenir y reportar estas amenazas. Asimismo, deberá analizar los reportes recibidos y adoptar oportunamente las medidas técnicas, organizativas y de seguridad que correspondan según la naturaleza y nivel de riesgo del evento, incluyendo el bloqueo preventivo de accesos, cambio de credenciales, aislamiento de equipos, preservación de evidencias, contención del incidente, recuperación de sistemas y coordinación con las instancias competentes.

La omisión deliberada del reporte o la ocultación consciente de un incidente constituirá infracción conforme a este Reglamento, sin perjuicio de las demás responsabilidades administrativas, civiles o penales que pudieren corresponder.

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

TÍTULO VII

SISTEMA INSTITUCIONAL DE PROTECCIÓN DE LA PRIVACIDAD, LA INFORMACIÓN Y LOS DATOS PERSONALES

Capítulo I

Sistema Institucional

Artículo 56.- Sistema Institucional. Establézcase el Sistema Institucional de Protección de la Privacidad, la Información y los Datos Personales de la Universidad Metropolitana, en adelante SIPPID, como el conjunto articulado, jerárquico y funcional de instancias, normas, políticas, procedimientos, herramientas, controles, indicadores y mecanismos de cultura institucional destinados a garantizar la observancia integrada de los deberes y obligaciones establecidos en el presente Reglamento, en el Reglamento sobre Inteligencia Artificial, en el Código de Ética Institucional, de la Investigación y el Aprendizaje, en las Políticas de Protección de Datos Personales y en la demás normativa interna y nacional aplicable.

El SIPPID operará mediante la coordinación del Comité Institucional y la distribución de funciones entre las autoridades, direcciones, unidades y responsables funcionales previstos en el Estatuto y en el Reglamento General al Estatuto, sin crear estructuras administrativas paralelas ni alterar las competencias orgánicas vigentes.

Artículo 57.- Componentes del SIPPID. El SIPPID está integrado por:

a) El Consejo Académico Superior, en su calidad de máximo órgano colegiado de dirección;

b) El Rector, como representante legal y máxima autoridad ejecutiva;

c) El Vicerrector Administrativo, en su calidad de autoridad interna responsable del Tratamiento de Datos Personales;

d) El Vicerrector Académico, respecto de la información académica, investigativa y de vinculación;

e) El Comité Institucional de Protección de la Privacidad, la Información, los Datos Personales y de Uso Ético de la Inteligencia Artificial;

f) El Delegado de Protección de Datos Personales;

g) La Dirección de Tecnologías Informáticas, incluida su función de seguridad de la información y ciberseguridad;

h) El Especialista en Cumplimiento, conforme al artículo 89 del Reglamento General al Estatuto, en sus funciones de cumplimiento normativo y control interno;

i) La Procuraduría Nacional, en sus funciones de asesoría jurídica y patrocinio institucional;

j) La Secretaría General Técnica, para los efectos de gestión documental, certificación y archivo;

k) El Comité Universitario de Ética y los Subcomités de Ética de Sede, en lo que respecta a las dimensiones éticas del tratamiento de la información;

l) Los Comités de Ética en Investigación con Seres Humanos y demás comités especializados, en sus respectivos ámbitos; y,

m) Las demás unidades académicas y administrativas que, por su ámbito funcional, intervengan en el tratamiento de información o de datos personales.

Artículo 58.- Principios de funcionamiento. El SIPPID se rige por los principios de unidad institucional, articulación, subsidiariedad, especialidad, mejora continua, proporcionalidad, responsabilidad proactiva y demostrada, transparencia y rendición de cuentas. Las instancias del Sistema actuarán de manera coordinada bajo los criterios técnicos, jurídicos y éticos del Comité Institucional, sin perjuicio de las competencias propias que el ordenamiento, el Estatuto y el Reglamento General al Estatuto atribuyen a cada autoridad, dirección, unidad o responsable funcional.

Capítulo II

Comité Institucional

Artículo 59.- Comité Institucional. El Comité Institucional de Protección de la Privacidad, la Información, los Datos Personales y de Uso Ético de la Inteligencia Artificial, o CIPPIA, es un órgano técnico, multidisciplinario, de carácter articulador, consultivo, preventivo y de seguimiento, encargado de coordinar el SIPPID y de procurar que las funciones ya existentes se ejerzan bajo criterios comunes, uniformes y documentados.

El Comité no ejerce dirección institucional, no aprueba reglamentos, no sustituye, ni condiciona las decisiones del Consejo Académico Superior y no asume las competencias propias del Vicerrectorado Administrativo, de la Dirección de Tecnologías Informáticas, del Especialista en Cumplimiento, de la Procuraduría Nacional, del Delegado de Protección de Datos Personales, de las unidades académicas ni de las áreas administrativas. Su función se circunscribe a la planificación, articulación, seguimiento, evaluación y control técnico-operativo del Sistema, sin perjuicio de las atribuciones del Consejo Académico Superior y de las competencias de cada autoridad, dirección, unidad o responsable funcional, las cuales se ejercerán a través de las unidades responsables de los procesos correspondientes.

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

Artículo 60.- Integración del Comité. El CIPPIA estará integrado por los siguientes miembros:

a) El Vicerrector Administrativo, en su calidad de Responsable interno del Tratamiento de Datos Personales, quien lo presidirá;

b) El Vicerrector Académico o su delegado;

c) El Delegado de Protección de Datos Personales;

d) El Director de Tecnologías Informáticas;

e) El Especialista en Cumplimiento;

f) El Procurador Nacional o su delegado, quien actuará como secretario y emitirá opinión jurídica cuando le sea requerida;

g) Un representante del Comité Universitario de Ética, designado por dicho Comité;

h) Un docente investigador con producción científica relevante en áreas vinculadas a la inteligencia artificial, ciencia de datos, ciberseguridad o informática, designado por el Vicerrector Académico de entre dos postulaciones; y,

i) Un representante estudiantil, preferentemente de carreras vinculadas a tecnologías de la información, designado por el Vicerrector Académico de entre dos postulaciones, observando los criterios académicos previstos en el Estatuto Institucional para la representación estudiantil.

Cada miembro designado en los numerales g), h) e i) contará con un alterno designado bajo iguales criterios. Podrá invitarse a las sesiones, sin derecho a voto, a personas con experticia técnica relevante en el caso concreto.

Artículo 61.- Funciones del Comité. Sin perjuicio de las demás funciones previstas en el Reglamento sobre Inteligencia Artificial, son funciones del Comité, en el marco del presente Reglamento:

1. Velar por la correcta aplicación e interpretación del presente Reglamento y de la normativa interna y nacional conexa;

2. Coordinar el funcionamiento del SIPPID y la articulación entre sus componentes;

3. Aprobar técnicamente los lineamientos, directrices, guías, formularios, plantillas y procedimientos operativos para la implementación de este Reglamento;

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

4. Conocer y emitir criterio técnico no vinculante respecto de la Política Institucional de Seguridad de la Información, la Política de Privacidad y demás instrumentos institucionales en su ámbito;

5. Validar la clasificación institucional de la información y la metodología de gestión de riesgos;

6. Supervisar el funcionamiento del SGSI, del Sistema de Gestión de Información de Privacidad y del Sistema de Gestión de Inteligencia Artificial, conforme a las normas ISO/IEC;

7. Recibir y canalizar consultas, alertas, denuncias y reportes de incidentes vinculados a la privacidad, información o datos personales, sin perjuicio de las competencias de los demás órganos de la Universidad;

8. Promover acciones de capacitación, sensibilización y cultura institucional en privacidad, seguridad de la información, protección de datos personales y uso ético de la inteligencia artificial;

9. Emitir un informe anual integrado de gobernanza, dirigido al Rector, al Consejo de Regentes y al Consejo Académico Superior, sobre el desempeño del SIPPID;

10. Proponer al Consejo Académico Superior, a través del Rector, las reformas y actualizaciones del presente Reglamento, así como los instrumentos complementarios necesarios;

11. Coordinar con la Superintendencia de Protección de Datos Personales y demás autoridades de control en los asuntos de su competencia, a través del Delegado y de la Procuraduría Nacional;

12. Promover y supervisar los procesos de certificación institucional bajo las normas ISO aplicables y su mantenimiento; y,

13. Las demás que le sean asignadas por el presente Reglamento, por el Reglamento sobre Inteligencia Artificial o por el Consejo Académico Superior.

Artículo 62.- Sesiones, *quórum* y confidencialidad. El Comité sesionará ordinariamente al menos una vez por trimestre y extraordinariamente cuando sea convocado por su Presidente o a solicitud fundamentada de la mayoría de sus miembros. El *quórum* se constituirá con la mitad más uno de sus miembros principales y las decisiones se adoptarán por mayoría simple de los presentes; en caso de empate, el Presidente tendrá voto dirimente. Las sesiones podrán realizarse de manera presencial, virtual o híbrida.

Los miembros del Comité, sus alternos, secretarios e invitados deberán suscribir un compromiso de confidencialidad respecto de la información, los hechos y los datos personales a los que tengan acceso en ejercicio de sus funciones. Su incumplimiento generará responsabilidad conforme a la normativa institucional vigente y, en particular, conforme al Código de Ética Institucional, de la Investigación y el Aprendizaje.

Capítulo III

Roles institucionales

Artículo 63.- Autoridad interna responsable del tratamiento. El Vicerrector Administrativo asumirá la coordinación institucional del cumplimiento del presente Reglamento en sus dimensiones de protección de datos personales, seguridad de la información y articulación con la inteligencia artificial, sin perjuicio de la responsabilidad indelegable de la Universidad Metropolitana frente a los titulares, la sociedad y el Estado.

Artículo 64.- Delegado de Protección de Datos Personales. El Delegado de Protección de Datos Personales ejercerá sus funciones con independencia técnica y funcional y tendrá atribuciones de asesoría, supervisión, vigilancia, alerta y recomendación especializada en materia de protección de datos personales.

En particular, le corresponderá:

a) Asesorar al responsable del tratamiento y a las unidades institucionales sobre el cumplimiento de la normativa aplicable;

b) Supervisar la atención de los derechos de los titulares y verificar el cumplimiento de los plazos, requisitos y garantías correspondientes;

c) Emitir recomendaciones sobre la elaboración y actualización del Registro de Actividades de Tratamiento;

d) Asesorar y supervisar la realización de Evaluaciones de Impacto del Tratamiento;

e) Emitir alertas y recomendaciones respecto de transferencias nacionales e internacionales de datos personales;

f) Supervisar la gestión de incidentes que involucren datos personales y recomendar las medidas de contención, corrección, notificación y prevención que correspondan;

g) Cooperar con la autoridad de protección de datos personales y actuar como punto de contacto institucional en el ámbito de sus competencias; y,

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

h) Elaborar informes, recomendaciones y reportes sobre el nivel de cumplimiento institucional.

El Delegado no asumirá funciones operativas, resolutivas o de ejecución directa propias del responsable del tratamiento, de los encargados, de la Dirección de Tecnologías Informáticas, de la Secretaría General Técnica, de la Procuraduría Nacional o de otras unidades institucionales. Tampoco determinará por sí mismo los fines y medios del tratamiento ni adoptará decisiones institucionales sobre el tratamiento de datos personales.

Artículo 65.- Dirección de Tecnologías Informáticas. Corresponde a la Dirección de Tecnologías Informáticas, conforme al Reglamento General al Estatuto, administrar y mantener la infraestructura, plataformas, aplicaciones y servicios tecnológicos institucionales, así como implementar las medidas técnicas de seguridad, controles de acceso, mecanismos de monitoreo, planes de continuidad, gestión técnica de incidentes e inventario tecnológico de activos.

En los procesos de adquisición, contratación, renovación, actualización o implementación de licencias, aplicaciones, servicios en la nube, sistemas informáticos o herramientas de inteligencia artificial, la Dirección de Tecnologías Informáticas deberá:

a) Recibir y analizar el requerimiento funcional formulado por la unidad académica o administrativa interesada;

b) Verificar la viabilidad técnica, compatibilidad, interoperabilidad, seguridad, escalabilidad, soporte, continuidad, licenciamiento y sostenibilidad tecnológica de la solución propuesta;

c) Evaluar los riesgos de seguridad de la información, ciberseguridad, alojamiento, transferencias, accesos, integraciones y dependencia tecnológica del proveedor;

d) Emitir el informe técnico correspondiente, con las condiciones, recomendaciones y controles necesarios para su implementación;

e) Coordinar con el Vicerrectorado Administrativo, el Delegado de Protección de Datos Personales, el Especialista en Cumplimiento, la Procuraduría Nacional, el Comité Institucional y las demás unidades competentes, cuando la naturaleza, finalidad, nivel de riesgo o datos tratados así lo requieran;

f) Gestionar técnicamente las relaciones con proveedores y supervisar el cumplimiento de las condiciones de integración, soporte, seguridad y continuidad de los servicios contratados; y,

g) Mantener actualizado el inventario institucional de licencias, aplicaciones, sistemas y servicios tecnológicos.

La Dirección de Tecnologías Informáticas no determinará por sí sola la necesidad sustantiva de adquisición o contratación, la cual corresponderá a la unidad requirente conforme a sus funciones, objetivos y planificación. Tampoco aprobará por sí misma la afectación presupuestaria ni la contratación definitiva, que se sujetarán al Plan Operativo Anual, al presupuesto institucional, al procedimiento contractual aplicable y a la autorización de la autoridad competente.

La calificación de un sistema como de alto riesgo no constituirá, por sí sola, causal automática de rechazo o de no adquisición. En estos casos deberán establecerse medidas reforzadas de evaluación, autorización, supervisión, seguridad, protección de datos personales, trazabilidad y control humano, de manera previa a su implementación.

Artículo 66.- Especialista en Cumplimiento. El Especialista en Cumplimiento ejercerá, en el marco del SIPPID, las funciones de seguimiento, control interno y verificación del cumplimiento normativo en materia de privacidad, protección de datos personales y seguridad de la información, y coordinará la ejecución de las revisiones y auditorías internas del Sistema, cuando no exista conflicto de interés y cuente con independencia funcional, sin perjuicio de la contratación de auditores externos especializados cuando la naturaleza del aspecto evaluado lo requiera.

Artículo 67.- Procuraduría Nacional. La Procuraduría Nacional asesorará jurídicamente a las autoridades, órganos colegiados y unidades en la aplicación e interpretación del presente Reglamento, intervendrá en la revisión de cláusulas contractuales relativas a la protección de información y datos personales, emitirá criterio jurídico no vinculante en los casos previstos en este Reglamento y patrocinará a la Universidad en los asuntos que se deriven de su aplicación.

Artículo 68.- Custodios y responsables operativos. Cada autoridad académica o administrativa, decano, director de escuela, coordinador de carrera, director departamental, director de sede o responsable de unidad, será custodio funcional de los activos de información que se encuentren bajo su responsabilidad, con sujeción a los procedimientos institucionales aplicables. Los custodios designarán, cuando corresponda, responsables operativos para la gestión cotidiana, sin perjuicio de su propia responsabilidad.

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

TÍTULO VIII

CUMPLIMIENTO, CERTIFICACIÓN Y MEJORA CONTINUA

Artículo 69.- Mejora continua basada en estándares internacionales. La Universidad adoptará un enfoque de mejora continua basado en las normas técnicas internacionales aplicables, en particular las normas ISO/IEC vigentes y se mantendrá debidamente actualizada en las nuevas versiones, mediante ciclos de planificación, ejecución, verificación y acción correctiva y procesos sistemáticos de revisión por la dirección.

Las normas técnicas internacionales referidas constituyen referentes metodológicos aplicables exclusivamente a la seguridad de la información, la privacidad, la protección de datos personales, la gestión de la inteligencia artificial, la gestión de riesgos y la continuidad institucional.

Esas normas no sustituyen, modifican, ni reinterpretan los estándares de calidad de la educación superior, los cuales se rigen por la Constitución, la Ley Orgánica de Educación Superior, la normativa del Consejo de Educación Superior, los modelos del Consejo de Aseguramiento de la Calidad de la Educación Superior, el Estatuto, el Reglamento General al Estatuto y el Plan Estratégico de Desarrollo Institucional, así como por los sistemas de evaluación externa, acreditación y cualificación. La mejora continua de la calidad académica e institucional continuará rigiéndose por dichos instrumentos.

Artículo 70.- Auditoría interna. El SIPPID se someterá a revisión y auditoría interna periódica, al menos una vez por año, conforme al programa anual que conozca el Comité. Esta función no implica la creación de una unidad administrativa permanente de auditoría interna y podrá ser ejecutada por un equipo técnico *ad hoc* con suficiente independencia y competencia técnica, por el Especialista en Cumplimiento cuando no exista conflicto de interés y cuente con independencia funcional, o mediante la contratación de auditores externos especializados, según la naturaleza jurídica, técnica, ética, de privacidad y de seguridad de la información de los aspectos que deban evaluarse.

Artículo 71.- Auditoría externa y verificación. Cuando las circunstancias lo justifiquen, la Universidad podrá disponer auditorías externas independientes o verificaciones por terceras partes, en especial respecto de los sistemas críticos, las contrataciones con proveedores de información o nube, los procesos de tratamiento a gran escala y los sistemas de inteligencia artificial considerados de alto riesgo.

Artículo 72.- Indicadores y métricas. El Comité, con apoyo del Delegado de Protección de Datos Personales y de la Dirección de Tecnologías Informáticas, definirá

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

un cuadro de indicadores y métricas de desempeño del SIPPID, que se reportará periódicamente al Rector y, anualmente, al Consejo Académico Superior. El cuadro de indicadores identificará, respecto de cada métrica, la unidad responsable del levantamiento de la información, la periodicidad de la medición, la fuente de verificación y el destinatario del reporte.

TÍTULO IX

RÉGIMEN DE INFRACCIONES Y RESPONSABILIDADES

Artículo 73.- Reenvío al régimen disciplinario y ético. El régimen aplicable a las infracciones a las disposiciones del presente Reglamento se regirá, sin perjuicio de las responsabilidades civiles, administrativas, penales o constitucionales que correspondan, por las disposiciones de la Ley Orgánica de Educación Superior, el Código del Trabajo, el Estatuto Institucional, el Reglamento Interno de Trabajo, el Reglamento que Regula el Procedimiento Disciplinario para los Estudiantes, Profesores e Investigadores y el Código de Ética Institucional, de la Investigación y el Aprendizaje.

Artículo 74.- Conductas constitutivas de infracción. Sin perjuicio de las infracciones tipificadas en otras normas internas y en el ordenamiento jurídico, constituyen infracción al presente Reglamento:

a) Vulnerar el deber perpetuo de protección de los datos personales establecido en el Título II, en cualquiera de sus formas;

b) Revelar, divulgar, comunicar o transferir información sensible, delicada o reservada sin base jurídica, autorización institucional o consentimiento;

c) Tratar datos personales sin observar los principios y obligaciones legales y reglamentarios aplicables;

d) Cargar, ingresar o compartir información institucional confidencial, sensible o reservada en sistemas externos no autorizados, incluyendo sistemas de inteligencia artificial no aprobados;

e) Omitir las medidas de seguridad de la información exigibles, conforme a la clasificación del activo;

f) Omitir el reporte oportuno de incidentes, vulnerabilidades o sospechas razonables;

g) Conservar copias, extractos, reproducciones o derivaciones de información institucional o datos personales con posterioridad al cese del vínculo;

h) Utilizar la información institucional o los datos personales para fines distintos de aquellos para los que fueron recolectados o tratados;

i) Obstaculizar las actividades de auditoría, supervisión o ejercicio de derechos de los titulares; y,

j) Cualquier otra conducta que vulnere los principios, deberes o prohibiciones establecidos en este Reglamento.

Artículo 75.- Subsistencia de responsabilidades. La terminación, por cualquier causa, del vínculo académico, laboral, contractual o de colaboración con la Universidad Metropolitana, no extingue las responsabilidades civiles, administrativas, éticas o penales derivadas del incumplimiento de los deberes establecidos en este Reglamento y en particular, del deber perpetuo de protección de los datos personales.

Artículo 76.- Acciones institucionales. Sin perjuicio del régimen sancionador aplicable a la persona infractora, la Universidad Metropolitana podrá adoptar las acciones institucionales necesarias para contener, mitigar y reparar las consecuencias del incumplimiento, incluida la suspensión, restricción o desactivación de sistemas y servicios, la solicitud de remediación, la notificación a las autoridades competentes y la implementación de medidas correctivas.

TÍTULO X

ARTICULACIÓN, TRANSPARENCIA Y REVISIÓN

Artículo 77.- Articulación con el Reglamento sobre Inteligencia Artificial. El presente Reglamento y el Reglamento para el Uso Ético, Responsable y Seguro de la Inteligencia Artificial constituyen un cuerpo normativo articulado y coherente. Las instancias del SIPPID son comunes a ambos instrumentos. Cuando una situación involucre simultáneamente el tratamiento de información o datos personales y el uso de inteligencia artificial, las disposiciones de uno y otro reglamento se aplicarán de manera complementaria y bajo el principio de protección más favorable a los derechos fundamentales.

Artículo 78.- Transparencia institucional. La Universidad publicará y mantendrá actualizada información clara, accesible y comprensible sobre sus políticas, procedimientos, mecanismos de atención de derechos, canales de denuncia y reportes anuales en materia de privacidad, información y protección de datos personales, sin perjuicio de las disposiciones específicas previstas en otros instrumentos internos.

Artículo 79.- Revisión periódica y actualización extraordinaria. El CIPPIA realizará una revisión integral del contenido, aplicación y efectividad del presente

Reglamento al menos cada tres años, contados a partir de su entrada en vigencia o de su última reforma sustancial.

De manera extraordinaria, el Reglamento será revisado y, de ser procedente, actualizado cuando la *International Organization for Standardization* —ISO— actualice, modifique, sustituya, derogue, reforme, renueve o emita nuevas versiones de las normas ISO que sirven de fundamento técnico al presente instrumento.

Como resultado de la revisión ordinaria o extraordinaria, el Comité Institucional podrá proponer al Consejo Académico Superior, a través del Rector y previo informe favorable del Consejo de Regentes en lo que corresponda, las reformas que estime necesarias.

DISPOSICIONES GENERALES

PRIMERA. - Para efectos de la aplicación e interpretación del presente Reglamento, sin perjuicio de las definiciones contenidas en la Ley Orgánica de Protección de Datos Personales, su Reglamento General, las normas secundarias de la Superintendencia de Protección de Datos Personales, el Estatuto Institucional, el Código de Ética Institucional, de la Investigación y el Aprendizaje, el Reglamento sobre Inteligencia Artificial y demás normativa aplicable, se establecen las siguientes definiciones, ordenadas alfabéticamente:

Activo de información: todo dato, documento, registro, base de datos, sistema, plataforma, infraestructura, conocimiento o cualquier otro elemento que contenga, soporte o permita el tratamiento de información de la Universidad Metropolitana, con valor para la institución, su comunidad o terceros vinculados.

Anonimización: proceso técnico o procedimental por el cual los datos personales pierden de modo irreversible toda capacidad de identificar al titular, directa o indirectamente, mediante medios razonablemente disponibles.

Auditoría: proceso documentado, sistemático e independiente de revisión, evaluación y verificación, interna o externa, del cumplimiento de obligaciones jurídicas, técnicas, éticas y organizativas aplicables a la protección de la privacidad, de la información y de los datos personales.

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

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

Comité o CIPPIA: Comité Institucional de Protección de la Privacidad, la Información, los Datos Personales y de Uso Ético de la Inteligencia Artificial de la Universidad Metropolitana, conformado conforme al presente Reglamento, en concordancia con el Reglamento sobre Inteligencia Artificial.

Confidencialidad: atributo de la información que asegura que esta no se ponga a disposición ni se revele a personas, entidades o procesos no autorizados.

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

Continuidad: capacidad institucional de mantener, ante un evento adverso o disruptivo, la operación de los procesos críticos vinculados al tratamiento de información y datos personales, dentro de plazos y niveles de servicio aceptables.

Control: medida técnica, organizativa, jurídica o física destinada a prevenir, detectar, corregir o mitigar riesgos sobre la información, los datos personales o los sistemas que los soportan.

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

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

Disponibilidad: atributo de la información que asegura su acceso y utilización a quienes están autorizados, en el momento y forma en que lo requieran.

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

Especialista en Cumplimiento: responsable funcional previsto en el Reglamento General al Estatuto, a cuyo cargo se encuentran, conforme a su artículo 89, las funciones de cumplimiento normativo y control interno, incluida la verificación del cumplimiento en materia de privacidad, protección de datos personales y seguridad de la información.

Información delicada: información cuyo tratamiento, revelación, alteración o pérdida puede causar afectación significativa a los derechos, intereses, seguridad o reputación de personas, comunidades o de la institución, sin que necesariamente constituya dato personal sensible o información reservada.

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

Información institucional: toda información que la Universidad Metropolitana genera, recibe, posee, custodia, procesa, comunica, conserva, transmite o elimina en el desarrollo de sus actividades, en cualquier soporte y formato.

Información reservada y estratégica institucional: información de la Universidad Metropolitana o de terceros que, por su valor institucional, estratégico, contractual, tecnológico, financiero o reputacional, no es de conocimiento público, ha sido objeto de medidas razonables para mantener su reserva y cuya divulgación no autorizada puede causar perjuicio académico, operativo, tecnológico, reputacional, económico o estratégico, sin perjuicio de los deberes de transparencia propios del Sistema de Educación Superior.

Información sensible: categoría de información que comprende, según el contexto, los datos personales sensibles definidos por la Ley Orgánica de Protección de Datos Personales y aquella información cuya divulgación, alteración o pérdida puede causar afectación grave a los derechos fundamentales, a la seguridad o a la dignidad de las personas o comunidades.

Integridad de la información: atributo que asegura la exactitud, completitud y no alteración no autorizada de la información durante todo su ciclo de vida.

ISO/IEC: normas técnicas internacionales emitidas por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional, que constituyen referente metodológico de buenas prácticas en seguridad de la información, privacidad, gestión de riesgos, continuidad y gestión de inteligencia artificial.

Mejora continua: principio de gestión que orienta el perfeccionamiento sistemático y progresivo de los procesos, controles y resultados del Sistema Institucional, mediante ciclos de planificación, ejecución, verificación y acción correctiva.

Política institucional: instrumento de alto nivel aprobado por la autoridad competente, que define la voluntad institucional, los objetivos, las directrices y los compromisos de la Universidad Metropolitana en materia de protección de la privacidad, la información, los datos personales y el uso ético de la inteligencia artificial.

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

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

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

Pseudonimización: tratamiento de datos personales de modo tal que ya no puedan atribuirse a un titular sin utilizar información adicional, siempre que dicha información se conserve por separado y esté sujeta a medidas técnicas y organizativas de protección.

Registro de Actividades de Tratamiento o RAT: documento o sistema que recoge, de manera estructurada y actualizada, las actividades de tratamiento de datos personales realizadas por la Universidad Metropolitana, conforme a la Ley Orgánica de Protección de Datos Personales y su Reglamento General.

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

Resiliencia: capacidad de un sistema, proceso o institución de resistir, absorber, adaptarse y recuperarse de eventos adversos manteniendo sus funciones esenciales.

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

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

Saberes ancestrales: conocimientos colectivos, prácticas, expresiones culturales y patrimonio intelectual de los pueblos y nacionalidades indígenas, montubios, afroecuatorianos y comunidades, protegidos conforme a la Constitución, los instrumentos internacionales de derechos humanos y el ordenamiento jurídico ecuatoriano.

SGSI: Sistema de Gestión de Seguridad de la Información, conforme a los lineamientos de la norma ISO/IEC 27001 y normas conexas.

SIPPID: Sistema Institucional de Protección de la Privacidad, la Información y los Datos Personales de la Universidad Metropolitana, creado por el presente Reglamento como marco unificado de gobernanza.

Secreto profesional: deber jurídico y deontológico de no revelar información obtenida en el ejercicio de una profesión, oficio o función, salvo causa legal de exoneración debidamente acreditada.

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información, así como de otros atributos como autenticidad, no repudio, trazabilidad y resiliencia.

Sistema Institucional o el Sistema: Sistema Institucional de Protección de la Privacidad, la Información y los Datos Personales (SIPPID), creado en el Título VII (artículo 56) del presente Reglamento.

Tratamiento de datos personales: cualquier operación o conjunto de operaciones realizadas sobre datos personales, automatizada o no, conforme a la Ley Orgánica de Protección de Datos Personales.

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

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

Vínculo institucional: relación de cualquier naturaleza —académica, laboral, contractual, civil, mercantil, de cooperación, de pasantía, de investigación o equivalente— que una persona natural o jurídica mantiene con la Universidad Metropolitana.

SEGUNDA. - La Universidad Metropolitana adoptará como política institucional alcanzar y mantener la certificación bajo las normas técnicas internacionales aplicables a la seguridad de la información, la privacidad y la gobernanza de la inteligencia artificial, en particular, las normas ISO/IEC 27001, ISO/IEC 27701 e ISO/IEC 42001, sus reformas y sustituciones, conforme a un plan progresivo aprobado por el Rector. Una vez obtenida la certificación, la Universidad implementará los procesos institucionales necesarios para mantenerla en estado vigente, mediante auditorías periódicas, revisiones por la dirección y procesos de mejora continua.

TERCERA. - Las referencias contenidas en este Reglamento a leyes, reglamentos, resoluciones o instrumentos normativos se entenderán hechas a las disposiciones vigentes en cada momento de aplicación. En caso de modificación de la denominación, numeración o contenido de tales instrumentos, las referencias se entenderán actualizadas de oficio en lo pertinente, sin perjuicio de la actualización formal del Reglamento cuando corresponda.

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

CUARTA. - Toda referencia contenida en otros instrumentos normativos internos a la regulación general de la privacidad, la confidencialidad institucional, la seguridad de la información o la protección de datos personales, se entenderá hecha al presente Reglamento, sin perjuicio de las disposiciones específicas previstas en el Código de Ética Institucional, de la Investigación y el Aprendizaje, en las Políticas de Protección de Datos Personales, en el Reglamento sobre Inteligencia Artificial y en los demás reglamentos internos.

QUINTA. - La Universidad Metropolitana incluirá, en sus contratos laborales, contratos de servicios profesionales, convenios, acuerdos de pasantía, contratos con proveedores y demás instrumentos jurídicos, cláusulas expresas de protección de la información, confidencialidad reforzada, deber perpetuo de protección de los datos personales y obligaciones de seguridad, en términos compatibles con este Reglamento.

La ausencia de tales cláusulas no afectará la exigibilidad de las obligaciones, que derivan directamente del presente Reglamento y del ordenamiento jurídico aplicable.

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

Corresponderá al Consejo Académico Superior, en su calidad de intérprete máximo y auténtico del Estatuto, reglamentos y demás normativa interna de la Universidad Metropolitana, resolver de manera definitiva las controversias interpretativas que sean sometidas a su conocimiento.

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

OCTAVA. - Sin perjuicio del régimen general de responsabilidad de la Universidad Metropolitana como responsable del tratamiento, los integrantes de la Comunidad Universitaria responderán personalmente, en el ámbito ético, disciplinario, civil, administrativo o penal según corresponda, por el uso indebido de la información institucional o de los datos personales. Las acciones institucionales se ejercerán sin perjuicio de las acciones que correspondan a los titulares de los datos.

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

NOVENA. La distribución general de responsabilidades en materia de privacidad, protección de datos personales, seguridad de la información y ciberseguridad se efectuará conforme a una Matriz de Responsabilidades que se anexa al presente Reglamento como parte integrante de él, elaborada con arreglo a la estructura orgánico-funcional vigente, al Reglamento General al Estatuto y a la Política de Protección de Datos Personales aprobada.

La Matriz identifica, respecto de cada función, la autoridad, dirección, unidad o responsable funcional a cargo —en particular el Vicerrectorado Administrativo, la Dirección de Tecnologías Informáticas, el Especialista en Cumplimiento, el Delegado de Protección de Datos Personales, la Procuraduría Nacional, la Secretaría General Técnica y los custodios funcionales—, sin crear competencias nuevas, ni desplazar las ya previstas en el orgánico funcional. El Comité Institucional propondrá sus actualizaciones, conforme al trámite institucional correspondiente.

DÉCIMA. La UMET, en ejercicio de su interés legítimo institucional de proteger sus activos de información, datos personales, información confidencial, propiedad intelectual, continuidad operativa, seguridad de la información y responsabilidad frente a titulares, autoridades de control y terceros, podrá implementar mecanismos proporcionales de control, monitoreo, trazabilidad, auditoría y prevención de fuga de información respecto de los equipos, cuentas, plataformas, sistemas, redes, repositorios, aplicaciones, servicios tecnológicos y entornos digitales institucionales asignados, administrados, financiados, autorizados o puestos a disposición de los miembros de la Comunidad Universitaria.

Cuando un trabajador, docente, servidor, directivo, contratista, proveedor o colaborador utilice dispositivos personales para acceder, almacenar, descargar, transmitir, procesar o custodiar información institucional, datos personales o activos de información de la Universidad, la institución podrá exigir medidas razonables y proporcionadas de seguridad, tales como autenticación reforzada, cifrado, gestión de accesos, separación lógica de información institucional, instalación de perfiles o contenedores corporativos, herramientas de prevención de pérdida de datos, bloqueo remoto del acceso institucional, eliminación remota exclusivamente de información institucional y registro de eventos vinculados al acceso a sistemas o información de la Universidad.

La aplicación de estos controles deberá sujetarse a los principios de legalidad, legitimidad, transparencia, finalidad determinada, minimización, proporcionalidad, necesidad, seguridad, confidencialidad, privacidad desde el diseño, privacidad por defecto, responsabilidad proactiva y enfoque basado en riesgos. En ningún caso los mecanismos institucionales podrán habilitar el acceso general, permanente o indiscriminado al contenido privado del dispositivo personal del trabajador o colaborador,

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

incluyendo comunicaciones personales, fotografías, archivos privados, redes sociales, geolocalización no vinculada a la finalidad institucional, micrófono, cámara, historial de navegación personal o cualquier otra información ajena a la relación laboral, contractual, académica o institucional.

Previo a la implementación de controles tecnológicos que puedan incidir en derechos de privacidad, intimidad, protección de datos personales o secreto de las comunicaciones, la Universidad deberá realizar un análisis de interés legítimo, necesidad y proporcionalidad y, cuando corresponda por el nivel de riesgo, una evaluación de impacto en protección de datos personales y seguridad de la información. Dicho análisis deberá documentar la finalidad perseguida, los activos protegidos, los riesgos identificados, las alternativas menos invasivas consideradas, las medidas de mitigación, los plazos de conservación de registros, los perfiles de acceso autorizados y los mecanismos de supervisión institucional.

La Universidad deberá informar previamente a los trabajadores, docentes, servidores, directivos, contratistas, proveedores y colaboradores sobre la existencia, naturaleza, finalidad, alcance, límites y consecuencias de los controles institucionales de seguridad de la información, así como sobre los canales disponibles para consultas, reclamos o ejercicio de derechos en materia de protección de datos personales.

Los controles previstos en esta disposición se aplicarán sin perjuicio de las obligaciones de confidencialidad, reserva, protección de datos personales, seguridad de la información y uso adecuado de recursos institucionales previstas en la Ley Orgánica de Protección de Datos Personales, su Reglamento General, la normativa secundaria de la Superintendencia de Protección de Datos Personales, el Reglamento Interno de Trabajo, los contratos, convenios, acuerdos de confidencialidad y demás normativa interna aplicable.

DÉCIMA PRIMERA. La Universidad no podrá realizar vigilancia masiva, intrusiva, secreta, permanente o indiscriminada sobre dispositivos personales, comunicaciones privadas, ubicación, imágenes, audios, archivos personales o actividades digitales no vinculadas con finalidades institucionales legítimas, salvo requerimiento de autoridad competente o habilitación expresa del ordenamiento jurídico aplicable.

La protección de la información institucional no autoriza, por sí sola, el acceso al contenido privado de los dispositivos personales de los trabajadores o colaboradores. Toda medida de control deberá limitarse estrictamente a los sistemas, cuentas, accesos, registros, aplicaciones, contenedores, archivos o información institucional involucrada, conforme a criterios de necesidad, proporcionalidad, trazabilidad y mínima intervención.

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

DÉCIMA SEGUNDA. El acceso a sistemas, cuentas, aplicaciones, redes o información institucional desde dispositivos personales estará condicionado al cumplimiento de las medidas de seguridad, autenticación, configuración y protección definidas por la Dirección de Tecnologías Informáticas.

Cuando resulte necesario verificar el cumplimiento de dichas medidas, la revisión se limitará exclusivamente al entorno, cuenta, aplicación, perfil o contenedor institucional utilizado en el dispositivo, sin que pueda extenderse a archivos, comunicaciones, cuentas, aplicaciones o contenidos de carácter personal ajenos a la actividad universitaria. La verificación deberá ser realizada por personal autorizado, con información previa al usuario, alcance definido, respeto a los principios de necesidad, proporcionalidad y minimización y constancia documentada de la actuación.

La Universidad no podrá exigir la entrega indiscriminada del dispositivo personal ni acceder a información privada no vinculada con los recursos institucionales. Cuando no sea posible efectuar una verificación técnicamente limitada o cuando el usuario no consienta el control del entorno institucional, la Universidad podrá restringir o suspender el acceso desde dicho dispositivo y, cuando corresponda, proporcionar o autorizar un medio institucional alternativo. La negativa a someter el dispositivo personal a una revisión general no constituirá por sí sola infracción, sin perjuicio de las responsabilidades que pudieren derivarse del uso indebido de recursos institucionales, de la vulneración de medidas de seguridad o del incumplimiento de obligaciones expresamente establecidas en este Reglamento.

DÉCIMA TERCERA. Toda persona que mantenga o haya mantenido vínculo laboral, académico, administrativo, contractual, profesional, civil, mercantil, investigativo, de cooperación, pasantía, prácticas, consultoría, prestación de servicios o cualquier otra relación institucional con la Universidad Metropolitana deberá proteger, custodiar, reservar y no divulgar la información institucional a la que acceda por razón de sus funciones, encargos, actividades, relaciones o autorizaciones, aun cuando no exista cláusula expresa de confidencialidad en el instrumento que regule su vínculo.

Este deber comprende la información confidencial, sensible, reservada, estratégica, académica, investigativa, administrativa, financiera, jurídica, técnica, tecnológica, comercial, operativa, disciplinaria, contractual, de seguridad y de propiedad intelectual, así como secretos institucionales o empresariales, datos personales, datos sensibles, bases de datos, credenciales, documentos internos, informes, proyectos, modelos, algoritmos, códigos, metodologías, planes, indicadores, evaluaciones, expedientes, comunicaciones institucionales y cualquier otra información que deba ser protegida por su naturaleza, finalidad, riesgo, valor institucional o nivel de clasificación.

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

La ausencia de una cláusula contractual específica no exime del cumplimiento de este deber, por cuanto la obligación de confidencialidad, reserva, lealtad, custodia, seguridad de la información, protección de datos personales y prohibición de aprovechamiento indebido deriva del ordenamiento jurídico aplicable, del presente Reglamento, del Reglamento Interno de Trabajo, del Código de Ética Institucional, de la buena fe contractual, de la naturaleza del vínculo institucional y de la responsabilidad de proteger los activos de información de la Universidad.

DÉCIMA CUARTA. Respecto de la información institucional confidencial, reservada, estratégica, técnica, comercial, investigativa, académica, operativa o financiera, el deber de reserva subsistirá mientras conserve tal carácter y, en todo caso, por un plazo mínimo de diez años contados desde la terminación del vínculo con la Institución, salvo que la ley, el contrato, una resolución institucional, la naturaleza de la información o una decisión de autoridad competente establezcan un plazo mayor.

Durante dicho plazo, la persona obligada no podrá utilizar, explotar, reproducir, transferir, comunicar, divulgar, vender, ceder, publicar, cargar en sistemas externos, incorporar en herramientas de inteligencia artificial, entregar a terceros ni aprovechar en beneficio propio o ajeno la información institucional protegida. Esta prohibición no impedirá el libre ejercicio del trabajo, profesión, docencia, investigación o actividad económica lícita, siempre que no implique uso, revelación, explotación, apropiación o aprovechamiento de información protegida de la Universidad.

El incumplimiento de esta disposición constituirá infracción muy grave, según la naturaleza de la información, el daño causado, el riesgo generado, la intencionalidad, la reincidencia, el beneficio obtenido y la afectación institucional. Podrá dar lugar a responsabilidades laborales, disciplinarias, contractuales, civiles, administrativas o penales, incluida la solicitud de visto bueno cuando corresponda. La Universidad podrá exigir la devolución, eliminación, bloqueo, cesación de uso, reparación integral, indemnización de daños y perjuicios y las demás medidas administrativas, judiciales o extrajudiciales que resulten procedentes.

DÉCIMA QUINTA. Toda persona que mantenga o haya mantenido vínculo laboral, académico, administrativo, contractual, profesional, civil, mercantil, investigativo, de cooperación, pasantía, prácticas, consultoría, prestación de servicios o cualquier otra relación institucional con la Universidad Metropolitana estará obligada a guardar reserva y proteger los datos personales y datos personales sensibles a los que acceda, conozca, trate o administre por razón de sus funciones, actividades, encargos, autorizaciones o relación con la Universidad. Este deber es perpetuo, permanente, indefinido, irrenunciable, intransferible y exigible sin necesidad de cláusula expresa de

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

confidencialidad, reserva o protección de datos en el contrato, nombramiento, convenio, acta, encargo, compromiso o instrumento equivalente.

La obligación comprende la prohibición de divulgar, comunicar, publicar, transferir, ceder, reproducir, conservar indebidamente, utilizar para fines no autorizados, cargar en sistemas externos o incorporar en herramientas de inteligencia artificial datos personales o sensibles tratados por la Universidad, salvo habilitación legal, contractual o institucional expresa. La terminación del vínculo con la Universidad no extingue este deber, sin perjuicio de las responsabilidades laborales, disciplinarias, contractuales, civiles, administrativas o penales que correspondan por su incumplimiento.

DÉCIMA SEXTA. - La Dirección de Tecnologías Informáticas, en coordinación con la Unidad de Talento Humano, planificará y ejecutará al menos una vez al año una capacitación obligatoria dirigida al personal académico, administrativo y de apoyo de la Universidad sobre seguridad de la información y ciberseguridad. La capacitación deberá comprender, al menos, identificación y prevención de intentos de *phishing*, suplantación de identidad, ingeniería social, obtención fraudulenta de credenciales, enlaces y archivos maliciosos, accesos no autorizados, uso seguro de cuentas y dispositivos, protección de información institucional y reporte oportuno de incidentes. La Unidad de Talento Humano incorporará esta actividad en el plan anual de capacitación, llevará el registro de asistencia y conservará las evidencias de cumplimiento. Por su parte, la Dirección de Tecnologías Informáticas actualizará periódicamente los contenidos conforme a los riesgos identificados, las amenazas emergentes y las necesidades institucionales.

DÉCIMA SÉPTIMA. El presente Reglamento prevalece sobre cualquier instrumento normativo interno de igual o inferior jerarquía que regule las materias aquí tratadas, sin perjuicio del carácter especial de las disposiciones contenidas en el Reglamento sobre Inteligencia Artificial respecto de las cuestiones específicas de inteligencia artificial.

DÉCIMA OCTAVA. La participación del Delegado de Protección de Datos Personales en los procedimientos, proyectos, contratos, evaluaciones, incidentes y demás actuaciones institucionales tendrá carácter de asesoría, supervisión, alerta y recomendación técnica especializada. La intervención del Delegado no sustituirá las decisiones del responsable del tratamiento ni las funciones operativas, administrativas, tecnológicas, documentales o jurídicas atribuidas a las unidades competentes.

Las unidades responsables deberán proporcionar al Delegado acceso oportuno a la información necesaria para el cumplimiento de sus funciones y documentar la consideración de sus recomendaciones. Cuando una recomendación no sea acogida, la autoridad o unidad competente deberá dejar constancia motivada de su decisión.

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

DISPOSICIONES TRANSITORIAS

PRIMERA. - En el plazo máximo de noventa (90) días contados a partir de la aprobación del presente Reglamento, el CIPPIA deberá instalar su primera sesión con la integración prevista en este Reglamento.

En dicha sesión se conocerá la formalización, la emisión de sus instrumentos internos de funcionamiento y la incorporación expresa de las funciones adicionales previstas en este Reglamento.

SEGUNDA. - En el plazo máximo de ciento ochenta (180) días contados desde la aprobación del presente Reglamento, el Consejo Académico Superior aprobará, mediante resolución, la **Política Institucional de Seguridad de la Información**, la **Política Institucional de Privacidad** y los lineamientos generales para la implementación del Sistema Institucional de Protección de la Privacidad, la Información y los Datos Personales, de conformidad con este Reglamento, el Reglamento General al Estatuto y las normas técnicas internacionales aplicables.

La Política Institucional de Privacidad será un instrumento distinto y complementario de la Política de Protección de Datos Personales, aprobada mediante **Resolución No. 81-UMET-CAS-SO-09-2025**, a la cual no sustituirá, ni dejará sin efecto. La Política de Protección de Datos Personales continuará regulando específicamente el tratamiento de datos personales, las bases de legitimación, los derechos de los titulares, las responsabilidades del responsable y de los encargados del tratamiento, las transferencias, los plazos de conservación, las medidas de seguridad y los demás aspectos sujetos a la Ley Orgánica de Protección de Datos Personales y su normativa de desarrollo.

La Política Institucional de Privacidad tendrá un ámbito más amplio y regulará la protección de la vida privada y de la intimidad en el entorno universitario, incluida la confidencialidad de las comunicaciones, el uso de dispositivos y cuentas institucionales, la videovigilancia, el control y monitoreo tecnológico, la protección de la imagen, la privacidad en entornos académicos, laborales y digitales, la reserva de la información institucional y los límites a la observación, registro o seguimiento de las actividades de los integrantes de la comunidad universitaria.

La propia Política Institucional de Privacidad deberá desarrollar, precisar y estructurar su ámbito material y subjetivo, su relación de complementariedad con la Política de Protección de Datos Personales y con la Política Institucional de Seguridad de la Información, así como las reglas para resolver posibles superposiciones, evitar duplicidades y asegurar una aplicación armónica de los tres instrumentos.

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

TERCERA. - En el plazo máximo de tres (3) meses contados a partir de la aprobación del presente Reglamento, el Comité Institucional, en coordinación con el Vicerrectorado Administrativo, el Delegado de Protección de Datos Personales y la Dirección de Tecnologías Informáticas, levantará el primer Inventario Institucional de Activos de Información, definirá la metodología de gestión de riesgos institucionales y aprobará el primer programa de auditoría interna.

CUARTA. - La Universidad Metropolitana iniciará, dentro del plazo máximo de doce (12) meses contados a partir de la aprobación del presente Reglamento, las acciones preparatorias para la certificación bajo la norma ISO/IEC 27001:2022. La obtención de la primera certificación se procurará dentro de un plazo no mayor a treinta y seis (36) meses contados desde la aprobación de este Reglamento, conforme al plan progresivo que apruebe el Rector. Una vez obtenida, se implementarán las acciones necesarias para su mantenimiento permanente.

QUINTA. - Dentro de los plazos indicativos posteriores, el Rector dispondrá las acciones necesarias para la obtención de la certificación bajo las normas ISO/IEC 27701, ISO/IEC 42001 y demás normas técnicas pertinentes, atendiendo al avance institucional, a la disponibilidad presupuestaria y a las prioridades estratégicas de la Universidad. Los plazos específicos serán definidos en el plan progresivo correspondiente.

SEXTA. - En el plazo máximo de ciento ochenta (180) días contados desde la entrada en vigencia del presente Reglamento, las unidades competentes elaborarán y someterán a aprobación los instrumentos operativos estrictamente necesarios para su aplicación, evitando duplicidades, superposición normativa y proliferación de documentos secundarios.

Como mínimo, deberán elaborarse los siguientes instrumentos:

a) La Matriz de Clasificación y Acceso a la Información, con identificación de niveles de acceso, responsables funcionales, perfiles autorizados, plazos de conservación y criterios de revisión o desclasificación;

b) La Matriz de Responsabilidades, en la que se determine, conforme a la estructura orgánico-funcional vigente, qué autoridad, dirección, unidad o responsable interviene en cada función de ejecución, coordinación, supervisión, consulta o información;

c) El procedimiento para la atención de derechos de los titulares de datos personales, con definición de responsables, plazos, trazabilidad, mecanismos de respuesta y conservación de evidencias;

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

d) El procedimiento institucional para la gestión y notificación de incidentes de seguridad y vulneraciones de datos personales, incluidos los canales de reporte, responsables de análisis, medidas de contención, preservación de evidencias y escalamiento;

e) El inventario de activos de información y el Registro de Actividades de Tratamiento, con sus respectivos responsables de actualización, custodia y revisión; y,

f) Las cláusulas contractuales mínimas en materia de confidencialidad, seguridad de la información, protección de datos personales, uso de servicios en la nube, subcontratación, devolución o eliminación de información y gestión de incidentes.

La elaboración de manuales, instructivos, formularios, guías, protocolos o plantillas adicionales solo procederá cuando exista una necesidad operativa concreta, debidamente justificada por la unidad competente y siempre que su contenido no pueda incorporarse en alguno de los instrumentos señalados en esta disposición. Dichos documentos no podrán crear obligaciones, competencias, procedimientos o sanciones no previstos en la ley, el presente Reglamento o la normativa institucional superior.

SÉPTIMA. - En el plazo máximo de doce (12) meses contados desde la entrada en vigencia del presente Reglamento, las unidades competentes, bajo la coordinación del Vicerrectorado Administrativo y con el apoyo de la Procuraduría Nacional, la Dirección de Tecnologías Informáticas, el Delegado de Protección de Datos Personales y el Especialista en Cumplimiento, revisarán progresivamente los contratos, convenios, licencias, órdenes de servicio y demás instrumentos vigentes celebrados con proveedores, encargados del tratamiento y terceros que accedan, custodien, alojen, procesen, transfieran o administren información institucional o datos personales.

La revisión se ejecutará conforme a criterios de prioridad y riesgo, atendiendo especialmente a: a) proveedores que traten datos personales o datos sensibles; b) servicios en la nube, almacenamiento, alojamiento o respaldo de información; c) sistemas críticos para la operación institucional; d) plataformas que incorporen inteligencia artificial o decisiones automatizadas; e) contratos próximos a renovación, ampliación o terminación; f) tratamientos a gran escala o de alto riesgo; y g) servicios que impliquen transferencias nacionales o internacionales de información.

Como resultado de la revisión, deberán identificarse y corregirse, según corresponda, las deficiencias relativas a confidencialidad, seguridad de la información, protección de datos personales, subcontratación, transferencias, gestión de incidentes, devolución o eliminación de información, continuidad del servicio, auditoría, trazabilidad y terminación contractual. Las adecuaciones podrán instrumentarse mediante adendas, cláusulas complementarias, nuevos acuerdos de tratamiento, planes de regularización o,

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

cuando no sea jurídicamente viable mantener la relación, mediante la terminación o no renovación del instrumento.

La revisión deberá ejecutarse por fases. Dentro de los primeros ciento ochenta (180) días se atenderán los contratos de mayor riesgo o criticidad. Los restantes instrumentos deberán revisarse dentro del plazo total previsto en esta disposición. El Especialista en Cumplimiento realizará el seguimiento de avance y emitirá reportes trimestrales, sin sustituir las competencias operativas, técnicas, jurídicas o administrativas de las unidades responsables.

OCTAVA. - Los procedimientos, procesos, contrataciones y tratamientos en curso a la fecha de aprobación del presente Reglamento continuarán su trámite conforme a las disposiciones vigentes al momento de su inicio, sin perjuicio de su adecuación progresiva a las exigencias de este Reglamento dentro de los planes de regularización que apruebe el Comité Institucional.

NOVENA. - Hasta tanto se expidan las guías, directrices y demás instrumentos complementarios previstos en este Reglamento, sus disposiciones se interpretarán y aplicarán en consonancia con la Ley Orgánica de Protección de Datos Personales, su Reglamento General, la normativa secundaria de la Superintendencia de Protección de Datos Personales, el Código de Ética Institucional, de la Investigación y el Aprendizaje, las Políticas de Protección de Datos Personales y el Reglamento sobre Inteligencia Artificial.

DÉCIMA.- En el plazo máximo de ciento ochenta (180) días contados desde la entrada en vigencia del presente Reglamento, la Dirección de Tecnologías Informáticas, en coordinación con la Unidad de Talento Humano, diseñará, aprobará e implementará el primer programa institucional obligatorio de capacitación en seguridad de la información, ciberseguridad, protección de datos personales y reporte de incidentes, de conformidad con el artículo 55 y la Disposición General Décima Sexta de este Reglamento.

El programa deberá comprender, al menos, contenidos sobre identificación y prevención de *phishing*, suplantación de identidad, ingeniería social, obtención fraudulenta de credenciales, enlaces y archivos maliciosos, accesos no autorizados, uso seguro de cuentas y dispositivos, protección de información institucional, tratamiento seguro de datos personales y reporte oportuno de incidentes, vulnerabilidades, brechas o sospechas de afectación.

La Unidad de Talento Humano incorporará esta actividad en el plan anual de capacitación institucional, determinará los grupos obligados, administrará las convocatorias, registrará la asistencia y conservará las evidencias de cumplimiento. La Dirección de Tecnologías Informáticas elaborará y actualizará los contenidos técnicos,

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

impartirá o coordinará la capacitación y habilitará los canales institucionales para el reporte y atención de incidentes.

El Especialista en Cumplimiento verificará la ejecución del programa y emitirá el informe de seguimiento correspondiente, sin asumir funciones operativas de capacitación. Cuando el contenido involucre protección de datos personales, se contará con la asesoría del Delegado de Protección de Datos Personales. Cumplida esta primera implementación, la capacitación se ejecutará al menos una vez por año y se actualizará conforme a los riesgos identificados, las amenazas emergentes y las necesidades institucionales.

DÉCIMA PRIMERA. En el plazo máximo de seis (6) meses contados desde la entrada en vigencia del presente Reglamento, la Unidad 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 como infracción muy grave tanto el incumplimiento de los deberes de confidencialidad, reserva, protección de datos personales, seguridad de la información, ciberseguridad y reporte de incidentes como la comisión de cualquiera de las infracciones previstas en el presente Reglamento y en el Reglamento institucional sobre uso de inteligencia artificial.

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.

DÉCIMA SEGUNDA. Dentro del plazo improrrogable de seis (6) meses contados a partir de la entrada en vigencia del presente Reglamento, el CIPPIA elaborará y presentará, para conocimiento y aprobación del Consejo de Regentes y del Consejo Académico Superior (CAS), el *Plan de Implementación del Sistema de Gestión de Protección de la Privacidad, de la Información y de los Datos Personales de la Universidad Metropolitana* (en adelante, el «Plan»).

El Plan se concibe como instrumento de planificación plurianual, vivo y verificable, sujeto al ciclo de mejora continua, y deberá guardar conformidad con la Ley Orgánica de Protección de Datos Personales, su Reglamento General de aplicación, las resoluciones y guías expedidas por la Superintendencia de Protección de Datos Personales —en particular la normativa sobre gestión de riesgos y evaluación de impacto, tratamiento a gran escala, inteligencia artificial e interés legítimo— y los estándares técnicos internacionalmente reconocidos que el CIPPIA adopte de manera motivada. Su diseño observará el principio de proporcionalidad, atendiendo a la naturaleza de la Universidad como institución de educación superior que trata categorías especiales de

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

datos —entre ellas, datos de salud, datos de personas en situación de vulnerabilidad y datos de menores de edad— y a su autonomía responsable consagrada en el ordenamiento jurídico.

El Plan contendrá, como mínimo, los siguientes componentes:

1. Diagnóstico y línea base. — Análisis de brecha (GAP) entre el estado actual de la Universidad y las obligaciones legales, reglamentarias y de los estándares adoptados, con determinación del nivel de madurez por dominio. — Levantamiento o actualización del Registro de Actividades de Tratamiento (RAT), conforme a los campos exigidos por el Reglamento General de la Ley y por las resoluciones sobre tratamiento a gran escala e inteligencia artificial, como insumo fundacional de todo el Sistema. — Inventario de activos de información que soportan datos personales y mapeo de los flujos de datos, incluidas las transferencias y el acceso por terceros.

2. Gobernanza, estructura y asignación de responsabilidades. — Definición funcional de los roles del Delegado de Protección de Datos (DPO), del responsable funcional de seguridad de la información de la Dirección de Tecnologías Informáticas, de los dueños de los tratamientos y de las áreas operativas, conforme al modelo de las tres líneas de defensa, preservando la independencia del DPD y evitando conflictos de interés en su actuación. — Matriz de responsabilidades (RACI) por proceso y por tratamiento, de modo que la rendición de cuentas no se diluya y cada unidad académica o administrativa asuma la responsabilidad proactiva y demostrada sobre los tratamientos de su competencia. — Reglas de funcionamiento, convocatoria, cadencia y registro de decisiones del CIPPIA como órgano de gobierno y escalamiento del Sistema.

3. Planificación operativa. — Definición del alcance (unidades, procesos, sistemas, ubicaciones y terceros) y de objetivos específicos, medibles y verificables, descartando enunciados genéricos. — Plan Operativo Anual (POA) articulado bajo el ciclo planificar–hacer–verificar–actuar (PHVA), con implementación escalonada por fases (corto, mediano y largo plazo), cronograma e hitos. — Estimación de los recursos humanos, tecnológicos y presupuestarios necesarios, con la previsión de su provisión por la autoridad institucional como condición de viabilidad del Sistema.

4. Gestión documental. — Elaboración, numeración, versionamiento y consolidación en repositorio institucional de las políticas, procedimientos, avisos de privacidad, cláusulas y demás instrumentos del Sistema. — Política de conservación, bloqueo, anonimización y eliminación segura, con plazos vinculados a los términos legales de conservación y de prescripción aplicables. — Criterios de clasificación de la información y de trazabilidad documental que permitan demostrar el cumplimiento ante la autoridad de control.

5. Gestión de riesgos y evaluación de impacto. — Desarrollo de una **metodología propia** de gestión de riesgos de protección de datos personales —no una mera transcripción de directrices—, que satisfaga obligatoriamente los principios del Capítulo 1 de la Guía expedida por la Superintendencia y que documente el proceso en sus cinco etapas: establecimiento del contexto, identificación, análisis, evaluación de impacto y tratamiento del riesgo. — Determinación de criterios de probabilidad e impacto, niveles de severidad, métodos de análisis (cualitativos, cuantitativos o híbridos) elegidos según la disponibilidad de datos, y exigencia de justificación documentada (rational) de toda estimación. — Reconocimiento de que el objeto de protección son los derechos y libertades de los titulares, de modo que el apetito de riesgo que fije la autoridad institucional jamás podrá comprender la aceptación de una vulneración de tales derechos, cuya garantía se procurará al máximo conforme al principio de proporcionalidad. — Realización de las Evaluaciones de Impacto al Tratamiento (EIT) que correspondan, en su carácter de obligación legal, precedidas necesariamente de las etapas de contexto, identificación y análisis.

6. Medidas de seguridad y controles. — Definición de controles técnicos (entre otros, autenticación multifactor, cifrado, registro y trazabilidad de accesos, segmentación, respaldos probados y gestión de vulnerabilidades), organizativos y jurídicos, seleccionados a partir de los resultados del análisis de riesgo y de la EIPD, y no como catálogo desvinculado de aquellos. — Incorporación de la privacidad desde el diseño y por defecto en todo desarrollo, adquisición o contratación de sistemas y servicios que impliquen tratamiento de datos personales.

7. Derechos de los titulares. — Procedimiento de atención de los derechos de acceso, rectificación, actualización, eliminación, oposición, portabilidad y los demás reconocidos por la Ley, con canales visibles, verificación de identidad y plazos de respuesta medibles.

8. Gestión de incidentes y vulneraciones de seguridad. — Procedimiento y guías de actuación (*playbooks*) para la detección, contención, evaluación, notificación y remediación de incidentes, con observancia estricta de los plazos legales de notificación a la autoridad de control y a los titulares afectados. — Programa de simulacros y pruebas periódicas que verifiquen la capacidad de respuesta y su articulación con la continuidad de las actividades institucionales.

9. Encargados del tratamiento y transferencias internacionales. — Proceso de debida diligencia y de suscripción de acuerdos de tratamiento de datos (DPA) con encargados y subencargados, con cláusulas y medidas verificables. — Identificación de las transferencias internacionales, evaluación de las garantías aplicables, documentación de la evaluación de transferencia y registro correspondiente.

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

10. Formación, concienciación y cultura. — Plan de formación diferenciado por roles y plan de concienciación institucional, con métricas de cobertura y de eficacia, observando las limitaciones aplicables a la capacitación de terceros. — Capacitación continua del Delegado de Protección de Datos, con la provisión de los recursos necesarios para su actualización profesional.

11. Monitoreo, métricas, auditoría y mejora continua. — Sistema de indicadores de desempeño (KPI) y de riesgo (KRI), con tablero de reportería al CIPPIA y a la autoridad institucional, y umbrales y cadencias definidos. — Programa de auditorías internas independientes del Sistema, gestión de no conformidades con análisis de causa raíz, y mecanismos de mejora continua que retroalimenten el ciclo de planificación. — Preparación permanente para los procesos de control de la Superintendencia, incluyendo la organización de la evidencia y la designación de un interlocutor institucional único.

12. Cronograma, presupuesto e indicadores de cumplimiento del propio Plan. — Cronograma general con responsables, plazos y criterios objetivos de cierre por cada componente. — Presupuesto plurianual estimado y fuentes de financiamiento.

Una vez aprobado por el Consejo de Regentes y por el Consejo Académico Superior, el Plan adquirirá carácter vinculante para todas las unidades académicas y administrativas de la Universidad, se integrará a la planificación operativa institucional y será objeto de revisión y actualización, al menos, con periodicidad anual, así como ante cualquier cambio normativo, organizacional o tecnológico relevante que altere el contexto del tratamiento. El CIPPIA informará semestralmente al Consejo de Regentes y al Consejo Académico Superior sobre el grado de avance en la ejecución del Plan.

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 específicas del Código de Ética Institucional, de la Investigación y el Aprendizaje, de las Políticas de Protección de Datos Personales y del Reglamento para el Uso Ético, Responsable y Seguro de la Inteligencia Artificial, 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.

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

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

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ALEJANDRO RAFAEL
SOCORRO CASTRO

Ing. Alejandro Rafael Socorro Castro, PhD.

RECTOR Y PRESIDENTE DEL CONSEJO ACADÉMICO SUPERIOR

UNIVERSIDAD METROPOLITANA

Lo certifico:

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
AUGUSTO ANDRES
CUEVA GAIBOR

Abg. Augusto Andrés Cueva Gaibor, Mgs.

SECRETARIO GENERAL TÉCNICO

UNIVERSIDAD METROPOLITANA

Matriz Guayaquil: Campus FCEE, Cdla. La Garzota 1era etapa Mz. 23. Teléfonos: (04) 6038282 / (04) 6026609 / 09894172578.
Campus principal Quito: Campus Coruña, La Coruña N26-95 y San Ignacio. Teléfonos: (04) 6026608 – (04) 6026609
Sede Machala: Campus Junín, Calle Bolívar 609 entre Junín y Tarqui. Teléfonos: (07) 2923635 / (07) 293286.

ANEXO ÚNICO

MATRIZ DE RESPONSABILIDADES EN MATERIA DE PRIVACIDAD, PROTECCIÓN DE DATOS PERSONALES, SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Fundamento. La presente Matriz de Responsabilidades se expide en cumplimiento de la Disposición General Novena del Reglamento para la Protección de la Privacidad, de la Información y de los Datos Personales de la Universidad Metropolitana, conforme a la cual la distribución general de responsabilidades en materia de privacidad, protección de datos personales, seguridad de la información y ciberseguridad se efectúa mediante una Matriz que se anexa al Reglamento como parte integrante de él. Se elabora con arreglo a la estructura orgánico-funcional vigente, al Estatuto Institucional, al Reglamento General al Estatuto y a la Política de Protección de Datos Personales aprobada, y se articula con el Reglamento para el Uso Ético, Responsable y Seguro de la Inteligencia Artificial.

Naturaleza y alcance. La Matriz identifica, respecto de cada función, la autoridad, dirección, unidad o responsable funcional a cargo. No crea competencias nuevas ni desplaza las ya previstas en el orgánico funcional; se limita a ordenar y hacer trazable la distribución de funciones existentes. En todo caso, la responsabilidad de la Universidad Metropolitana como responsable del tratamiento, frente a los titulares, la sociedad y el Estado, es indelegable, y las competencias propias de cada órgano y autoridad se ejercen sin perjuicio de lo aquí ordenado. El Delegado de Protección de Datos Personales ejercerá funciones de asesoría, supervisión, alerta y recomendación, sin asumir la ejecución material ni la decisión de los procesos que deba supervisar. El Especialista en Cumplimiento realizará seguimiento y verificación, sin auditar procesos en cuya ejecución haya intervenido.

Metodología (RACI). Para cada función se identifica: (R) Responsable de ejecución, quien realiza materialmente la actividad; (A) quien aprueba o rinde cuentas, con autoridad para validar y responder por el resultado; (C) quien es consultado o coordina; e (I) quien es informado. En coherencia con la independencia funcional del Delegado de Protección de Datos Personales, este no ejecuta las actividades operativas que luego le corresponde supervisar, por lo que figura como asesor, supervisor o emisor de recomendación. El Especialista en Cumplimiento coordina el programa de auditoría y da seguimiento al cierre de hallazgos, pero no audita procesos en cuya ejecución haya intervenido. El Comité Institucional (CIPPIA) coordina, propone, recomienda, emite criterio técnico y da seguimiento, sin asumir competencias aprobatorias que corresponden al Rector, al Vicerrectorado Administrativo, al Consejo de Regentes o al Consejo Académico Superior. La intervención de la Procuraduría Nacional tiene, en todos los casos, carácter de criterio jurídico no vinculante y se circunscribe a requerimientos jurídicos, contestaciones formales, procedimientos sancionadores, interpretación normativa o defensa institucional.

Glosario de actores.

Sigla	Autoridad, dirección, unidad o responsable funcional
CAS	Consejo Académico Superior
CR	Consejo de Regentes
Rector	Rector y representante legal
VAD	Vicerrectorado Administrativo (Responsable interno del tratamiento)
VAC	Vicerrectorado Académico
CIPPIA	Comité Institucional de Protección de la Privacidad, la Información, los Datos Personales y de Uso Ético de la IA
DPO	Delegado de Protección de Datos Personales
DTI	Dirección de Tecnologías Informáticas
EC	Especialista en Cumplimiento
PN	Procuraduría Nacional
SGT	Secretaría General Técnica
CUE	Comité Universitario de Ética y Subcomités de Sede
Custodios funcionales	Decanos, directores de escuela, coordinadores de carrera, directores departamentales o de sede y responsables operativos de los activos de información
Comunidad	Comunidad Universitaria (usuarios en general)

Matriz de responsabilidades.

Nº	Función	Responsable de ejecución (R)	Aprueba / rinde cuentas (A)	Consultado / coordina (C)	Informado (I)
A. Gobernanza y dirección del Sistema Institucional (SIPPID)					
1	Aprobación y reforma de reglamentos, políticas e instrumentos normativos del SIPPID	VAD / unidad requirente, con propuesta del CIPPIA	CAS	CR (informe favorable); PN; CIPPIA	Rector; Comunidad
2	Aprobación de la Política de Seguridad de la Información y de la Política de Privacidad	VAD, con propuesta del CIPPIA	CR y CAS, según el trámite institucional	DPO; DTI; EC; PN	Rector; Comunidad

Nº	Función	Responsable de ejecución (R)	Aprueba / rinde cuentas (A)	Consultado / coordina (C)	Informado (I)
3	Coordinación institucional general del cumplimiento (Responsable interno del Tratamiento)	VAD	Rector	CIPPIA; DPO; DTI; EC	CAS
4	Articulación y coordinación entre los componentes del SIPPID	CIPPIA	VAD	DPO; DTI; EC; PN; SGT	Rector
5	Informe anual integrado de seguimiento del SIPPID	CIPPIA	Rector / CAS	DPO; DTI; EC	CR
6	Absolución de consultas e interpretación normativa	PN (criterio jurídico, no vinculante)	CAS (intérprete máximo)	CIPPIA (técnico); CUE (ético); DPO	VAD
B. Protección de datos personales					
7	Calidad de responsable del tratamiento y gestión funcional de responsabilidades	VAD (gestión funcional)	Rector	DPO; PN	CAS
8	Elaboración, actualización y consolidación del Registro de Actividades de Tratamiento (RAT)	Unidades tratantes y custodios funcionales	VAD	DPO; DTI	CIPPIA
9	Atención de los derechos de los titulares	Unidad tratante o custodio funcional competente	VAD	DPO; PN, cuando corresponda	CIPPIA
10	Evaluaciones de Impacto del Tratamiento (EIT)	Área requirente, con apoyo técnico de DTI	VAD	DPO; PN; EC	CIPPIA
11	Determinación de bases jurídicas y obtención del consentimiento	Unidad tratante / custodio funcional	VAD	DPO; PN	—
12	Transferencias y comunicaciones nacionales e internacionales de datos	Unidad tratante o área requirente	VAD	DPO; PN; DTI	CIPPIA
13	Inscripción en el Registro Nacional de Protección de Datos Personales (RNPD)	Unidad administrativa designada por el VAD	VAD	DPO; PN	CIPPIA
14	Relación y reporte con la Superintendencia de Protección de Datos Personales	Unidad administrativa designada por el VAD	VAD / Rector, según corresponda	DPO; PN	CIPPIA
15	Cláusulas contractuales de protección de datos con encargados del tratamiento	PN (revisa)	VAD	Área requirente; DPO; DTI	—
C. Clasificación y gestión de la información institucional					
16	Clasificación de la información institucional	Custodio funcional	Autoridad de la unidad	DPO; DTI; PN; CIPPIA, cuando exista duda técnica	VAD

Nº	Función	Responsable de ejecución (R)	Aprueba / rinde cuentas (A)	Consultado / coordina (C)	Informado (I)
17	Inventario de Activos de Información	DTI	VAD	Custodios funcionales; CIPPIA	—
18	Custodia funcional de los activos de información	Custodios funcionales	Autoridad de la unidad	DTI	—
19	Gestión documental, certificación y archivo	SGT	Rector	Custodios funcionales	—
20	Información reservada y estratégica y deber de reserva	Custodios funcionales	VAD	PN	—
D. Seguridad de la información (SGSI)					
21	Implementación y mantenimiento del SGSI	DTI	VAD	CIPPIA; EC	Rector
22	Análisis y tratamiento de riesgos de información	DTI	VAD	EC; Custodios funcionales	CIPPIA
23	Controles técnicos, organizativos y físicos	DTI	VAD	Custodios funcionales	—
24	Continuidad y recuperación ante desastres (ISO 22301)	DTI	VAD	Custodios funcionales	CIPPIA
25	Gestión de incidentes de seguridad de la información	DTI	VAD	DPO (si afecta datos personales); PN	CIPPIA
26	Notificación de brechas a la autoridad de control y a los titulares	Unidad administrativa designada por el VAD	VAD	DPO; DTI; PN	Rector; CIPPIA
E. Ciberseguridad					
27	Ciberseguridad, protección de infraestructura y monitoreo técnicamente disponible	DTI	VAD	EC	CIPPIA
28	Controles en dispositivos y prevención de fuga de información	DTI	VAD	EC; PN; DPO	Custodios funcionales
29	Gestión de accesos, identidades y privilegios	DTI	VAD	Custodios funcionales	—
F. Inteligencia artificial (articulación con el Reglamento de IA)					
30	Inventario de sistemas de IA y calificación de riesgo	Área requirente, con apoyo de DTI	VAD o autoridad competente	CIPPIA (criterio técnico); DPO; EC	Rector
31	Viabilidad técnica de adquisición o despliegue de sistemas de IA	DTI	VAD / autoridad competente	Área requirente	CIPPIA
32	Revisión jurídica de contratos e instrumentos de IA	PN (no vinculante)	VAD	DTI; DPO	—

Nº	Función	Responsable de ejecución (R)	Aprueba / rinde cuentas (A)	Consultado / coordina (C)	Informado (I)
33	Autorización de adquisición o despliegue de sistemas de IA	Área requirente	Autoridad competente / VAD	CIPPIA; PN; DTI; DPO	CAS (según cuantía)
34	Supervisión humana significativa de decisiones automatizadas	Autoridad o funcionario usuario	Autoridad competente	DPO	CIPPIA
G. Cumplimiento, auditoría y mejora continua					
35	Seguimiento y verificación del cumplimiento normativo	EC	VAD	DPO; DTI; PN	CIPPIA
36	Auditoría interna del SIPPID	Equipo técnico ad hoc independiente o auditor externo	VAD	EC; DPO; DTI; PN, según la materia	CIPPIA; Rector
37	Auditoría externa y verificación por terceros	Auditor externo	VAD	EC; DTI; DPO	CIPPIA; Rector
38	Indicadores y métricas de desempeño del SIPPID	CIPPIA (propone)	VAD	DPO; DTI; EC	Rector; CAS
39	Mejora continua y certificaciones ISO aplicables	CIPPIA (propone)	Rector	VAD; DTI; DPO; EC	CAS
40	Matriz de Responsabilidades: propuesta y actualización	CIPPIA (propone)	CAS; Rector para ajustes meramente operativos	CR, cuando corresponda; VAD; DTI; EC; DPO; PN; SGT	Comunidad
H. Ética					
41	Asuntos éticos del uso de la IA y de la información	CUE / Subcomités de Ética	CUE	CIPPIA; PN	VAD
I. Cultura, formación y alfabetización					
42	Capacitación, sensibilización y alfabetización	CIPPIA (propone)	VAD / VAC	DTI; DPO; EC	Comunidad
J. Deberes individuales					
43	Uso ético, lícito y diligente; confidencialidad perpetua; reporte de incidentes	Cada integrante de la Comunidad Universitaria	Autoridad de la unidad	DPO; DTI	—

Notas. 1) Cuando una función comprenda tratamiento de datos personales mediante sistemas de inteligencia artificial, la asignación se complementa con lo previsto en el Reglamento para el Uso Ético, Responsable y Seguro de la Inteligencia Artificial. 2) La calificación de un sistema

de IA como de alto riesgo no constituye causal automática de no adquisición. 3) La auditoría interna no supone la creación de una unidad administrativa permanente. Será ejecutada por un equipo técnico ad hoc con independencia funcional y competencia suficiente, por el Especialista en Cumplimiento cuando no exista conflicto de interés, o mediante auditores externos especializados. El Especialista en Cumplimiento coordinará administrativamente el programa, dará seguimiento a los hallazgos y verificará el cierre de los planes de acción, sin auditar procesos en cuya ejecución haya intervenido. 4) La gestión administrativa ordinaria ante la autoridad de control corresponde al Vicerrectorado Administrativo o a la unidad que este designe; la Procuraduría Nacional interviene únicamente cuando exista requerimiento jurídico, contestación formal, procedimiento sancionador, interpretación normativa o defensa institucional. 5) Los plazos, periodicidad, fuentes de verificación y destinatarios de cada reporte se precisan en los instrumentos operativos e indicadores que proponga el Comité Institucional y apruebe la autoridad competente.

Aprobación y actualización. La presente Matriz se aprueba como Anexo Único del Reglamento y forma parte integrante de este. El Comité Institucional (CIPPIA) podrá proponer su actualización cuando existan reformas normativas, cambios orgánico-funcionales o necesidades institucionales debidamente justificadas. Las actualizaciones que impliquen modificaciones sustantivas de responsabilidades serán aprobadas por el Consejo Académico Superior, previo informe favorable del Consejo de Regentes cuando corresponda. Los ajustes meramente operativos que no alteren competencias podrán ser aprobados por el Rector, previo criterio jurídico no vinculante de la Procuraduría Nacional.

Aprobada por el Consejo Académico Superior como Anexo Único del Reglamento

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ALEJANDRO RAFAEL SOCORRO CASTRO

Ing. Alejandro Rafael Socorro Castro, PhD.
RECTOR Y PRESIDENTE DEL CONSEJO ACADÉMICO SUPERIOR

Lo certifico:

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
AUGUSTO ANDRES CUEVA GAIBOR

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

REGLAMENTO PARA LA PROTECCION DE LA PRIVACIDAD, DE LA INFORMACION Y DE LOS DATOS PERSONALES DE LA UNIVERSIDAD METROPOLITANA.

UMET UNIVERSIDAD METROPOLITANA

Editorial UMET