RESOLUCIÓN N.º

CPSDP-O-005-2026-UTI

EL COMITÉ DE PRIVACIDAD Y SEGURIDAD DE DATOS PERSONALES DE LA UNIVERSIDAD TECNOLÓGICA INDOAMÉRICA

CONSIDERANDO:

Que, el numeral 19 del artículo 66 de la Constitución de la República del Ecuador reconoce el derecho a la protección de datos personales, cuyo texto dispone: *"19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos personales requerirán la autorización del titular o el mandato de la ley"*;

Que, el artículo 1 de la Ley Orgánica de Protección de Datos Personales establece: *"El objeto y finalidad de la presente Ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela"*;

Que, el literal k) del artículo 10 de la Ley Orgánica de Protección de Datos Personales determina: *"Responsabilidad proactiva y demostrada.- El responsable del tratamiento de datos personales deberá acreditar el haber implementado mecanismos para la protección de datos personales; es decir, el cumplimiento de los principios, derechos y obligaciones establecidos en la presente Ley"*;

Que, el artículo 47, numerales 2 y 4, de la Ley Orgánica de Protección de Datos Personales establece, entre las obligaciones del responsable del tratamiento: *"2) Aplicar e implementar requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas, a fin de garantizar y demostrar que el tratamiento de datos personales se ha realizado conforme a lo previsto en la presente Ley"* y *"4) Implementar políticas de protección de datos personales afines al tratamiento de datos personales en cada caso en particular"*;

Que, la Universidad Tecnológica Indoamérica, en observancia de la normativa aplicable y en ejercicio de sus mecanismos institucionales de gobernanza, considera necesario establecer reglas claras para informar a los niños, niñas y adolescentes, sus representantes legales respectivamente y demás titulares comprendidos en la política sobre el tratamiento de sus datos personales, sus finalidades y los mecanismos para ejercer sus derechos;

Que, el Comité de Privacidad y Seguridad de Datos Personales creado conforme a Resolución No. SO-04-010-CSU-2026, en el marco de las atribuciones institucionales que le han sido conferidas y conforme al orden del día de la Convocatoria N.º CPSI-E-002-2026-UTI, conoció y sometió a consideración Política de protección de datos personales para niños, niñas y adolescentes de la Universidad Tecnológica Indoamérica;

En ejercicio de las atribuciones conferidas al Comité,

RESUELVE:

Aprobar lo siguiente:

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

PARA NIÑAS, NIÑOS Y ADOLESCENTES

UNIVERSIDAD TECNOLÓGICA INDOAMÉRICA

Esta Política de Protección de Datos Personales informa el tratamiento de los datos personales de niñas, niños y adolescentes (en adelante, "NNA") que la Universidad Tecnológica Indoamérica (en adelante, "la Universidad" o "UTI") realiza en el marco de su misión institucional, de la Ley Orgánica de Educación Superior, del Código de la Niñez y Adolescencia y de la normativa aplicable de protección de datos.

Los datos personales de NNA son necesarios para el cumplimiento de las obligaciones académicas, administrativas, de bienestar estudiantil, de seguridad y de vinculación con la sociedad. La no entrega de determinados datos por parte de los representantes legales —o del adolescente, cuando la ley le reconoce capacidad para consentir— podrá impedir o limitar la prestación de servicios académicos, de bienestar u otros vinculados a las finalidades descritas.

De conformidad con la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales ("LOPDP"), el Reglamento General a la LOPDP ("RGLOPDP"), el Código de la Niñez y Adolescencia, la Ley Orgánica de Educación Superior y demás normativa aplicable, la Universidad informa lo siguiente.

1. Responsable del tratamiento de datos personales

La UNIVERSIDAD TECNOLÓGICA INDOAMÉRICA, con RUC 1891700772001 y domicilio principal en las calles Simón Bolívar 20-35 y Guayaquil, Ambato, provincia de Tungurahua, República del Ecuador, con sedes y campus adicionales en Quito, Latacunga y demás centros de apoyo que la Institución tenga habilitados, es la responsable del tratamiento de los datos personales objeto de este instrumento.

Contacto del responsable:

Teléfono (593) 3 2994560; correo rectorado@uti.edu.ec

Delegado de Protección de Datos Personales: Bolívar 20-35 y Guayaquil, Ambato; correo: **protecciondedatos@indoamerica.edu.ec.**

La Universidad pone a disposición la presente política a efecto de llevar a cabo el tratamiento de datos personales de niñas, niños y adolescentes, garantizando su derecho a la protección de estos, el interés superior del niño y el ejercicio progresivo de sus derechos.

2. Alcance

La presente Política de Tratamiento de Datos Personales aplica exclusivamente al tratamiento de datos personales de niñas, niños y adolescentes (en adelante, "NNA"), esto es, personas menores de dieciocho (18) años, en cualquiera de las siguientes calidades o contextos:

- Estudiantes de grado, posgrado, nivelación, preuniversitario o programas equivalentes que no hayan cumplido 18 años.
- Participantes en cursos de educación continua, talleres, campamentos, escuelas deportivas o culturales, programas de vinculación con la sociedad, ferias, visitas guiadas, olimpiadas, concursos y eventos institucionales.
- Hijas e hijos, o cargas familiares, de estudiantes, docentes, servidores o trabajadores de la Universidad, cuando sus datos se traten para beneficios, seguros, emergencias, bienestar o cumplimiento de obligaciones laborales y de seguridad social.
- Visitantes o usuarios de campus, bibliotecas, laboratorios, instalaciones deportivas, servicios de salud u orientación, plataformas digitales o aplicativos de la Universidad.
- Personas cuya imagen, voz o datos de identificación se capten en actividades académicas, culturales, deportivas, de investigación o de comunicación institucional.
- NNA que participen en proyectos de investigación, prácticas, voluntariado o movilidad, en la medida en que la Universidad trate sus datos.

Los tratamientos relativos a estudiantes mayores de edad, trabajadores, docentes, proveedores, aspirantes adultos y público en general se rigen por las políticas específicas que la Universidad emita para cada categoría de titulares.

Cuando un NNA cumpla 18 años durante la vigencia de la relación académica o de otra índole, el tratamiento posterior se sujetará a la política aplicable a titulares mayores de edad, sin perjuicio de la conservación de los datos ya recabados conforme a los plazos de esta política.

3. Recolección de datos personales

Los datos que tratará la Universidad serán obtenidos, principalmente, de las siguientes fuentes:

- Los facilitados por el propio NNA y, de manera preponderante, por su padre, madre, tutor o representante legal, a través de cualquier canal (físico o digital), al momento de la admisión, matrícula, inscripción a un programa, evento o servicio, o durante la relación académica.
- Datos generados como consecuencia de la relación jurídica o de la prestación del servicio educativo y conexos (asistencia, calificaciones, evaluaciones, reportes de bienestar, incidentes, uso de plataformas, credenciales, entre otros).
- Bases de datos de acceso público o registros oficiales, cuando exista habilitación legal (por ejemplo, validación de identidad o de estudios previos).
- Instituciones de origen (unidades educativas, MINEDUC u otros) en procesos de admisión, homologación, convenios o programas de articulación.
- El ingreso a instalaciones, el uso de sitios de internet, campus virtual, aplicativos móviles, correo institucional, sistemas de biblioteca, laboratorios y controles de acceso.

- Captación de imágenes, voz o video en eventos, clases, prácticas, actividades deportivas o de seguridad (videovigilancia), en los términos informados en esta política.
- Prestadores de servicios de salud ocupacional o estudiantil, orientación psicopedagógica y trabajo social, cuando el tratamiento esté habilitado.

Cuando los datos no se obtengan directamente del titular o de su representante legal, la Universidad informará el origen y las finalidades en los plazos y con el contenido que exige el artículo 12 de la LOPDP, con refuerzo de claridad por tratarse de NNA.

4. Tratamiento de datos personales

La Universidad tratará distintos tipos de datos personales para las finalidades descritas en esta política. El listado es enunciativo y se precisará con el RAT. Se tratarán únicamente los datos pertinentes, adecuados y limitados a lo necesario (principio de minimización).

Datos personales no sensibles (ordinarios)

- Datos identificativos: nombres y apellidos; número de cédula, pasaporte u otro documento de identidad; fecha y lugar de nacimiento; nacionalidad; fotografías institucionales; firma; credenciales estudiantiles; código o identificador interno; usuario de plataformas.
- Datos de contacto del NNA y de sus representantes legales: domicilio, correo electrónico, teléfono fijo y celular, persona de contacto en caso de emergencia.
- Datos de características personales: sexo, género, estado civil cuando aplique, número de cargas, lateralidad, datos de filiación necesarios para acreditar representación legal.
- Datos de circunstancias sociales y socioeconómicas: composición familiar, situación de vivienda cuando se requiera para becas o ayudas, información necesaria para beneficios o gratuidad, en lo estrictamente indispensable.
- Datos académicos: institución de origen, historial educativo, notas, asistencia, evaluaciones, necesidades educativas, participación en actividades extracurriculares, títulos o certificados, portafolios, trabajos.
- Datos financieros vinculados a la prestación del servicio: forma de pago, datos de facturación del representante, convenios, becas, créditos educativos, valores pendientes. No se solicitarán datos de tarjetas de crédito del NNA.
- Datos relativos a procesos administrativos o disciplinarios estudiantiles y, cuando exista obligación legal, información derivada de procesos judiciales que incidan en la representación, tenencia, visitas o medidas de protección. A la información judicial y de medidas de protección solo acceden Bienestar Universitario y la autoridad académica que deba ejecutar la medida, con registro de accesos.

Categorías especiales y datos sensibles

Conforme al artículo 25 de la LOPDP, los datos de niñas, niños y adolescentes constituyen por sí mismos una categoría especial. Además, podrán tratarse, solo cuando exista base de licitud reforzada y necesidad, los siguientes:

- Datos biométricos identificativos (huella, reconocimiento facial u otros): no se tratan mientras no consten en el RAT, no exista análisis de riesgos ni EIPD, y no se acredite —conforme a la Resolución N.º SPDP-SPD-2026-0039-R— que un

medio menos invasivo es insuficiente. Queda prohibido su uso como mecanismo ordinario de asistencia. La alternativa no biométrica es la regla.

- Datos de salud: ficha médica, alergias, discapacidades, enfermedades, medicamentos de emergencia, certificados de aptitud, atenciones en servicio médico o de primeros auxilios, restricciones deportivas, exámenes ocupacionales o de ingreso cuando procedan. La atención de NNA en el Centro Odontológico de la Universidad se rige, además, por el aviso de privacidad para pacientes y por la normativa sanitaria.
- Datos de salud mental y psicopedagógicos: evaluaciones de orientación, reportes de bienestar, adaptaciones curriculares, informes de inclusión, siempre bajo reserva y acceso restringido.
- Datos de menores que son cargas familiares de estudiantes o trabajadores (cédula, partida de nacimiento, certificados para beneficios).
- Características físicas o fisiológicas cuando sean necesarias para salud, deporte, laboratorios o inclusión.
- Origen étnico o racial, autoidentificación, o datos culturales, solo si el titular o su representante los proporcionan y son necesarios para acciones afirmativas, inclusión o reportes legalmente exigidos.
- Grupo sanguíneo, como dato de salud, únicamente para la atención de emergencias.
- Imagen y voz, que permiten identificar al NNA.
- Registros técnicos de plataforma (dirección IP, registro de acceso al campus virtual) para seguridad y funcionamiento del servicio educativo. La geolocalización activa del dispositivo no se trata, salvo que el RAT la identifique con finalidad, base y información previa específicas.
- Videovigilancia en campus e instalaciones.

La Universidad solo tratará categorías especiales de datos de NNA cuando concurra una condición del artículo 26 de la LOPDP. Por regla, será el consentimiento explícito del representante legal y, para adolescentes de 15 a 17 años, el del adolescente (art. 21 LOPDP y art. 19 RGLOPDP). Otras condiciones posibles son la protección de intereses vitales cuando el titular no pueda consentir o una obligación legal expresamente identificada. Respecto de los datos de salud, el tratamiento se realizará conforme a la normativa sanitaria y de educación inclusiva, con medidas de seguridad reforzadas.

5. Tratamiento legítimo de datos personales

Toda finalidad se interpreta y ejecuta a la luz del interés superior del niño, de la minimización de datos y de la prohibición de usar datos de NNA para mercadotecnia indiscriminada o elaboración de perfiles con efectos jurídicos, salvo las excepciones legales.

6. Acceso de datos personales

6.1. Con base en la ejecución de obligaciones contractuales o precontractuales

(Relación de matrícula, inscripción a programas, prestación del servicio educativo y servicios conexos, convenida con el representante legal y, cuando corresponda, con el adolescente.)

- Gestionar admisión, inscripción, matrícula, cambios de carrera o de modalidad, retiros y reinscripciones.

- Prestar el servicio de educación superior o de educación continua: planificación curricular, dictado de clases presenciales, híbridas o virtuales, tutorías, evaluaciones, registro de calificaciones y asistencia.
- Emitir y administrar credenciales, carnés, accesos a campus, bibliotecas, laboratorios y sistemas académicos.
- Operar el campus virtual, correo institucional, plataformas de aprendizaje, repositorios y herramientas colaborativas necesarias para la formación.
- Facturar, recaudar, gestionar convenios de pago, becas, descuentos y ayudas económicas a nombre del representante.
- Comunicarse con el NNA y con sus representantes sobre asuntos académicos, administrativos, de seguridad y de bienestar vinculados al servicio.
- Organizar prácticas, laboratorios, salidas de campo, movilidad y actividades extracurriculares que formen parte de la oferta académica.
- Administrar servicios de bienestar estudiantil, inclusión, trabajo social y orientación vocacional o psicopedagógica asociados a la matrícula.
- Atender requerimientos, quejas o reclamaciones del NNA o de sus representantes.
- Gestionar el ingreso, permanencia y salida del NNA de las instalaciones y la identificación ante terceros que deban verificar su calidad de estudiante o participante.

6.2. Con base en el cumplimiento de una norma u obligación legal

- Cumplir la Ley Orgánica de Educación Superior, su reglamento, resoluciones del CES, SENESCYT, CACES y demás órganos del Sistema de Educación Superior.
- Reportar información académica y estadística exigida por autoridades educativas y de control.
- Cumplir obligaciones tributarias y de facturación electrónica ante el Servicio de Rentas Internas.
- Observar el Código de la Niñez y Adolescencia, incluyendo el deber de comunicar a las autoridades competentes situaciones de amenaza o vulneración de derechos.
- Aplicar normativa de inclusión educativa, discapacidad y adaptaciones razonables.
- Cumplir normas de seguridad y salud, prevención de riesgos, gestión de emergencias y primeros auxilios en campus.
- Atender requerimientos de autoridades judiciales, fiscalía, juntas cantonales de protección de derechos, Defensoría del Pueblo u otras autoridades competentes.
- Conservar expedientes académicos y títulos por los plazos de archivo público e institucional.
- Cuando corresponda, cumplir obligaciones frente al IESS u otras entidades en relación con cargas familiares de trabajadores o estudiantes.
- Aplicar el régimen disciplinario estudiantil conforme a estatuto, reglamento interno y normativa de educación superior.
- Cumplir la propia LOPDP y las disposiciones de la Superintendencia de Protección de Datos Personales.

6.3. Con base en la protección de intereses vitales y en obligaciones legales de protección

- Atender emergencias médicas, accidentes o situaciones que pongan en riesgo la vida, la integridad o la salud del NNA, cuando no sea posible obtener el consentimiento de su representante (arts. 7 num. 6 y 26 lit. c, LOPDP).
- Adoptar medidas de protección frente a acoso, violencia, ciberacoso o discriminación, y comunicar a las autoridades competentes situaciones de amenaza o vulneración de derechos, en cumplimiento del Código de la Niñez y Adolescencia y del Art. 7 num. 2, LOPDP.
- Contactar de inmediato a representantes legales o a autoridades de protección cuando exista un riesgo actual.

En todos los casos, la Universidad aplica el principio del interés superior del NNA como criterio de interpretación y de proporcionalidad; ese principio no constituye por sí mismo una base de legitimación. Los ajustes razonables se rigen por la sección 6.2 y la videovigilancia, por la sección 11 de esta política.

6.4. Con base en el consentimiento libre, informado, inequívoco, específico y, cuando se trate de categorías especiales, explícito

Regla de edad para los tratamientos que sí dependen de consentimiento (esta sección 6.4):

- Menores de 15 años: el consentimiento lo otorga el representante legal. El NNA es oído según su edad y madurez.
- Adolescentes de 15 a 17 años: pueden otorgar por sí mismos consentimiento explícito, con información en lenguaje claro y adaptado (art. 21 LOPDP). El representante es informado. Para sus datos sensibles, incluidos los de salud y psicopedagógicos, se requiere además el consentimiento expreso del representante legal (art. 19 RGLOPDP).
- Los tratamientos de las secciones 6.1, 6.2 y 6.3 no se habilitan por este consentimiento.

En particular, el consentimiento de esta sección cubre:

- Uso de imagen, voz y producciones audiovisuales del NNA en canales institucionales (sitio web, redes sociales, revistas, pantallas de campus, material de difusión académica o de vinculación). Este consentimiento es independiente del consentimiento para el tratamiento académico.
- Participación en proyectos de investigación, encuestas, grupos focales o publicaciones académicas que identifiquen al NNA.
- Tratamiento de datos de salud o psicopedagógicos que excedan lo estrictamente necesario para una emergencia o para una obligación legal de inclusión.
- Uso de aplicativos con geolocalización o analítica de aprendizaje no indispensable para dictar la cátedra. Los datos biométricos se rigen por la sección 5.
- Inscripción en concursos, premios, actividades recreativas o programas no curriculares.
- Tratamiento de datos de familiares del NNA (hermanos, padres, tutores) para actualizar información, gestionar emergencias, beneficios o actividades vinculadas.
- Envío de comunicaciones no esenciales sobre oferta académica futura, eventos abiertos o actividades de comunidad universitaria. La Universidad no utilizará datos de NNA para mercadotecnia de productos ajenos a su objeto educativo ni para elaboración de perfiles comerciales.

El consentimiento podrá revocarse en cualquier momento, sin efectos retroactivos. La revocación no afectará los tratamientos que descansen en obligación legal, ejecución contractual o interés vital. Si la revocación impide continuar un servicio opcional (por ejemplo, publicación de imagen), ese servicio cesará; si impide un elemento esencial de la matrícula, se informará la consecuencia concreta.

6. Acceso a los datos personales

Para el cumplimiento de las finalidades informadas, sin que los datos sean usados para fines distintos, la Universidad podrá comunicar o encargar el tratamiento de datos de NNA a:

- Autoridades del Sistema de Educación Superior: Consejo de Educación Superior (CES), Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT), Consejo de Aseguramiento de la Calidad de la Educación Superior (CACES) y demás órganos competentes.
- Ministerio de Educación, cuando existan programas de articulación, nivelación o reportes exigidos.
- Servicio de Rentas Internas, Instituto Ecuatoriano de Seguridad Social y otras entidades públicas frente a las cuales exista obligación de reporte.
- Fiscalía General del Estado, unidades judiciales, juntas cantonales de protección de derechos, Defensoría del Pueblo, Consejo de la Judicatura y Superintendencia de Protección de Datos Personales, cuando medie requerimiento o deber legal.
- Prestadores de servicios de salud, seguros estudiantiles o de accidentes, laboratorios y servicios de emergencia.
- Proveedores tecnológicos y administradores de sistemas (campus virtual, correo, almacenamiento, bibliotecas digitales, control de acceso, videovigilancia), quienes actuarán como encargados y estarán sujetos a contrato de encargo con cláusulas LOPDP.
- Instituciones educativas, organismos de investigación o contrapartes de convenios de prácticas, vinculación o movilidad, solo en lo necesario para el programa.
- Auditores, consultores y asesores jurídicos o de cumplimiento, bajo deber de confidencialidad.
- Empresas de transporte, mensajería o logística, cuando el servicio contratado lo requiera (por ejemplo, salidas de campo).

Algunos encargados almacenan datos fuera del Ecuador. Conforme a la Resolución N.º SPDP-SPD-2026-0004-R, ese acceso del encargado no constituye una transferencia: la Universidad lo regula en el contrato de encargo, con cláusulas conforme a la Resolución N.º SPDP-SPD-2025-0006-R, e informa el país y las garantías aplicables.

Si se comparten datos personales, la Universidad exigirá que el destinatario otorgue un nivel adecuado de protección, limitará la comunicación a lo necesario y documentará la base de licitud. No se cederán datos de NNA para finalidades comerciales de terceros.

7. Derechos de los titulares y modo de ejercerlos

El titular —el NNA— es el titular del derecho a la protección de datos personales. El ejercicio de los derechos se rige por los artículos 12 a 24 de la LOPDP:

- Los adolescentes mayores de quince (15) años y menores de dieciocho (18) años podrán ejercitarlos de forma directa ante la Universidad o ante la Autoridad de Protección de Datos Personales.

- Las niñas y niños, y los adolescentes mayores de doce (12) y menores de quince (15) años, necesitarán de su representante legal para el ejercicio de estos derechos.
- En todos los casos, la Universidad valorará el interés superior del NNA y, cuando sea apropiado a su edad y madurez, recabará también su opinión.

Los derechos son, en lo principal:

- Derecho de información: conocer, de forma previa, clara y accesible, las finalidades, bases legales, tipos de datos, plazos, destinatarios, transferencias y canales de reclamo. Esta información se refuerza cuando el titular es NNA.
- Derecho de acceso: obtener gratuitamente los datos personales tratados y la información del artículo 12 de la LOPDP.
- Derecho de rectificación y actualización de datos inexactos o incompletos.
- Derecho de eliminación, cuando concurra alguna causal legal y no exista obligación de conservación.
- Derecho de oposición, en los supuestos del artículo 16 de la LOPDP, incluyendo la oposición a mercadotecnia directa y a elaboración de perfiles.
- Derecho a la suspensión del tratamiento, en los casos del artículo 19 de la LOPDP.
- Derecho a la portabilidad, cuando concurra alguna de las condiciones del artículo 17 de la LOPDP.
- Derecho a revocar el consentimiento, sin que ello afecte la licitud del tratamiento previo.
- Derecho a no ser objeto de decisiones basadas única o parcialmente en valoraciones automatizadas, con la protección reforzada del artículo 21 de la LOPDP para datos de NNA y datos sensibles.
- Derecho a la educación digital, en los términos del artículo 23 de la LOPDP.

El ejercicio de estos derechos está sujeto a las excepciones legales (interés público, prevención de infracciones, obligaciones de archivo académico, derechos de terceros, entre otras). La Universidad verificará la legitimidad de la solicitud —incluida la representación— y responderá dentro del término de diez (10) días previsto en el artículo 62 de la LOPDP.

Las solicitudes pueden presentarse al correo **protecciondedatos@indoamerica.edu.ec** o por escrito en las secretarías de las sedes, acreditando identidad y, de ser el caso, la representación legal (cédula y documento que acredite patria potestad, tenencia, tutela o autorización). Las resuelve la unidad responsable del tratamiento, con el asesoramiento y la supervisión del Delegado de Protección de Datos Personales.

Si el titular o su representante no está satisfecho con el uso de la información o con la respuesta recibida, puede presentar una reclamación ante la Superintendencia de Protección de Datos Personales, por los canales que esa Autoridad habilite.

8. Protección de los datos personales de NNA

La Universidad aplica un nivel de protección reforzado, por diseño y por defecto, al tratamiento de datos de NNA. Solo acceden a estos datos las personas que los necesitan para las finalidades informadas, bajo perfiles de usuario, deber de confidencialidad y principio de privilegio mínimo.

Entre las medidas técnicas, organizativas, administrativas y jurídicas se encuentran, de manera enunciativa:

- Minimización: no se recaban datos que no sean necesarios; se evitan categorías especiales si un dato ordinario basta.
- Expediente de bienestar, inclusión y psicopedagogía segregado del expediente académico general; acceso restringido a personal autorizado; trazabilidad de accesos; prohibición de uso disciplinario indiscriminado.
- Cifrado, copias de seguridad, control de privilegios y registro de accesos en sistemas institucionales.
- Formación al personal docente y administrativo que trata datos de NNA.
- Contratos de encargo con proveedores y cláusulas de confidencialidad.
- Protocolos de notificación de violaciones de seguridad, con evaluación reforzada del riesgo para NNA.
- Evaluación de impacto previa de los tratamientos de datos de NNA que incluyan datos de salud, psicopedagógicos o videovigilancia (art. 42 LOPDP y Resolución N.º SPDP-SPD-2026-0005-R), y revisión periódica de las medidas y de esta política.

Queda prohibido al personal de la Universidad publicar, reenviar o difundir datos, imágenes o trabajos de NNA en cuentas personales o canales no institucionales, salvo autorización expresa y específica.

9. Uso de imagen, voz y grabaciones

La captación y uso de fotografías, videos o grabaciones de voz de NNA con fines de difusión institucional (sitio web, redes sociales, material promocional, memorias de eventos) requiere consentimiento específico, informado y revocable del representante legal y, desde los 15 años, también del adolescente. Ese consentimiento no se entiende otorgado por el solo hecho de la matrícula.

Se exceptúan las grabaciones estrictamente necesarias para dictar o evidenciar una actividad académica (por ejemplo, una clase virtual o una evaluación), las cuales se usarán solo para esa finalidad y con acceso restringido a docentes y estudiantes del curso, y la videovigilancia de seguridad, que no se destinará a difusión pública.

Revocado el consentimiento de difusión pública, la Universidad cesará usos futuros y retirará o dejará de difundir el contenido en los canales que administra. Respecto de reenvíos o copias en poder de terceros, adoptará medidas razonables de cese de uso y no reutilización. Ello no constituye una exclusión general de responsabilidad.

10. Plataformas digitales, correo institucional y videovigilancia

Si la Universidad asigna al NNA un usuario, correo o espacio en campus virtual, dichos recursos son institucionales y están destinados al desempeño académico. Podrán ser administrados, suspendidos o auditados conforme a las políticas de uso aceptable y de seguridad de la información, respetando la expectativa razonable de privacidad y el interés superior del NNA. No se usarán como herramienta de vigilancia desproporcionada de la vida privada.

Los campus e instalaciones pueden contar con videovigilancia para la seguridad de las personas y de los bienes. La base de este tratamiento no es el consentimiento, sino el deber de cuidado y el interés legítimo, sujeto a la Resolución N.º SPDP-SPD-2025-0041-R y a ponderación que se documentará con el RAT. El plazo concreto lo fijará la política institucional de videovigilancia y el RAT; será el mínimo necesario, con excepción por incidente, investigación o autoridad. Las zonas se señalizarán. Las grabaciones no se usan

para difusión pública.

Queda prohibida la decisión puramente automatizada con efectos jurídicos sobre un NNA. Si existiera analítica de aprendizaje, se documentará en el RAT, con intervención humana y sin perfilamiento comercial.

11. Supervisión de cumplimiento

El Delegado de Protección de Datos Personales de la Universidad supervisa internamente el cumplimiento de esta política. El titular o su representante podrá presentar una reclamación ante la Superintendencia de Protección de Datos Personales, a través de los medios que esa Autoridad haya habilitado.

12. Tiempo de conservación de los datos

La Universidad distingue plazos según el tipo de dato y la norma que lo regula:

- Datos necesarios para la prestación del servicio educativo: mientras dure la matrícula, inscripción o participación en el programa, y el tiempo adicional indispensable para cierre académico, atención de reclamos y auditorías.
- Expediente académico, actas, títulos y documentos de archivo institucional: por los plazos que impongan la normativa de educación superior y el régimen de archivo; este plazo puede ser indefinido o de larga duración respecto de títulos y certificaciones.
- Datos de salud, bienestar y psicopedagogía: el tiempo necesario para la atención y el plazo sanitario o de responsabilidad que corresponda; después, bloqueo, anonimización o eliminación.
- Imagen de difusión pública y comunicaciones opcionales: hasta la revocación o hasta cumplir la finalidad.
- Videovigilancia y registros técnicos de plataforma: el plazo que fije la política institucional y el RAT, el mínimo necesario.
- Datos de cargas familiares de trabajadores: política de trabajadores y obligaciones de seguridad social.

No existe un plazo residual único de diez años para datos de NNA. El RAT fijará el número por categoría. Transcurrido el plazo aplicable, se eliminará, anonimizará o bloqueará conforme a la LOPDP y al RGLOPDP.

En canales digitales, sitios web o aplicativos, podrán existir plazos adicionales determinados en las Políticas de Cookies, que deben consultarse de manera singularizada.

13. Actualización de la política

Esta política podrá actualizarse para reflejar cambios normativos, el resultado del RAT, nuevas actividades de tratamiento o instrucciones de la Autoridad. La versión vigente se publicará en el sitio web institucional www.indoamerica.edu.ec, en la sección de protección de datos o privacidad.

Última actualización: 15 de octubre del 2026.

Se recomienda a los representantes legales y a los adolescentes mayores de 15 años revisar periódicamente la versión publicada.

14. Aceptación y consentimientos específicos

La Universidad podrá recabar la aceptación de la política en formato físico o electrónico, incluyendo casillas en formularios de matrícula o inscripción, siempre que se preserve evidencia del consentimiento, de la versión de la política aceptada y de la fecha, aceptación que deberá contar con:

La firma del Titular o el Representante Legal y la declaración de: (i) haber sido informado, en lenguaje claro, sobre el tratamiento de los datos personales del NNA, incluidas las secciones 6.1, 6.2 y 6.3, que no se habilitan por consentimiento; (ii) que los datos que proporciona son veraces; y (iii) que ostenta la representación legal o la autorización correspondiente. La firma no equivale a un consentimiento general sobre todos los tratamientos descritos.

Los tratamientos de la sección 6.4 y del numeral 11 que sí dependen de consentimiento se autorizan solo si se marcan las casillas correspondientes, por quien corresponda según la regla de edad.

Marque con una X lo que autoriza de manera adicional y específica:

☐ Autorizo el registro académico interno de imagen o voz del NNA (clase virtual, evidencia de aprendizaje), con acceso restringido al curso o actividad.

☐ Autorizo la difusión pública de imagen, voz o producciones del NNA en sitio web, redes sociales, revistas o material promocional institucional.

☐ Autorizo el tratamiento de datos de salud o psicopedagógicos que excedan la atención de emergencias y las obligaciones legales de inclusión, para seguimiento de bienestar. Si el NNA tiene entre 15 y 17 años, esta casilla la marcan el adolescente y su representante legal.

☐ Autorizo el envío de comunicaciones sobre oferta académica, eventos y actividades de comunidad universitaria no estrictamente indispensables para la matrícula vigente.

La falta de marcado de estas casillas no impide, por sí sola, la matrícula o inscripción, salvo que el dato o el tratamiento sea estrictamente necesario para prestar el servicio concreto que se solicita.