RESOLUCIÓN N.º

CPSDP-O-006-2026-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 proveedores de bienes, obras y servicios 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 proveedores de bienes, obras y servicios de la Universidad Tecnológica Indoamérica;

En ejercicio de las atribuciones conferidas al Comité,

RESUELVE:

Aprobar lo siguiente:

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

PARA PROVEEDORES DE BIENES, OBRAS Y SERVICIOS

UNIVERSIDAD TECNOLÓGICA INDOAMÉRICA

1. Responsable del tratamiento de datos personales

La UNIVERSIDAD TECNOLÓGICA INDOAMÉRICA (en adelante, "la Universidad" o "UTI"), 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.

La Universidad es una institución de educación superior particular, sujeta a la Constitución de la República, la Ley Orgánica de Educación Superior, su normativa conexa y, cuando corresponda, al Sistema Nacional de Contratación Pública.

Este instrumento se aplica a todo tratamiento de datos personales de personas naturales que actúen como proveedores de bienes, obras o servicios, y de las personas naturales vinculadas a proveedores personas jurídicas: representantes legales, socios, accionistas, directores, apoderados, contactos comerciales y personal que preste servicios en o para la Universidad (incluyendo quienes requieran acceso a campus, sistemas o información institucional).

La política cubre datos almacenados en medio electrónico, en soporte papel o en archivos mixtos.

Delegado de Protección de Datos Personales:

Dirección: Bolívar 20-35 y Guayaquil, Ambato; Correo: **protecciondedatos@indoamerica.edu.ec.**

Contacto del responsable: teléfono (593) 3 2994560; correo rectorado@uti.edu.ec

Los proveedores se clasifican, según el rol frente a los datos, en:

(i) Proveedor sin acceso a datos personales de estudiantes, trabajadores u otros titulares de UTI, más allá de los datos propios de la relación comercial;
(ii) Encargado, cuando trata datos de titulares de UTI por instrucción de la Universidad;
(iii) Destinatario, cuando recibe datos para una finalidad propia habilitada;
(iv) Eventual responsable conjunto, cuando determine con UTI fines y medios.

2. Alcance

Esta política informa los datos del propio proveedor. Los roles (ii) y, cuando corresponda, (iv) exigen contrato de encargo o acuerdo específico, con cláusulas conforme a la Resolución N.º SPDP-SPD-2025-0006-R, cuya verificación es requisito previo a la firma.

3. Recolección de datos personales

Los datos que tratará la Universidad serán, principalmente, los siguientes:

- Los facilitados por el propio titular a través de cualquier canal (físico o digital), o por la organización que representa.
- Datos de socios, accionistas, directores, apoderados, contactos y personal asignado a la ejecución del contrato, entregados por el proveedor.
- Datos generados como consecuencia de la relación precontractual o contractual: órdenes de compra, actas, facturas, garantías, informes de avance, evaluaciones, incidentes y comunicaciones.
- Información obtenida solo de las fuentes y para las finalidades que se indican: RUP/SOCE, para habilitación como contratista cuando el procedimiento se sujete al SNCP; SRI, para validación tributaria; IESS, para verificar cumplimiento cuando sea requisito; Registro Civil, para identidad del representante; registro mercantil, para representación societaria. El RAT confirmará cuáles de estas fuentes se usan realmente. No se realizarán consultas indiscriminadas.
- Información proporcionada en procesos de cotización, invitación, concurso, contratación directa o cualquier procedimiento de compras institucional.
- Correo electrónico, portales de proveedores, contratos, anexos habilitantes y documentación de cumplimiento.

Si existiera fundamento jurídico, podrán obtenerse datos de otras entidades con las que la Universidad trabaje (por ejemplo, aseguradoras, bancos o contrapartes de un convenio). En ese caso se informará el origen y la finalidad, en los términos del artículo 12 de la LOPDP.

El proveedor declara que la información que entrega es completa, correcta y actualizada, y que si comunica datos de terceros cuenta con habilitación para hacerlo y los ha informado. Esa declaración no sustituye las obligaciones de UTI como responsable. Cuando un trabajador del proveedor se acredite para ingresar a campus o a sistemas de UTI, la Universidad le entregará un aviso breve con responsable, finalidad, origen del dato y canal de derechos.

4. Tratamiento de datos personales

Se tratarán únicamente los datos pertinentes, adecuados y limitados a lo necesario para evaluar, contratar y ejecutar la relación con el proveedor.

4.1. Datos personales no sensibles (ordinarios)

- Identificativos: nombres y apellidos; número de cédula o pasaporte; RUC; RUP u otro registro de proveedor; fotografía institucional cuando se emita credencial de acceso;

firma y firma electrónica; nombramiento de representante legal.

- Contacto: correo electrónico, teléfono celular y convencional, dirección domiciliaria o del establecimiento.

- Características personales, solo si resultan necesarias para identificar al titular o cumplir un requisito legal: fecha y lugar de nacimiento, nacionalidad, género.

- Circunstancias sociales o de establecimiento: dirección del local comercial o de ejecución, datos de domicilio del representante cuando el procedimiento lo exija.

- Financieros y económicos: número de cuenta bancaria para pagos, información tributaria y de facturación, retenciones, estado de obligaciones con el SRI o el IESS cuando sea requisito de contratación, indicadores financieros presentados en la oferta. No se solicitarán datos de tarjeta de crédito como regla del relacionamiento con proveedores.

- Profesionales y académicos: formación, títulos, experiencia, hoja de vida, certificaciones técnicas, historial de contrataciones o de prestación de servicios, producción o portafolio cuando el objeto del contrato lo requiera.

4.2. Datos del personal del proveedor

- Identificación y contacto de quienes ingresen a campus, laboratorios, residencias u otras instalaciones, o accedan a sistemas institucionales.

- Credenciales, registros de ingreso, videovigilancia y, si existieran, controles de acceso.

- Acreditaciones de competencia, permisos de trabajo en altura o en laboratorios, y demás requisitos de seguridad y salud en el trabajo aplicables a la actividad contratada.

4.3. Categorías especiales y datos de mayor protección

Como regla, la Universidad no recaba categorías especiales de los proveedores. Solo se tratarán cuando una norma lo exija o sean estrictamente necesarios para la ejecución segura del contrato, con una circunstancia del artículo 26 de la LOPDP:

- Datos de salud ocupacional o de aptitud del personal del proveedor que ejecute actividades de riesgo en campus. La Universidad solo recibirá el certificado de aptitud, no la historia clínica.

- Discapacidad, cuando el titular la declare para ajustes razonables o para verificar un criterio de inclusión de la convocatoria.

- Antecedentes o certificados de no tener impedimento, únicamente si el objeto del contrato lo justifica de manera proporcional (por ejemplo, servicios en contacto con NNA, manejo de valores o seguridad). Por tratarse de pasado judicial (dato sensible), se requerirá una norma que lo exija o el consentimiento explícito del titular (art. 26 LOPDP).

- Datos biométricos identificativos: no se tratan mientras no se autorice

expresamente. La credencial o el registro nominativo es el medio por defecto.

Los datos de niñas, niños y adolescentes no forman parte de este tratamiento, salvo que un proveedor los comunique de manera excepcional (por ejemplo, un dependiente en un siniestro). En ese caso rige la política de NNA.

5. Tratamiento legítimo de datos

La Universidad trata los datos de proveedores y de las personas naturales vinculadas a ellos para cumplir su objeto educativo e institucional, gestionar la contratación de bienes, obras y servicios, y observar las obligaciones legales y contractuales aplicables. Las finalidades son las siguientes.

- Tramitar cotizaciones, invitaciones, concursos, contrataciones directas y, cuando el procedimiento se sujete al Sistema Nacional de Contratación Pública, los procesos previstos en la LOSNCP y en la normativa SERCOP.
- Validar identidad, representación legal, RUC, RUP, datos tributarios, bancarios y de cumplimiento formal.
- Contrastar referencias comerciales o profesionales indicadas por el proveedor.
- Verificar conflictos de interés entre el proveedor, sus socios o directivos y las autoridades, docentes o servidores de la Universidad.
- Evaluar idoneidad técnica, experiencia y capacidad para el objeto contractual.
- Crear, actualizar o desactivar el perfil del proveedor en los sistemas de compras, tesorería, contabilidad y logística.
- Formalizar y administrar el contrato, las órdenes de compra, las garantías, las actas y las modificaciones.
- Gestionar pagos, facturación electrónica, retenciones, descuentos, notas de crédito y demás operaciones tributarias y financieras derivadas del contrato.
- Controlar la ejecución, la calidad, los plazos y el cumplimiento de obligaciones de ambas partes.
- Autorizar y controlar el acceso de personal del proveedor a instalaciones, laboratorios, residencias, eventos o sistemas institucionales.
- Gestionar seguros, siniestros y recuperaciones vinculados a los bienes o servicios contratados.
- Atender auditorías internas o externas y requerimientos de órganos de control.
- Ejercer o defender pretensiones derivadas del contrato, incluyendo cobranzas, multas, garantías y acciones judiciales o arbitrales.
- Elaborar estadísticas e indicadores de compras y de desempeño de proveedores, con datos agregados siempre que sea posible.

- Cumplir políticas internas de integridad, transparencia y prevención de fraude o corrupción, en lo proporcional al riesgo de la contratación.

- Contactar al proveedor sobre la ejecución del contrato, renovaciones, nuevas necesidades institucionales de compra o evaluaciones de servicio.

La Universidad no utilizará los datos de proveedores para mercadotecnia de productos ajenos a su objeto institucional. Las comunicaciones sobre nuevas contrataciones no vinculadas a un proceso en curso se basan en el consentimiento de la casilla correspondiente.

Si se incorporan tratamientos distintos de los aquí descritos, se informará al titular y se recabará consentimiento cuando la ley lo exija.

6. Base legitimadora

Cada finalidad de la sección del **Tratamiento legítimo de datos** tiene una base determinada: medidas precontractuales y ejecución del contrato para la contratación, administración, pagos, accesos y control (6.1); obligación legal para las finalidades tributarias, de control y de seguridad y salud (6.2); interés legítimo para la verificación de conflictos de interés, la prevención de fraude, la evaluación de desempeño y la defensa de reclamaciones (6.3); y consentimiento para el contacto de referencias, el registro de proveedores y las comunicaciones no vinculadas a un proceso en curso (6.4).

6.1. Medidas precontractuales y ejecución del contrato

Evaluación de ofertas, negociación y ejecución del contrato de suministro, obra o servicio, incluyendo pagos, garantías, accesos y control de cumplimiento.

6.2. Obligación legal

Normativa tributaria y de facturación electrónica; obligaciones ante el SRI y el IESS; Ley Orgánica de Educación Superior y normas de control institucional; LOSNCP, RUP y SOCE cuando el procedimiento se sujete al Sistema Nacional de Contratación Pública; requerimientos de Contraloría u otras autoridades competentes; LOPDP y disposiciones de la Superintendencia de Protección de Datos Personales; normativa de seguridad y salud cuando personal del proveedor trabaje en campus.

6.3. Interés legítimo

Verificación de conflictos de interés limitada a datos declarados y fuentes pertinentes, control de acceso, prevención de fraude en compras, evaluación de desempeño y defensa de reclamaciones. Estos tratamientos se sujetan a la Resolución N.º SPDP-SPD-2025-0041-R. La ponderación se documenta, antes del tratamiento, en el registro de ponderaciones de la Universidad. El titular puede oponerse a estos tratamientos por motivos relacionados con su situación particular (art. 16 num. 3 LOPDP). No se tratan categorías especiales ni datos de NNA con cargo a esta base, salvo excepción legal.

6.4. Consentimiento

Contacto de las referencias comerciales o profesionales; inclusión en el registro de proveedores para futuras invitaciones no vinculadas a un proceso en curso, por un máximo de veinticuatro (24) meses, renovables con nueva manifestación; comunicaciones no

esenciales; y categorías especiales no amparadas en obligación legal. Revocable, sin efectos retroactivos.

7. Acceso a los datos personales

La Universidad solo comunicará o encargará el tratamiento si existe fundamento jurídico o, cuando corresponda, consentimiento. Los destinatarios, en lo necesario, pueden ser:

- Áreas internas de compras, tesorería, contabilidad, jurídica, tecnología, infraestructura, bienestar, investigación o la unidad requirente del bien o servicio.
- Autoridades y entidades públicas competentes: SRI, IESS, SERCOP, Contraloría General del Estado, Ministerio del Trabajo, CES, SENESCYT, CACES, Procuraduría, Función Judicial, Fiscalía, Superintendencia de Protección de Datos Personales y demás órganos que legalmente puedan requerir la información.
- Entidades bancarias o financieras que procesen pagos institucionales.
- Auditores externos, asesores jurídicos, tributarios o de cumplimiento, bajo confidencialidad.
- Prestadores tecnológicos de nube, facturación electrónica, firma electrónica, mensajería, transporte, seguridad física o mantenimiento de sistemas, en calidad de encargados.
- Aseguradoras, cuando el contrato o el bien asegurado lo requiera.
- Contrapartes de un convenio o proyecto cofinanciado, solo en lo indispensable para ejecutar esa relación.

Algunos proveedores tecnológicos 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. Toda transferencia o comunicación internacional de sus datos a terceros se realizará conforme a los artículos 55 a 60 de la LOPDP y a la Resolución N.º SPDP-SPD-2026-0004-R.

Todo contrato que conlleve tratamiento de datos personales incorporará cláusulas conforme a la Resolución N.º SPDP-SPD-2025-0006-R. Sin esa verificación no se suscribe el contrato.

Si en el futuro se produjera una reorganización institucional, fusión o cesión de activos que implique transmitir archivos de proveedores, se informará y se exigirá al cesionario un nivel adecuado de protección.

La Universidad no cederá datos de proveedores para finalidades comerciales de terceros.

8. Derechos de los Titulares

El titular puede ejercer los derechos previstos en la LOPDP:

- Información y acceso a los datos contenidos en los ficheros o sistemas de la Universidad.

- Rectificación y actualización de datos inexactos o incompletos.
- Eliminación, cuando concurra una causal legal y no exista obligación de conservación contractual, tributaria o de archivo.
- Oposición, incluso al envío de comunicaciones no esenciales sobre nuevas contrataciones.
- Suspensión del tratamiento, en los casos del artículo 19 de la LOPDP.
- Portabilidad, cuando concurra alguna de las condiciones del artículo 17 de la LOPDP.
- Revocación del consentimiento, cuando esa sea la base.
- No ser objeto de decisiones basadas única o parcialmente en valoraciones automatizadas que produzcan efectos jurídicos o afecten derechos fundamentales. Las decisiones de adjudicación o de evaluación de ofertas cuentan con intervención humana del área competente.

El ejercicio está sujeto a las excepciones legales. La Universidad verificará la legitimidad de la solicitud —incluida la representación de la persona jurídica— y responderá dentro del término de diez (10) días previsto en el artículo 62 de la LOPDP.

Las solicitudes se dirigirán al Delegado de Protección de Datos Personales, al correo **protecciondedatos@indoamerica.edu.ec** o por escrito en las secretarías de las sedes, acreditando identidad y, de ser el caso, la representación. Las resuelve la unidad de compras o la unidad competente, con la supervisión del Delegado.

Si el titular no está satisfecho, puede presentar una reclamación ante la Superintendencia de Protección de Datos Personales, por los canales que esa Autoridad habilite.

9. Protección de datos personales

Solo acceden a los datos las personas que los necesitan para gestionar la relación con el proveedor o para las finalidades de esta política. Se aplican medidas técnicas, organizativas, administrativas y jurídicas orientadas a la confidencialidad, integridad y disponibilidad de la información, revisadas periódicamente.

Quienes intervengan en el tratamiento están obligados a guardar confidencialidad, incluso después de terminar su vínculo con la Universidad, salvo las excepciones legales.

El personal del proveedor que acceda a campus o a sistemas institucionales deberá cumplir las políticas de seguridad de la información y de uso aceptable que se le notifiquen, y no podrá copiar, extraer ni tratar datos de estudiantes, docentes o trabajadores para finalidades ajenas al contrato.

10. Supervisión de cumplimiento

El Delegado de Protección de Datos Personales supervisa internamente el cumplimiento de esta política. El titular puede reclamar ante la Superintendencia de Protección de Datos Personales.

11. Tiempo de conservación de datos personales

Los plazos se determinan según el tipo de dato y la norma que lo regula:

- Mientras dure el procedimiento de selección y la relación contractual, y el tiempo adicional indispensable para pagos, garantías, liquidación y atención de reclamos.
- Documentación tributaria, contable y de facturación: los plazos de la normativa tributaria y societaria aplicable.
- Expedientes de contratación pública, cuando el proceso se haya sujeto a la LOSNCP, y archivos institucionales: los plazos de SERCOP, Contraloría y de gestión documental.
- Registro de futuras invitaciones (consentimiento): máximo veinticuatro (24) meses, renovable, revocable. Al vencimiento, eliminación o anonimización del contacto, sin perjuicio del expediente si hubo contrato.
- Registros de acceso y videovigilancia: el plazo de la Política de Videovigilancia, que no excede de noventa (90) días, salvo incidente o requerimiento de autoridad.

En canales digitales podrán existir plazos adicionales en las Políticas de Cookies. Transcurridos los plazos, se cesará el tratamiento y se procederá a la eliminación, anonimización o bloqueo, conforme a la LOPDP y al RGLOPDP.

12. Actualización de esta política

La Universidad podrá actualizar esta política por cambio normativo, instrucciones de la Autoridad, resultado del RAT o variación sustancial de los procesos de compras. La versión vigente se publicará en www.indoamerica.edu.ec, en la sección de protección de datos o privacidad.

Última actualización: 15 de septiembre del 2026.

Se recomienda al proveedor y a sus representantes consultarla periódicamente mientras subsista el registro o el contrato.

13. Aceptación y consentimientos específicos

La Universidad podrá recabar esta aceptación en formato físico o electrónico, incluyendo casillas en portales de proveedores u órdenes de compra, siempre que se preserve evidencia del consentimiento, de la versión de la política aceptada y de la fecha.

Con la aceptación o con la presentación de una oferta, factura o registro de proveedor en los canales institucionales, el titular declara haber sido informado del tratamiento necesario para evaluar, contratar y ejecutar la relación (secciones 5 y 6.1 a 6.3), que no se funda en su consentimiento.

Los tratamientos opcionales se autorizan solo si se marcan las casillas correspondientes.

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

☐ Autorizo que mis datos de contacto e identificación se conserven en el registro de proveedores para futuras invitaciones o cotizaciones, por hasta veinticuatro (24) meses o hasta que revoque esta autorización.

☐ Autorizo que la Universidad contacte las referencias comerciales o profesionales que he consignado.

La falta de marcado de la base de futuras invitaciones no impide participar en un proceso ya iniciado ni ejecutar un contrato vigente. La falta de datos indispensables para pagar, facturar o verificar la representación sí puede impedir vincular o mantener al proveedor.