



**Escuela de Conducción
MIGUEL ITURRALDE**

**POLÍTICA INTERNA DE PROTECCIÓN
DE DATOS PERSONALES**



POLÍTICA INTERNA DE PROTECCIÓN DE DATOS PERSONALES PIPDP

1. POLÍTICA INTERNA DE PROTECCIÓN DE DATOS PERSONALES ECMI.

CONSIDERACIONES

Que, el numeral 19 del artículo 66 de la Constitución de la República del Ecuador les reconoce y garantiza el derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de carácter personal;

Que, la Ley Orgánica de Protección de Datos Personales (LOPDP) y su normativa conexas establecen los principios, derechos, obligaciones y responsabilidades aplicables al tratamiento de datos personales;

Que, los institutos superiores tecnológicos, en el ejercicio de sus funciones sustantivas de docencia, investigación, vinculación con la sociedad y gestión administrativa, realizan tratamiento de datos personales de estudiantes, docentes, personal administrativo, proveedores y terceros;

Que los artículos 67 y 68 de la LOPDP tipifican las conductas que, respectivamente, son consideradas como infracciones leves e infracciones graves del responsable del tratamiento, de la misma manera que lo hacen los artículos 69 y 70, en su orden, respecto del encargado;

Que los numerales 2 y 5 del artículo 76 de la LOPDP le atribuyen a la SPDP, entre otras funciones, atribuciones y facultades, la de “*ejercer la potestad sancionadora respecto de responsables, delegados, encargados y terceros (...)*”, así como la de “*emitir normativa general o técnica, criterios y demás actos que sean necesarios para el ejercicio de sus competencias y la garantía del ejercicio del derecho a la protección de datos personales*”.

Que, es obligación institucional adoptar políticas claras, transparentes y auditables que garanticen el tratamiento lícito, seguro y responsable de los datos personales;

En uso de sus atribuciones legales y reglamentarias, la Escuela de Formación Conductores No Profesionales Miguel Iturralde expide la presente Política Interna de Protección de Datos Personales (PIPDP), de cumplimiento obligatorio para todos sus estudiantes, docentes, personal administrativo, proveedores y terceros vinculados conforme a la Ley Orgánica de Protección de Datos Personales (LOPDP).



POLÍTICA GENERAL DE PROTECCIÓN DE DATOS PERSONALES

CAPÍTULO I: OBJETO, ÁMBITO Y GLOSARIO DE TÉRMINOS

Artículo. 1.- Introducción y objeto

La presente Política Interna de Protección de Datos Personales (en adelante, la *Política*) se fundamenta en las mejores prácticas nacionales e internacionales relacionadas con el tratamiento de datos personales, y tiene como finalidad fortalecer los mecanismos de control institucional, garantizar un uso lícito, leal, transparente y seguro de la información, y proteger los datos personales de todas las personas que mantienen relación con la Escuela de Formación Conductores No Profesionales Miguel Iturralde (ECMI), incluyendo estudiantes, docentes, personal administrativo, proveedores, aliados estratégicos y demás actores vinculados.

Esta Política se enmarca en lo dispuesto por la Ley Orgánica de Protección de Datos Personales (LOPD) y su normativa complementaria, y se articula con los lineamientos internos, reglamentos, procedimientos y protocolos que integran la política interna de Protección de Datos Personales del Instituto. El objetivo principal de la presente Política es establecer los principios, mecanismos, criterios y lineamientos que regulen el tratamiento de los datos personales, en estricto cumplimiento de la Ley Orgánica de Protección de Datos Personales del Ecuador y su normativa aplicable, garantizando la protección integral de la información y el respeto de los derechos de los titulares. A través de este marco normativo, la ECMI establece principios, responsabilidades, medidas técnicas y organizativas, y controles de seguridad orientados a prevenir riesgos, accesos no autorizados, pérdidas, alteraciones o divulgaciones indebidas de información.

Artículo 2.- Ámbito de Aplicación

La presente Política es de aplicación obligatoria para todas las personas naturales y jurídicas que mantengan relación directa o indirecta con la ECMI, incluyendo empleados, docentes, estudiantes, personal administrativo, proveedores, contratistas, aliados estratégicos, contrapartes y cualquier otro actor vinculado a el instituto. Su observancia es de carácter obligatorio y constituye un compromiso institucional orientado a garantizar el adecuado tratamiento y la protección de los datos personales.

Artículo 3.- Disposiciones para la protección de datos personales

La ECMI, mediante la Política, establece las disposiciones para el tratamiento adecuado y correcto de los datos personales a los cuales tenga acceso para el cumplimiento de su operación. De conformidad con el régimen jurídico aplicable, prevalecerá el derecho de toda persona natural a



la protección de sus datos personales, a la confidencialidad, al tratamiento de estos de acuerdo con los principios enmarcados en la LOPDP.

Artículo 4.- Glosario de términos y abreviaturas. A efectos de la presente política, se tomarán en consideración las siguientes definiciones:

Alumnos: Toda persona que empieza su carrera en el instituto y concluye sus niveles de estudio

Base de datos o ficheros: Conjunto de información perteneciente a un mismo contexto, ordenada de modo sistemático para su análisis, almacenamiento, organización recuperación o transmisión.

Cookies: Archivos de información que sirven de identificador y se almacenan en el computador de un usuario de un sitio web. A menudo se utilizan para gestionar preferencias del usuario y para personalización de los sitios web.

Comunidad institucional: se compone de estudiantes, directivos, personal académico, personal de apoyo académico, personal administrativo y de servicios.

Consentimiento: Manifestación de la voluntad libre, específica, informada e inequívoca, por el que el titular de los datos personales autoriza al responsable del tratamiento de los datos personales a tratar los mismos.

Dato biométrico: Dato personal único, relativo a las características físicas o fisiológicas, o conductas de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre otros.

Datos de acceso a sistemas: Datos relativos a usuarios y contraseñas para ingreso a plataformas e interfaces.

Datos de navegación: Datos relativos al historial de navegación en páginas web de un usuario con sus credenciales. o con los equipos del instituto.

Datos personales: Datos que identifican o hacen identificable a una persona natural, directa o indirectamente.

Datos personales crediticios: Datos que integran el comportamiento económico de personas naturales, para analizar su capacidad financiera.

Datos de salud: datos personales relativos a la salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

Datos sensibles: Datos relativos a etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, sexo biológico, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda



dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.

Encargado del tratamiento de datos personales: Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo que solo o conjuntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales.

Exestudiante: persona que, habiendo sido admitida en alguna experiencia de aprendizaje en el instituto, interrumpió sus estudios y, por lo tanto, no obtuvo titulación o certificación alguna.

Ley Orgánica de Protección de Datos Personales: Ley que norma el tratamiento de datos personales realizado por empresas públicas y privadas, a fin de garantizar el derecho constitucional de protección de datos personales, su abreviatura es LOPDP.

Medidas o controles: Se entiende por tales aquellas aceptadas por el estado de la técnica, sean estas organizativas, técnicas o de cualquier otra índole.

Protección de datos: Es el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de tal carácter, así como su correspondiente protección.

Responsable de tratamiento de datos personales: persona natural o jurídica, pública o privada, autoridad, u otro organismo, que solo o juntamente con otros decide sobre la finalidad y el tratamiento de datos personales.

Seguridad de los datos personales: seguridad de la información en el ámbito específico de información clasificada como datos personales.

Terceros: Se entiende como terceros a los representantes de los estudiantes, aspirantes, proveedores, contratistas, jubilados y, en general cualquier persona natural o jurídica que mantenga una relación con el instituto.

Titulares de datos personales: Persona natural cuyos datos son objeto de tratamiento. Se considerará titulares a todos los miembros del instituto, exestudiantes y jubilados, abarcando todas las sedes y campus del instituto.

Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recolección, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión,



comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales.

Vulneración de la seguridad de los datos personales: Incidente de seguridad que afecta la confidencialidad, disponibilidad o integridad de los datos personales.

CAPÍTULO II: DEL TRATAMIENTO DE DATOS PERSONALES

Artículo 5.- Identificación del Responsable de Tratamiento. De conformidad con lo dispuesto en la LOPDP se desprende la siguiente información:

Responsable de Tratamiento: Escuela de Formación de Conductores No profesionales Miguel Iturralde, (en adelante la “ECMI” o el “Responsable del Tratamiento”)

Número de RUC: 1793194672001

Dirección: Av. Matilde Álvarez y Hugo Díaz Romero. Sector Chillogallo Quito-Ecuador.

Número de teléfono: 3032894 / 0969064410

Correo electrónico: dpd@istpet.edu.ec

Artículo 6.- Tipos de tratamiento. La ECMI podrá realizar cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: recolección, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales de los titulares.

Por medio de esta política, el Instituto declara que ha tomado todas las medidas organizativas, jurídicas y técnicas para salvaguardar la confidencialidad, integridad y disponibilidad de los datos de los titulares.

Artículo 7.- Datos que se recolectan. El Instituto a través de sus sistemas de procesamiento de información, recolecta legítimamente en forma física o digital, la siguiente información:

- a) Datos biométricos;
- b) Datos crediticios;
- c) Datos personales;
- d) Datos de acceso a sistemas;
- e) Datos de navegación;



- f) Categorías especiales de datos y datos sensibles: datos de niñas, niños y adolescentes, datos de salud y datos de personas con discapacidad y de sus sustitutos relativos a la discapacidad.

Artículo 8.- Finalidad del tratamiento de datos personales. La finalidad del tratamiento de los datos personales corresponde a cada una de las actividades de tratamiento que realiza el Instituto para el cumplimiento de sus funciones sustantivas y que se encuentran accesibles en el Registro de Actividades de Tratamiento.

Si el instituto necesita tratar datos personales de los titulares para otros fines informará, en cumplimiento de la LOPDP, a los titulares con anticipación antes de proceder al tratamiento de sus datos.

Artículo 9.- Base legal del tratamiento de datos personales. El tratamiento de datos personales realizado por el Instituto es legítimo y lícito conforme lo previsto en el artículo 7 de La Ley Orgánica de Protección de Datos Personales cuando se cumpla una de las siguientes condiciones:

- a) Por consentimiento del titular para una o varias finalidades;
- b) En cumplimiento de una obligación legal por parte del Instituto;
- c) En cumplimiento de orden judicial, debiendo observarse los principios de la LOPDP;
- d) En cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos en el instituto;
- e) Para la ejecución de medidas precontractuales a petición del titular o para el cumplimiento de obligaciones contractuales perseguidas por el instituto, por el encargado de tratamiento de datos personales o un Tercero legalmente habilitado;
- f) Para proteger intereses vitales del interesado o de otra persona natural, como su vida, salud o integridad;
- g) Para tratamiento de datos personales que consten en bases de datos de acceso público;
- h) Para satisfacer un interés legítimo de la PUCE o de un tercero, siempre que no prevalezca el interés o derechos fundamentales de los titulares al amparo de lo dispuesto en la LOPDP.

Artículo 10.- Responsabilidades de los integrantes del Comité

Responsable del tratamiento

Rol de responsable

En general, el rol del responsable de tratamiento de Datos Personales, abarca las obligaciones previstas en el art. 47 de la LOPDP:



- a) Tratar datos personales en estricto apego a los principios y derechos desarrollados en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia;
- b) 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, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia;
- c) Aplicar e implementar procesos de verificación, evaluación, valoración periódica de la eficiencia, eficacia y efectividad de los requisitos y herramientas administrativas, Técnicas, físicas, organizativas y jurídicas implementadas;
- d) Implementar políticas de protección de datos personales afines al tratamiento de datos personales en cada caso en particular;
- e) Utilizar metodologías de análisis y gestión de riesgos adaptadas a las particularidades del tratamiento y de las partes involucradas;
- f) Realizar evaluaciones de adecuación al nivel de seguridad previas al tratamiento de datos personales;
- g) Tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas;
- h) Notificar a la Autoridad de Protección de Datos Personales y al titular de los datos acerca de violaciones a las seguridades implementadas para el tratamiento de datos personales conforme a lo establecido en el procedimiento previsto para el efecto;
- i) Implementar la protección de datos personales desde el diseño y por defecto;
- j) Suscribir contratos de confidencialidad y manejo adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales;
- k) Asegurar que el encargado del tratamiento de datos personales ofrezca mecanismos suficientes para garantizar el derecho a la protección de datos personales conforme a lo establecido en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, normativa sobre la materia y las mejores prácticas a nivel nacional o internacional;
- l) Registrar y mantener actualizado el Registro Nacional de Protección de Datos Personales, de conformidad a lo dispuesto en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales;
- m) Designar al Delegado de Protección de Datos Personales, en los casos que corresponda;



- n) Permitir y contribuir a la realización de auditorías o inspecciones, por parte de un auditor acreditado por la Autoridad de Protección de Datos Personales; y,
- o) Los demás establecidos en la presente Ley en su reglamento, en directrices, lineamientos, regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

Por efectos internos, el área que desempeñara internamente como responsable del tratamiento es el coordinador de cada unidad o coordinación, por medio de su coordinador o responsable de la unidad.

Encargado del tratamiento

La ECMI, son los encargados del tratamiento, son cada una de las coordinaciones o unidades que tratan datos personales de acuerdo con las definiciones del responsable del tratamiento.

Rol de Encargado

Los encargados de tratamiento de Datos Personales, entre otras, cumplirán con las siguientes obligaciones:

- a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
- b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
- c) Realizar la actualización, rectificación o supresión de los Datos Personales en los términos de la LOPDP;
- d) Actualizar la información reportada por el responsable del Tratamiento;
- e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en las Políticas y en la LOPDP;
- f) Anotar en la Base de Datos Personales la leyenda “información en discusión judicial” una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del Dato Personal;
- g) Abstenerse de circular información que esté siendo controvertida por el Titular;
- h) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;
- i) Informar al responsable cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares; y,
- j) Cumplir las instrucciones y requerimientos que imparta el responsable.



CAPÍTULO III

Artículo 11.- Principios del tratamiento de datos

El tratamiento de datos personales por parte de la ECMI se realizará en cumplimiento con los principios enmarcados en el Art. 10 de la LOPDP, y los que especialmente se resaltan en esta Política:

- a) **Principio de Juridicidad:** El tratamiento de datos personales deberá efectuarse con estricto apego a la Constitución, los instrumentos internacionales, la LOPDP, su Reglamento, la normativa secundaria y la jurisprudencia aplicable, garantizando el respeto de los derechos y obligaciones en materia de protección de datos.
- b) **Principio de Lealtad:** El tratamiento de datos personales deberá realizarse de forma leal y legítima, garantizando que los titulares conozcan que sus datos están siendo recolectados, utilizados, consultados o tratados, así como las modalidades de dicho tratamiento. En ningún caso los datos podrán tratarse mediante medios o para fines ilícitos o desleales.
- c) **Principio de Transparencia:** Toda información o comunicación relacionada con el tratamiento de datos personales deberá ser clara, accesible y comprensible, utilizando un lenguaje sencillo. Las relaciones derivadas del tratamiento se regirán por las disposiciones establecidas en la LOPDP y la normativa vigente.
- d) **Principio de Finalidad:** Las finalidades del tratamiento deberán ser determinadas, explícitas, legítimas y comunicadas al titular; no podrán tratarse datos personales con fines distintos para los cuales fueron recopilados, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en la LOPDP; Principio de Pertinencia y minimización de datos personales: Los datos personales deben ser pertinentes y estar limitados a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento;
- e) **Principio de Proporcionalidad del tratamiento:** El tratamiento debe ser adecuado, necesario, oportuno, relevante y no excesivo con relación a las finalidades para las cuales hayan sido recogidos o a la naturaleza misma de las categorías especiales de datos;
- f) **Principio de Confidencialidad:** El Tratamiento de datos personales debe concebirse sobre la base del debido sigilo y secreto, es decir, no debe tratarse o comunicarse para un fin distinto para el cual fueron recogidos, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en la LOPDP;



- g) **Principio de Calidad y exactitud:** Los datos personales que sean objeto de tratamiento deben ser exactos, íntegros, precisos, completos, comprobables, claros; y, de ser el caso, debidamente actualizados; de tal forma que no se altere su veracidad. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para que se tratan. En caso de tratamiento por parte de un encargado, la calidad y exactitud será obligación del responsable del tratamiento de datos personales;
- h) **Principio de Conservación:** Los datos personales serán conservados durante un tiempo no mayor al necesario para la finalidad de su tratamiento; y,
- i) **Principio de Seguridad de datos personales:** Los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas y necesarias, entendiéndose por tales, las aceptadas por el estado de la técnica, sean estas organizativas, técnicas o de cualquier otra índole, para proteger los datos personales frente a cualquier riesgo, amenaza, vulnerabilidad, atendiendo a la naturaleza de los datos de carácter personal, al ámbito y el contexto.

Estos principios prevalecerán en: el diseño, desarrollo e implementación de todos los procedimientos que impliquen el tratamiento de datos personales; todos los contratos y obligaciones que formalice la ECMI con personas naturales o jurídicas; y, la implantación de cuantos sistemas y plataformas permitan el acceso, por parte de los funcionarios de la ECMI y/o de terceros, a datos personales y el tratamiento de dichos datos.

Artículo 12.- Tratamiento y Finalidades de los Datos Personales

La ECMI, actuando en calidad de Responsable y/o Encargado, según sea el caso, del tratamiento de Datos Personales: recolecta, almacena, usa, circula, transfiere y suprime Datos Personales correspondientes a personas naturales y jurídicas con quienes tiene o ha tenido relación o que accede como consecuencia de relaciones comerciales, civiles o contractuales, tales como, sin que la enumeración signifique limitación: trabajadores y familiares de éstos, clientes y proveedores, para los siguientes propósitos o finalidades:

- a) Controlar el acceso a sus oficinas y establecer medidas de seguridad, incluyendo áreas de videovigilancia;
- b) Dar respuesta a consultas, peticiones, quejas y reclamos efectuados por los Titulares y órganos de control; así como, transmitir los Datos Personales a las demás autoridades, que en virtud de la ley aplicable deban recibirlos;
- c) Para eventualmente contactar, vía correo electrónico o por cualquier otro medio, a personas naturales con quienes tiene o ha tenido relación, tales como, sin que la



- enumeración signifique limitación, trabajadores y familiares de éstos, accionistas, clientes y proveedores, estudiantes, docentes, para las finalidades antes mencionadas;
- d) Registrar sus datos personales en los sistemas de información y en sus bases de datos;
 - e) Cualquier otra actividad de naturaleza similar a las anteriormente descritas que sea necesaria para desarrollar su objeto principal: formar profesionales con solvencia ética y académica; y, generar y transferir conocimientos científicos y tecnológicos para contribuir a las necesidades de la sociedad y al desarrollo del país.

En general, la ECMI tratará la información que se le facilite con la finalidad de gestionar la relación que les une, gestionar el envío de la información que se solicita, facilitar a los interesados ofertas de nuestros servicios y/o productos de su interés y/o gestionar su candidatura o admisión.

Los Datos Personales que se pudieran recabar directamente de la persona interesada serán tratados de forma confidencial y quedarán incorporados a la correspondiente actividad de tratamiento titularidad de la ECMI. La relación actualizada de las actividades de tratamiento que la ECMI lleva a cabo, así como la finalidad de cada tratamiento, se encuentra disponible en el área de Secretaría General.

Artículo 13.- Legitimación para el tratamiento de Datos Personales

Según el caso, las bases legales que habilitan al ECMI a tratar los Datos Personales son la siguientes:

- a) El interesado otorgo su autorización/consentimiento para el tratamiento de sus Datos Personales para uno o varios fines específicos;
- b) El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
- c) El tratamiento es necesario para el cumplimiento de una obligación legal aplicable en la ECMI;
- d) El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
- e) El tratamiento es necesario para el cumplimiento de una misión.

Artículo 14.- Destinatarios de los Datos Personales

Con carácter general no se comunicarán los datos personales a terceros, salvo obligación legal, entre las que pueden estar las comunicaciones a autoridades de control, Jueces y Tribunales.



CAPÍTULO IV

Artículo 15.- Derechos de los Titulares de los Datos Personales

Las personas naturales cuyos Datos Personales sean objeto de tratamiento por parte de la ECMI, tienen los derechos previstos en el régimen jurídico aplicable, en particular al LOPDP. Sin perjuicio, en cualquier momento pueden:

- a) Conocer los Datos Personales sobre los cuales la ECMI está realizando el tratamiento. De igual manera, el titular puede solicitar en cualquier momento, que sus datos sean actualizados o rectificados;
- b) Solicitar prueba de la autorización otorgada la ECMI o a sus clientes (responsables del tratamiento), para el tratamiento de sus Datos Personales;
- c) Ser informado por la ECMI, previa solicitud, respecto del uso que ésta le ha dado a sus Datos Personales;
- d) Solicitar al ECMI la supresión de sus Datos Personales y/o revocar la autorización otorgada para el tratamiento de estos. La solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el titular de la información tenga un deber legal o contractual de permanecer en la base de datos y/o archivos, ni mientras se encuentre vigente la relación entre el Titular y la ECMI o sus clientes (responsables del tratamiento), en virtud de la cual fueron recolectados sus datos; y,
- e) Acceder de forma gratuita a los Datos Personales que hayan sido objeto de tratamiento.

Estas solicitudes o requerimientos originados por los titulares de datos personales serán debidamente atendidas por la ECMI en aquellos casos en los que fuere directamente responsable del tratamiento de los datos personales sobre los que verse la petición.

Los lapsos de atención y el procedimiento interno se ajustan a las previsiones de la LOPDP, es por ello, que serán atendidas antes del cumplimiento del término legal y, serán respondidas directamente por el responsable interno identificado de la ECMI.

CAPÍTULO V

Artículo 16.- Deberes de la ECMI como responsable del Tratamiento de Datos Personales

La ECMI tiene presente que los Datos Personales son de propiedad de las personas a las que se refieren y solamente ellas pueden decidir sobre los mismos. En ese sentido, hará uso de los Datos Personales recolectados únicamente para las finalidades para las que se encuentra debidamente facultadas y respetando, en todo caso, la normatividad vigente sobre la Protección de Datos



Personales en Ecuador, en particular, la LOPDP, su Reglamento y disposiciones de la Autoridad de Protección de Datos.

1. Autorización/Consentimiento

La ECMI solicitará autorización/consentimiento de manera previa, libre, expresa, inequívoca e informada a los titulares de los Datos Personales sobre los que requiera realizar el Tratamiento. Esta manifestación de voluntad del Titular puede darse por medio de diferentes mecanismos puestos a disposición por la ECMI, tales como:

- a) Por escrito, diligenciando un formato de autorización (medios físicos o electrónicos) para el tratamiento de Datos Personales determinado por la ECMI;
- b) Vía digital mediante la aceptación de la matrícula, o a su vez la aceptación de las medidas de cookies plasmadas en las páginas web institucionales.
- c) De forma oral, a través de una conversación telefónica o en videoconferencia; y,
- d) Mediante conductas inequívocas que permitan concluir que otorgó su autorización/consentimiento, a través de su aceptación expresa a los términos y condiciones de una actividad dentro de los cuales se requiera la autorización de los participantes para el Tratamiento de sus Datos Personales.

En ningún caso la ECMI asumirá el silencio del titular como una conducta inequívoca.

2. Disposiciones Especiales para el Tratamiento de Datos Personales

2.1. Datos Personales de Naturaleza Sensible.

La ECMI para el tratamiento de los Datos Personales de naturaleza sensible, además de cumplir con los requisitos establecidos para la autorización/consentimiento, informará al Titular:

- (i) Que por tratarse de datos sensibles no está obligado a autorizar su tratamiento; y,
- (ii) Cuáles de los datos que serán objeto de tratamiento son sensibles y la finalidad del tratamiento.

Adicionalmente, la ECMI tratará los datos sensibles recolectados bajo estándares de seguridad y confidencialidad correspondientes a su naturaleza.

2.2. Datos Personales de Niños, Niñas y Adolescentes

La ECMI únicamente realizará el tratamiento correspondiente de Datos Personales de niños, niñas y adolescentes, cuando sea necesario en la ejecución de los proyectos de las funciones sustantivas que tiene el instituto como son Vinculación e Investigación que responda y respete su interés superior y asegure el respeto de sus derechos fundamentales. La ECMI deberá obtener la autorización/consentimiento del representante legal del niño, niña o adolescente para dicho tratamiento, salvo los casos de adolescentes mayores de quince (15) años y menores de dieciocho



(18) años, puesto que en base al artículo 24 de la LOPDP, podrán ejercitarlos de forma directa ante la Autoridad de Protección de Datos Personales o ante el responsable del Tratamiento de Datos Personales.

3. Seguridad de los Datos Personales

En base al cumplimiento del principio establecido, la ECMI adoptará las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los Datos Personales evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. La obligación y responsabilidad de la ECMI se limita a disponer de los medios adecuados para este fin.

La ECMI exigirá a los proveedores de servicios que contrata, la adopción y cumplimiento de las medidas técnicas, humanas y administrativas adecuadas para la protección de los Datos Personales en relación con los cuales los proveedores actúen como encargados de tratamiento.

4. Transferencia, Transmisión y Revelación de Datos Personales

La ECMI podrá entregar los Datos Personales a terceros no vinculados a ésta, por lo tanto, cuando se envíe o transmita datos a uno o varios encargados de tratamiento, establecerá cláusulas contractuales o celebrará acuerdos en los que, entre otros, se establecerá lo siguiente:

- a) Los alcances y finalidades del tratamiento;
 1. Las actividades que el Encargado realizará en nombre de la ECMI;
 2. Las obligaciones que debe cumplir el encargado de tratamiento respecto del titular del dato personal y de la ECMI;
 3. El deber del encargado de tratamiento de tratar los datos personales de acuerdo con la finalidad autorizada para el mismo, observando los principios establecidos en la LOPDP e indicaciones de la Política;
- b) La obligación del encargado de tratamiento de proteger adecuadamente los datos personales y las bases de datos, así como de guardar confidencialidad respecto del tratamiento de los datos personales transmitidos; y,
- c) Una descripción de las medidas de seguridad concretas que van a ser adoptadas tanto por la ECMI como por el encargado de tratamiento de los datos en su lugar de destino.

La ECMI no solicitará la autorización cuando la transferencia de datos se encuentre amparada en alguna de las excepciones previstas en la LOPDP o normativa complementaria vigente.

5. Información obtenida en forma pasiva

Cuando se accede al contenido de la sede electrónica de la ECMI, ésta podrá recopilar información en forma pasiva a través de tecnologías para el manejo de la información, tales como



“cookies”, a través de los cuales se recolecta información acerca de sesiones, número de usuarios, tiempo de sesión, porcentaje de rebote del sitio web, idioma, país, ciudad y sistema operativo; mediante el uso de estas herramientas no se recolectan directamente Datos Personales de los usuarios.

No obstante, el usuario de los sitios web de la ECMI tiene la posibilidad de configurar el funcionamiento de las “cookies”, de acuerdo con las opciones de su navegador de internet.

6. Legislación Aplicable

La Política de Protección de Datos Personales de la ECMI se rige por lo dispuesto en el régimen jurídico aplicable de la República del Ecuador, en particular, la LOPDP, su Reglamento y disposiciones de la Autoridad Nacional de Protección de Datos Personales, y demás normativa complementaria que se expida para el efecto.

7. Responsabilidad

La ECMI, confiere la responsabilidad sobre la gestión para la protección de los datos personales a la unidad o Departamento designada como responsable para fines internos del tratamiento de Datos Personales. La Unidad o Departamento que deberá establecer directrices y orientación, incluyendo el control y la coordinación de tareas en el ámbito de la gestión de la protección de los Datos Personales, lo cual incluye, pero no se limita a la atención de peticiones, consultas, quejas y reclamos, ante la cual el titular de la información podrá ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización. Este responsable puede ser ubicado en la siguiente dirección: dpd@istpet.edu.ec

8. Transmisión y Transferencia de Datos Personales

Para la Transmisión de los Datos Personales de los Titulares, así como para cualquier Transmisión que la ECMI efectúe para el cumplimiento de las finalidades del tratamiento o para delegar el tratamiento en un tercero que se convierta en encargado, la ECMI tomará todas las medidas que sean necesarias para garantizar el cumplimiento de la presente Política, así como para garantizar al Titular el ejercicio de sus derechos.

En el evento en que la ECMI transfiera temporal o definitivamente los Datos Personales a un tercero, dentro o fuera del país, caso en el cual dicho tercero se convertirá en el responsable del tratamiento de los Datos Personales, tomará las medidas necesarias para preservar los derechos de los titulares durante la transferencia.

La ECMI podrá comunicar, transmitir o transferir sus datos personales a terceros localizados dentro o fuera del territorio nacional. Ante comunicaciones de esta naturaleza, la ECMI garantiza que lo hará con las garantías adecuadas establecidas en la legislación vigente y enviará la



información a puertos seguros de información. La información personal de los titulares podrá ser comunicada a las empresas que prestan servicios al Instituto, sea que se localicen dentro o fuera del país, a los establecimientos de comercio y aliados comerciales con los que tenga una relación contractual vigente para el cumplimiento de las finalidades autorizadas por los titulares, y a terceros que requieran la información para su tratamiento de acuerdo con las finalidades contenidas en la presente Política.

11.- Seguridad

La ECMI garantiza que cumplirá con el deber de confidencialidad sobre los Datos Personales del titular y los conservará hasta que el titular comunique su voluntad de darse de baja o mientras existan obligaciones legales o contractuales que justifiquen mantener los datos, de acuerdo con la política vigente. La ECMI adoptará las medidas de seguridad exigidas por la legislación aplicable para evitar, en relación con los Datos Personales del titular, su alteración, pérdida, tratamiento o acceso no autorizado, siempre de acuerdo con el estado de la tecnología disponible. Y se debe regir a la política de seguridad de la información

12.- Tiempo de Conservación

El tiempo requerido para la debida prestación y operación de los servicios que brinda la ECMI. La conservación ampliada de tratamiento de datos personales únicamente se realizará con fines de archivo en interés público, fines de investigación científica, histórica o estadística, siempre y cuando se establezcan las garantías de seguridad y protección de datos personales, oportunas y necesarias.

En concordancia con la normativa vigente en el Ecuador, los plazos de conservación de datos personales se ajustarán a lo dispuesto en la Ley Orgánica de Protección de Datos Personales (LOPD) y en la normativa sectorial aplicable, de acuerdo con las siguientes referencias:

- **Documentos tributarios y financieros:** Conforme al Servicio de Rentas Internas (SRI) exige conservar comprobantes y registros contables por 7 años para efectos de fiscalización.
- **Registros laborales y nómina:** Conforme al Ministerio de Trabajo y normativa de seguridad social requieren conservar expedientes laborales y aportes al IESS por al menos 15 años.
- **Registros académicos:** Mínimo 7 años o conservación permanente, conforme a las disposiciones del Ministerio de Educación Superior y buenas prácticas de gestión documental.
- **Historias clínicas y datos de salud:** Conforme a la Normativa sanitaria ecuatoriana exige conservar historias clínicas por 15 años desde la última atención.



La ECMI garantizará que, cumplidos los plazos legales de conservación, los datos personales serán eliminados, anonimizados o archivados bajo medidas de seguridad que aseguren la protección de los derechos de los titulares.

Vigencia

Esta Política Interna de Protección de Datos Personales está vigente desde el mes de noviembre del 2025.

CAPITULO VI

Artículo 17.- Registro de actividades de tratamiento

Sobre la base de las reuniones mantenidas y las capacitaciones brindadas al personal de la ECMI, se pudo evidenciar los diferentes tratamientos de datos personales que efectúa el instituto en el ejercicio del cumplimiento de su objeto y misión. A continuación, se proporciona el registro de aquellas actividades de tratamiento.

Artículo 18.- Actividades Académicas

Las actividades académicas que realiza el Instituto se encuentran enfocadas a todas las operaciones que se realizan dentro del marco del proceso de enseñanza aprendizaje, encaminadas a reforzar los conocimientos adquiridos en el aula, a desarrollar nuevas habilidades y vincular al alumno con su campo de trabajo y con su entorno social. Las actividades académicas que necesitan tratamiento en el instituto se dividen en: actividades de investigación, actividades de vinculación, Educación Continua, actividades pedagógicas y estudios generales, actividades de planificación y registro académico, actividades de educación online y actividades de dirección académica.

Actividades Financieras y Administrativas.

Breve descripción del tipo de actividades que requieren tratamiento	Las actividades financieras y administrativas que requieren tratamiento en el Instituto están enfocadas en la gestión, registro, actualización y almacenamiento de la información económico-financiera de la ECMI. Estas acciones comprenden el desarrollo de procesos de facturación de alumnos y representantes, el registro de facturas y pagos a proveedores, así como la presentación de declaraciones de impuestos y el cumplimiento de pagos de contribuciones. De igual manera, se incluyen los pagos internacionales de servidores tecnológicos que garantizan el funcionamiento de las plataformas educativas, y la gestión de gastos en publicidad institucional, asegurando la transparencia y trazabilidad de cada operación financiera.
--	--



Encargado del tratamiento	Dirección Administrativa Financiera
Categoría de datos	El instituto trata datos de carácter personal de estudiantes, trabajadores, personal institucional, representantes y proveedores, que incluyen: nombres completos, apellidos, dirección domiciliaria, correos electrónicos (institucionales y personales), número de cédula, número de teléfono celular y convencional, número de RUC, número de RIMPE, razón social y número de cuentas bancarias.
Finalidades de los datos personales	Los datos de carácter personal de estudiantes y trabajadores y representantes serán utilizados para emitir las facturas correspondientes por el servicio adquirido y para el cobro de los aranceles de las distintas carreras que oferta el Instituto, en cambio los datos de carácter personal de proveedores serán utilizados para el pago de los servicios y bienes adquiridos.
Medidas de seguridad	Los datos de carácter personal de estudiantes, trabajadores, representantes y proveedores se almacenan en los servidores locales del Instituto, aplicando todas las medidas de seguridad tecnológicas implementas por el Instituto, por ningún motivo se compartirá datos de carácter personal o sensible con terceras personas, salvo obligaciones legales.

Actividades de Recursos Humanos

Breve descripción del tipo de actividades que requieren tratamiento	El Departamento de Recursos Humanos ejecuta actividades de carácter técnico, administrativo y normativo orientadas a la gestión integral del talento humano, asegurando el cumplimiento de la normativa vigente y el adecuado funcionamiento institucional. Gestiona los procesos de reclutamiento, selección, inducción y capacitación del personal, así como el levantamiento, actualización y validación de perfiles de cargos en función de los requerimientos institucionales. Administra los beneficios institucionales y desarrolla acciones de reconocimiento y bienestar laboral, garantizando condiciones adecuadas para el desempeño del personal. Es responsable de la administración y custodia de los expedientes del personal, la generación de información para auditorías internas y externas, y el control de asistencia, permisos y vacaciones. De igual forma, organiza y ejecuta concursos de méritos y oposición para la vinculación y promoción del personal docente, conforme a la normativa aplicable. En el ámbito legal y administrativo, gestiona procesos disciplinarios y atiende denuncias internas relacionadas con conflictos laborales, acoso o situaciones que afecten el entorno de trabajo. Administra los procesos vinculados a la nómina, afiliación al IESS, elaboración de contratos,
--	--



	liquidaciones laborales y registros ante el Ministerio de Trabajo. Administra y registra en el sistema contable institucional Megued la información del personal, incluyendo datos personales, cuentas bancarias y valores de remuneración conforme a la escala salarial vigente en el Ecuador. Para el desarrollo de sus funciones, el departamento utiliza herramientas tecnológicas como el sistema contable institucional Megued, que permite el registro y control de la información administrativa y financiera del personal. Asimismo, emplea el sistema Kudert como plataforma especializada para la aplicación de evaluaciones psicológicas en línea, orientadas a medir competencias, rasgos conductuales y aspectos del desarrollo del talento humano. Esta herramienta apoya los procesos de selección, evaluación y desarrollo del personal, proporcionando información relevante para la toma de decisiones en la gestión del talento. El Departamento de Recursos Humanos no tiene bajo su responsabilidad la coordinación de la Unidad de Seguridad y Salud Ocupacional; no obstante, mantiene una articulación funcional con dicha unidad en aspectos relacionados con el bienestar y la prevención de riesgos laborales.
Encargado del tratamiento	Recursos Humanos
Categoría de datos	El departamento trata datos personales y sensibles de trabajadores, docentes, aspirantes, personal administrativo y de servicios del ISTPET, tales como su número de cédula, lugar de nacimiento, nombres completos, apellidos, fecha de nacimiento, nacionalidad, dirección domiciliaria, tiempo de residencia, antecedentes curriculares, reconocimientos académicos, antecedentes laborales y en docencia, fotografías, idiomas, historial laboral y curriculum vitae. Datos de carácter sensible del personal administrativo, docentes y aspirantes tales como datos relativos a la etnia, identidad de género, enfermedades, discapacidades, pertenencia a grupos minoritarios, récord crediticio, situación financiera, datos bancarios, número de cuenta bancaria, huella dactilar, resultados de exámenes ocupacionales y ficha medica ocupacional.



Finalidades de los datos personales	Los datos de carácter personal y sensibles serán utilizados para la contratación, inducción y capacitación del nuevo personal del ISTPET, incluyendo de manera explícita a docentes, trabajadores, personal administrativo y de servicios. Además los datos antes mencionados servirán para gestionar los distintos procesos internos del Instituto, entre estos se encuentran el control de asistencia del personal que se lo realiza por medios electrónicos como son las huellas digitales, la promoción de beneficios institucionales, agasajos y reconocimientos para el personal, la gestión de los distintos procesos disciplinarios al interior del Instituto, la gestión de comunicación, gestión documental de expedientes e información para auditorias y organismos de control, los distintos servicios de atención medica primaria, ocupacional y prevención de riesgos laborales, la coordinación de los distintos concursos de méritos y oposición de docentes del Instituto, la emisión de certificados a petición de cada titular y la gestión de nómina del personal, en beneficio de los intereses institucionales del Instituto.
Medidas de seguridad	Toda la información de carácter personal y sensible serán almacenados de dos formas, en primer lugar, mediante un expediente físico con acceso restringido, bajo custodia y responsabilidad de la Dirección de Talento Humano. En segundo lugar, mediante los distintos sistemas informáticos que se manejan al interior del Instituto, el acceso a esta información únicamente podrá desarrollarse mediante una clave personal, la misma que es otorgada por la Dirección de Talento Humano. La Dirección de Talento Humano y sus encargados garantizan el almacenamiento reservado y la protección de los datos de carácter personal, por ningún motivo se compartirá datos de carácter personal o sensible con terceras personas, salvo obligaciones legales.



Dirección administrativa.

Breve descripción del tipo de actividades que requieren tratamiento	L dirección administrativa de la ECMI se encarga de mantener y gestionar los datos recopilados de los estudiantes, supervisar el cumplimiento de los docentes, coordinar la obtención de permisos ante la Agencia Nacional de Tránsito (ANT), controlar la asistencia mediante fichas y registros, administrar las bitácoras mecánicas y custodiar los archivos institucionales. Es el área principal que centraliza la documentación y asegura la trazabilidad de los procesos académicos y administrativos.
Encargado del tratamiento	Director Administrativo.
Categoría de datos	Se manejan datos personales y académicos de los estudiantes y docentes, tales como: • Datos de identificación (cédula, nombres completos). • Datos de matrícula y asistencia. • Registros de cumplimiento docente. • Permisos y autorizaciones requeridas por la ANT. • Bitácoras mecánicas y fichas de control de asistencia.
Finalidades de los datos personales	Estos datos son indispensables para garantizar la correcta gestión administrativa, el cumplimiento normativo y la coordinación con la ANT, validar la matrícula de los estudiantes, supervisar el cumplimiento de los docentes, gestionar permisos ante la ANT, llevar el control de asistencia y mantener registros mecánicos y administrativos que respalden la formación de conductores no profesionales.
Medidas de seguridad	Los datos se almacenan en archivos físicos y digitales bajo custodia del Departamento Administrativo, con acceso restringido al personal autorizado. Se implementan controles de asistencia y bitácoras mecánicas como parte de la trazabilidad institucional. Por ningún motivo se compartirá datos de carácter personal o sensible con terceras personas, salvo obligaciones legales.



Actividades de Educación online

Breve descripción del tipo de actividades que requieren tratamiento	Las actividades de educación online para todas las carreras que oferta el instituto que necesitan tratamiento se encuentran enfocadas en la administración de plataformas de Ingles y Moodle, en dichas plataformas los estudiantes pueden compartir, cargar y modificar tareas que contienen información de carácter personal, además en dichas plataformas los estudiantes pueden observar clases pre grabadas, calificaciones y comunicaciones por parte de sus docentes. Es importante conocer que, para el correcto funcionamiento de las plataformas antes mencionadas, los docentes deben realizar un proceso de virtualización de contenidos, cediendo de manera voluntaria y bajo un contrato de servicios profesionales su imagen y su voz Por otro lado, las actividades de educación online del instituto también realizan soporte de helpdesk y capacitación a la comunidad institucional acerca del uso de las plataformas antes mencionadas y las distintas herramientas digitales que manejan en el instituto.
Encargado del tratamiento	Coordinador Académico – Gestor Académico – Coordinadores de carrera
Categoría de datos	Datos de carácter personal de docentes y estudiantes, tales como nombres completos, número de cédula, teléfono celular, correo electrónico personal y correo electrónico institucional, así también las imágenes, audios y videos de docentes que permitan identificarlos.
Finalidades del tratamiento de datos personales	Los datos de carácter personal de docentes y estudiantes son utilizados exclusivamente para la elaboración de videos de bienvenida y virtualización de contenidos, además mediante el uso de los datos de carácter personal de alumnos se efectiviza la matrícula manual de usuarios en cursos de validación de conocimientos, programas de educación continua y cursos complexivos, mediante las grabaciones de clase, reuniones y capacitaciones se efectivizan las actividades académicas de los estudiantes



	matriculados, garantizando el fiel cumplimiento de los distintos propósitos educativos.
Medidas jurídicas de protección de datos	Toda la información de carácter personal de estudiantes y docentes mencionada anteriormente se encuentra bajo la tutela y protección de la Dirección de Educación Online y sus delegados, cabe mencionar que toda la información inmersa en las plataforma Moodle se encuentran almacenadas en servidores tecnológicos externos que tienen su domicilio en Estados Unidos de América, dicha información cuenta con las medidas tecnológicas y técnicas adecuadas para evitar la fuga o transmisión de información que contengan datos de carácter personal. Por lo tanto, por ningún motivo se compartirá con terceras personas datos de carácter personal, salvo obligación legal

Actividades académicas de inspección de la Escuela de conducción.

Breve descripción del tipo de actividades que requieren tratamiento	Las actividades de inspección de la Escuela de Conductores Profesionales se orientan a la supervisión integral del control y acompañamiento académico de estudiantes y docentes, asegurando el cumplimiento de la normativa vigente y la trazabilidad de los procesos formativos. Entre los procesos educativos comprenden: matriculación de estudiantes y docentes en las plataformas académicas institucionales.
Encargado del tratamiento	Inspectores de la Escuela de Conducción Profesional
Categoría de datos	Los datos personales que se manejan dentro del departamento de inspección incluyen: Estudiantes: nombres completos, apellidos, número de cédula, correo institucional y personal, número de teléfono celular, número de referencia familiar y firma manual.



	Docentes: nombres completos, número de cédula, correo institucional y personal, número de teléfono celular.
Finalidades de los datos personales	Matriculación de estudiantes y docentes en las plataformas académicas institucionales (entorno virtual de aprendizaje EVA, PORTAL DOCENTE, PLATAFORMA MICROSOFT) para controlar la asistencia mediante sistemas biométricos y listados físicos/digitales, sirviendo como respaldo en recuperaciones pedagógicas, actividades académicas, realizar seguimiento del desempeño académico de los estudiantes, garantizando trazabilidad y transparencia en el proceso formativo.
Medidas de seguridad	La información se almacenan en registros físicos y digitales bajo custodia institucional, se conserva en las oficinas de Secretaría e Inspección con acceso restringido al personal autorizado, los datos no se comparten con terceros, salvo obligaciones de instituciones gubernamentales.

Actividades Prácticas de la Escuela de conducción.

Breve descripción del tipo de actividades que requieren tratamiento	Las actividades prácticas se enfocan en el registro, coordinación y seguimiento de las clases prácticas de conducción.
Encargado del tratamiento	Coordinador de Prácticas
Categoría de datos	Los datos personales que se manejan en relación con los estudiantes abarcan: Nombres completos, apellidos, correo institucional, número de cedula, número de teléfono celular. Docentes de prácticas: nombres completos, número de cédula, correo institucional y personal, número de teléfono celular. Datos de control: horarios y fechas de prácticas, registro biométrico de asistencia.



Finalidades de los datos personales	Coordinar y asignar horarios y fechas de las prácticas de conducción. Registrar la asistencia de estudiantes y docentes en las clases prácticas. Garantizar la correcta identificación de usuarios internos y externos. Mantener trazabilidad académica y administrativa del proceso formativo.
Medidas de seguridad	Los registros de estudiantes y docentes se almacenan en sistemas digitales y físicos bajo custodia institucional, el acceso a la información está restringido únicamente al personal autorizado. Por ningún motivo se compartirá información personal o sensible con terceros, salvo en casos de obligación legal expresa. La misma información reposa en las oficinas del Departamento de Prácticas, en formato físico y digital.

Actividades del Departamento del Psicosensométrico

Breve descripción del tipo de actividades que requieren tratamiento	El Departamento Psicosensométrico tiene como responsabilidad la evaluación técnica y psicológica de los aspirantes y conductores profesionales, en cumplimiento de los requisitos establecidos por la Agencia Nacional de Tránsito (ANT). Sus actividades incluyen: Aplicación del examen psicosensométrico
Encargado del tratamiento	Personal médico
Categoría de datos	Los datos personales y sensibles que se manejan incluyen: Identificación del estudiante o conductor (nombres y apellidos completos, número de cédula, teléfono, dirección, profesión, tipo de sangre). Fotografía tomada por el departamento para la ficha del examen. Datos de salud: certificado médico, resultados del examen psicosensométrico, test de ansiedad y validación de aptitudes.



	Información académica y administrativa vinculada al proceso de matrícula y renovación de licencias. Datos complementarios: género y firma manual.
Finalidades de los datos personales	Los datos se utilizan para: Aplicación del examen psicosensoométrico requisito previo para la matriculación de estudiantes en la Escuela de Conducción, como requisitos legales y técnicos exigidos por la ANT, tanto para la matriculación de estudiantes como para la renovación de licencias profesionales. Validar la aptitud del conductor y determinar si se encuentra en condiciones de ejercer la actividad de conducción de manera segura.
Medidas de seguridad	La documentación de los resultados y registros fotográficos se almacenan en archivos físicos y digitales bajo custodia institucional, con acceso restringido al personal autorizado. Se aplican protocolos de confidencialidad y reserva, conforme a la Ley Orgánica de Protección de Datos Personales (LOPDP) y política institucional. La información no se comparte con terceros, salvo en casos de obligación legal expresa por parte de entidades de control.

Actividades de secretaría y recaudación

Breve descripción del tipo de actividades que requieren tratamiento	Las actividades de Secretaría y Recaudación de la Escuela de Conducción Miguel Iturralde (ECMI) se enfocan en la gestión administrativa, académica y financiera del proceso de matriculación para la obtención de licencia no profesional Tipo B. Incluyen: • Elaboración de oficios y recepción/validación de documentos previos a la matrícula. • Envío de estudiantes a exámenes psicosensoométricos y test de ansiedad con el médico de planta. • Registro de datos en el sistema de matrículas SIGAFI y en el sistema contable MEGUED. • Ingreso de huellas biométricas para control de asistencia en clases prácticas. • Procesos de recaudación: cobro de matrícula, validación de transferencias y emisión de facturas con datos de identificación, domicilio, correo y teléfono.
--	---



	• Coordinación académica: envío de nómina de alumnos para creación de aulas virtuales en EVA Conducción Iturralde, organización de vehículos e instructores para clases prácticas, seguimiento de clases virtuales y descarga de notas. • Armado de carpetas finales: récord de calificaciones, actas de grado, certificados, permisos de aprendizaje y documentación exigida por la Agencia Nacional de Tránsito (ANT).
Encargado del tratamiento	Secretaría General.
Categoría de datos	Se manejan datos personales y sensibles de los estudiantes, tales como: • Edad. • Fotografías: dos fotos tamaño carné. • Identificación: tres copias de cédula o visa en caso de extranjeros. • Formación académica: copia del título de bachiller o certificado probado hasta décimo año, notariado. • Evaluaciones médicas y psicológicas: resultados del examen psicosenométrico y test de ansiedad. • Biometría: huella biométrica de estudiantes y docentes. Estos datos son indispensables para validar la matrícula y cumplir con los requisitos de la Agencia Nacional de Tránsito (ANT).
Finalidades de los datos personales	Los datos se utilizan para formalizar la matrícula de los estudiantes, validar su idoneidad para obtener una licencia no profesional, cumplir con los requisitos legales y técnicos exigidos por la ANT, y garantizar la correcta identificación y seguridad de estudiantes y docentes.
Medidas de seguridad	Los datos se almacenan en registros físicos y digitales bajo custodia del departamento administrativo, con acceso restringido al personal autorizado. Se utilizan sistemas biométricos para la identificación de estudiantes y docentes. Por ningún motivo se compartirá datos de carácter personal o sensible con terceras personas, salvo obligaciones legales.

Actividades de Admisiones y Marketing

Breve descripción del tipo de actividades que requieren tratamiento	Las actividades de admisiones, ventas y marketing del instituto están orientadas a la promoción, difusión y comercialización de la oferta académica institucional. Estas incluyen la participación en ferias educativas, visitas a instituciones de educación secundaria, eventos
--	---



	empresariales, charlas informativas, campañas publicitarias y estrategias de marketing digital. Además, se realizan procesos de captación de prospectos mediante formularios físicos y digitales, gestión de bases de datos, seguimiento a aspirantes, generación de contenido para redes sociales, registro fotográfico y audiovisual, así como el uso de plataformas tecnológicas para la automatización de procesos comerciales y comunicacional.
Encargado del tratamiento	Coordinación de Ventas - Admisiones - Comunicación
Categoría de datos	Datos personales de identificación: nombres completos, apellidos, número de cédula, copia de documento de identidad. Datos de contacto: teléfono convencional, teléfono celular, correo electrónico personal, dirección domiciliaria. Datos sociodemográficos: edad, fecha de nacimiento. Datos del representante (cuando aplique): nombres, teléfono, correo electrónico. Datos académicos: historial académico, nivel de estudios, institución de procedencia. Datos de interacción digital: registros de navegación en formularios, interacción en campañas digitales.
Finalidades del tratamiento de datos personales	Los datos de carácter personal y sensible de aspirantes son utilizados para: Promocionar la oferta académica institucional. Gestionar procesos de admisión y matrícula. Contactar y dar seguimiento a aspirantes. Enviar información sobre carreras, cursos, eventos, becas y servicios educativos. Ejecutar campañas de marketing y publicidad digital. Generar estadísticas e informes para la mejora de estrategias comerciales. Difundir contenido institucional en medios digitales (incluyendo uso de fotografías y videos).



Medidas jurídicas de protección de datos	Los datos personales serán recolectados únicamente con el consentimiento informado del titular, mediante la firma de formularios físicos o aceptación digital. Se garantiza el cumplimiento de la normativa vigente en materia de protección de datos personales. Se aplicarán medidas de seguridad técnicas y organizativas para evitar pérdida, acceso no autorizado, alteración o divulgación indebida de la información. El uso de los datos estará limitado exclusivamente a fines institucionales relacionados con admisiones, ventas y comunicación. No se compartirán datos personales con terceros, salvo en casos requeridos por ley o autoridades competentes. Los titulares podrán ejercer sus derechos de acceso, rectificación, actualización o eliminación de sus datos conforme a la normativa aplicable.
---	--

Medidas de seguridad técnicas de datos.

Breve descripción del tipo de actividades que requieren tratamiento	El Departamento de Medidas de Seguridad Técnicas de Datos se encarga de implementar, supervisar y mantener las herramientas tecnológicas y protocolos que garantizan la confidencialidad, integridad y disponibilidad de los datos personales y sensibles de estudiantes, docentes y personal administrativo. A esta actividad se la conoce como protección ejecutiva y consiste en cuidar a personalidades que ocupan cargos altos en el instituto, depositar, custodiar, contar y clasificar dinero u objetos de valor que puedan requerir protección especial, instalar y mantener aparatos, dispositivos y sistemas de seguridad y planificar y asesorar las actividades de seguridad.
Encargado del tratamiento	Jefe de Seguridad física
Categoría de datos	No gestiona directamente los datos académicos o administrativos, sino que protege: • Datos de identificación (cédula, nombres completos). • Datos biométricos (huella digital). • Datos académicos y de matrícula. • Resultados de evaluaciones psicosenométricas y médicas. • Registros administrativos y de asistencia.



Finalidades de los datos personales	La finalidad es garantizar que los datos recopilados por los distintos departamentos se mantengan seguros frente a accesos no autorizados, pérdida, alteración o divulgación indebida. Se busca cumplir con la normativa de la Agencia Nacional de Tránsito (ANT) y la Ley Orgánica de Protección de Datos Personales (LOPDP).
Medidas de seguridad	Toda la información de carácter personal y sensible de estudiantes, docentes, personal administrativo, se encuentra bajo la tutela y protección del Encargado de Seguridad Física y del Responsable de Tecnologías de la Información. Se mantendrá total confidencialidad acerca de los datos que puedan conocerse en relación con las actividades institucionales. Los distintos dispositivos electrónicos de control (como cámaras de videovigilancia y sistemas biométricos) se encuentran debidamente señalizados y operan conforme a la normativa vigente. Por ningún motivo se compartirán datos personales o sensibles con terceras personas, salvo en los casos en que exista una obligación legal.

CAPITULO VII

Artículo 19.- Medidas de seguridad técnicas de datos.

1. OBJETIVO

Establecer las directrices generales de la información y uso de activos tecnológicos, con el fin de proteger la confidencialidad, integridad y disponibilidad de los datos personales y de la información institucional que gestiona la ECMI. Esta política se emite en cumplimiento del Artículo 37 de la Ley Orgánica de Protección de Datos Personales (LOPDP) y demás normativa aplicable, asegurando que:

- El tratamiento de datos personales se realice bajo principios de legalidad, transparencia y seguridad.
- Los activos tecnológicos sean utilizados de manera responsable, segura y conforme a las políticas internas.
- Se establezcan medidas preventivas y correctivas frente a riesgos que puedan afectar la información institucional.

2. CONTRASEÑAS Y ACCESOS

Para garantizar el acceso seguro a los sistemas, se establece la siguiente configuración técnica obligatoria:

- Contraseñas con mínimo de 12 caracteres, incluyendo mayúsculas, minúsculas, números y caracteres especiales.
- Prohibida la reutilización de las últimas 5 contraseñas.
- Cambio obligatorio cada 90 días.



- Bloqueo automático de cuenta tras 5 intentos fallidos.
- Autenticación multifactor (MFA) obligatoria para sistemas críticos (plataformas en la nube, portales administrativos).

Adicionalmente, todo el personal debe cumplir las siguientes normas de conducta:

- **Prohibición de compartir credenciales:** Usuario y clave son personales e intransferibles. Queda prohibido compartir contraseñas o anotarlas en lugares visibles.
- **Cierre de sesión:** Es obligatorio bloquear o cerrar sesión al dejar el puesto de trabajo, incluso por breves momentos (ejemplo: Tecla Windows + L).
- **Uso de dispositivos externos:** Está prohibido almacenar contraseñas en dispositivos externos no autorizados (ej. USB, aplicaciones no corporativas).
- **Revisión periódica:** El área de TI podrá auditar el cumplimiento de esta política y solicitar cambios inmediatos en caso de vulnerabilidades detectadas.

3. ESCRITORIO LIMPIO Y PANTALLA LIMPIA

- **Documentos Físicos:** No se deben dejar documentos con datos personales (facturas, carpetas de clientes, nóminas) sobre los escritorios al finalizar la jornada laboral o durante recesos largos. Deben guardarse en cajones o archivadores bajo llave.
- **Impresiones:** Los documentos impresos no deben permanecer abandonados en la bandeja de la impresora. Si se imprimen datos sensibles, deben recogerse de inmediato.
- **Pantallas:** Los monitores no deben estar orientados hacia ventanas, pasillos o zonas de espera donde personas no autorizadas puedan visualizar la información.
- **Dispositivos Electrónicos:** Laptops, tablets y memorias externas deben guardarse en lugares seguros al finalizar la jornada.
- **Responsabilidad del Usuario:** Cada empleado es responsable de mantener su espacio de trabajo libre de información expuesta y de cumplir con esta política como parte de la cultura de seguridad institucional.

4. USO DE EQUIPOS Y SOFTWARE

- **Software No Autorizado:** Queda terminantemente prohibido instalar programas piratas, juegos, herramientas de *cracking* o software no autorizado por la Gerencia en los equipos de la empresa.
- **Antivirus:** Está prohibido desactivar el antivirus o las actualizaciones automáticas del sistema operativo bajo cualquier circunstancia.
- **Uso Personal:** Los equipos informáticos y correos corporativos son herramientas de trabajo propiedad de la empresa. Se debe limitar su uso para fines personales.



- **Dispositivos Externos:** No conectar memorias USB (Flash memories) o discos duros externos de procedencia desconocida en los equipos de la red corporativa para evitar infecciones de malware.

5. COPIAS DE SEGURIDAD (BACKUPS)

Para asegurar la recuperación de datos ante desastres, fallas técnicas o ataques (ej. Ransomware), se establece el siguiente esquema de respaldos:

- **Frecuencia:** Copias de seguridad diarias para datos críticos (registros de estudiantes, sistemas académicos) y semanales para datos menos críticos.
- **Características:** Las copias serán completas, cifradas y almacenadas en una ubicación externa o en la nube.
- **Retención:** Los registros académicos tendrán un período de conservación de 7 años.
- **Pruebas:** Se realizarán restauraciones trimestrales para verificar la integridad y disponibilidad de los respaldos.
- **Responsable:** La ejecución y verificación corresponde al Área de Sistemas o al proveedor tecnológico designado.
- **Ubicación:** Las copias no deben guardarse únicamente en el mismo equipo original; deben replicarse en la nube o en un dispositivo externo desconectado.
- **Monitoreo:** El Área de Sistemas llevará un registro de las copias realizadas y de las pruebas de restauración para asegurar trazabilidad.

6. CORREO ELECTRÓNICO E INTERNET

Phishing: Está prohibido abrir correos sospechosos o hacer clic en enlaces de remitentes desconocidos que soliciten datos bancarios, contraseñas o descargas urgentes.

Envío de Datos Sensibles: Si por necesidad del servicio se debe enviar información sensible por correo electrónico, el archivo adjunto debe estar cifrado y protegido con contraseña. La contraseña debe enviarse al destinatario por un canal distinto (ejemplo: llamada telefónica o mensajería segura).

Uso Responsable: El correo institucional debe utilizarse únicamente para fines laborales; queda prohibido reenviar información confidencial a cuentas personales o externas no autorizadas.

7. GESTIÓN DE INCIDENTES

Todo empleado que detecte un riesgo o anomalía (ej. pérdida de una laptop, posible virus, archivos borrados accidentalmente, correos extraños) debe reportarlo de inmediato al responsable del departamento u unidad para activar el protocolo de respuesta.



Advertencia: Ocultar o no reportar un incidente de seguridad será considerado una falta grave y podrá acarrear sanciones disciplinarias

Registro: Todo incidente reportado debe documentarse en el Formulario de Registro de Incidentes para asegurar trazabilidad y seguimiento.

CAPÍTULO VII

COMITÉ DE PROTECCIÓN DE DATOS PERSONALES

Artículo 20.- Conformación.

Se conforma el Comité de Protección de Datos Personales, integrado por:

Organigrama de Responsabilidades





CAPITULO IX

AUDITORÍA, CONTROL Y MEJORA CONTINUA

Artículo 21.- Auditorías.

El Instituto realizará auditorías internas periódicas para verificar el cumplimiento de la LOPDP y de las presentes políticas.

Artículo 22.- Mejora continua.

Las políticas serán revisadas y actualizadas cuando existan cambios normativos, tecnológicos o institucionales.

CAPÍTULO X

RÉGIMEN SANCIONATORIO

Artículo 33.- Incumplimientos.

El incumplimiento de estas políticas dará lugar a sanciones administrativas conforme a la normativa interna y legal vigente.

1. Procedimiento para la aplicación de sanciones

El procedimiento tiene por objeto establecer las normas, etapas y criterios para la determinación y aplicación de sanciones ante el incumplimiento de la Política Institucional de Protección de Datos Personales, en concordancia con la Ley Orgánica de Protección de Datos Personales, garantizando el debido proceso, el derecho a la defensa y la proporcionalidad de las sanciones.

2. Ámbito de aplicación

Este procedimiento será aplicable a:

- Autoridades institucionales.
- Docentes.
- Personal administrativo y de servicios.
- Estudiantes.
- Pasantes, practicantes, contratistas y terceros que, en el ejercicio de sus funciones, accedan, traten o gestionen datos personales bajo responsabilidad del instituto.



3. **Autoridades competentes:** En el procedimiento sancionatorio por Incumplimiento de la Política de Protección de Datos Personales intervienen autoridades del comité:

- Responsable del Tratamiento de Datos Personales (el instituto).
- Delegado de Protección de Datos (DPD) o quien haga sus veces.
- Unidad Jurídica Institucional.
- Autoridad Máxima del instituto, según corresponda.

4. **Principios para la aplicación procedimiento:** El procedimiento se rige por los principios de:

- Legalidad
- Debido proceso
- Proporcionalidad
- Responsabilidad proactiva
- Presunción de inocencia
- Confidencialidad
- Interés superior de niñas, niños y adolescentes (cuando aplique)

5. Clasificación de las infracciones

3.1 Infracciones leves

Se consideran infracciones leves aquellas acciones u omisiones que, sin causar un daño significativo a los derechos de los titulares de los datos personales, constituyan un incumplimiento parcial o no reiterado de la normativa institucional, tales como:

- Manejo inadecuado de datos personales por desconocimiento o negligencia leve.
- Incumplimiento de procedimientos internos sin afectación directa a los titulares.
- Falta de adopción oportuna de medidas administrativas básicas de protección de datos.
- Acceso no autorizado a datos personales sin uso indebido ni difusión.

Conforme a lo dispuesto en los artículos 69 y 71 de la LOPDP.

3.2 Infracciones graves

Se consideran infracciones graves aquellas acciones u omisiones que vulneren de forma significativa los derechos de los titulares de los datos personales o impliquen dolo, reiteración o afectación institucional, entre ellas:

- Tratamiento de datos personales sin base legal o sin consentimiento cuando este sea exigible.



- Divulgación, cesión o transferencia no autorizada de datos personales.
- Uso indebido de datos personales con fines distintos a los autorizados.
- Negativa injustificada a atender los derechos de los titulares.
- Reincidencia en infracciones leves.
- Incumplimiento de medidas de seguridad que derive en una violación de datos personales.

De conformidad con los artículos 70 y 72 de la LOPDP.

4. Etapas del Procedimiento

4.1 Inicio

El procedimiento sancionatorio se inicia por:

- Denuncia presentada por el titular de los datos.
- Reporte interno de una autoridad, unidad académica o administrativa.
- Informe del responsable o encargado del tratamiento de datos personales.
- Auditorías internas o procesos de control institucional.

4.2. Investigación preliminar

La unidad responsable de protección de datos personales realizará una verificación inicial de los hechos, recopilando evidencias y determinando la existencia de indicios de infracción.

4.3 Notificación

De existir indicios suficientes, se notificará por escrito a la persona presuntamente responsable, detallando los hechos, la calificación provisional de la infracción y concediendo un plazo razonable para presentar cargos y descargos.

4.4. Descargos y defensa

La persona investigada podrá presentar pruebas, explicaciones o alegatos dentro del plazo establecido, garantizando su derecho a la defensa.

4.5. Análisis técnico jurídico, a cargo del delegado de Protección de Datos y la Unidad Jurídica.

4.6. Informe motivado, En esta fase contendrá la recomendación de sanción o archivo.

4.7. Resolución

Concluida la fase de análisis, la autoridad competente emitirá una resolución motivada en la que se determine:

- La existencia o inexistencia de la infracción.



- Su calificación como leve o grave.
- La sanción aplicable, de ser el caso.

5. Sanciones aplicables

5.1 Sanciones por infracciones leves: Podrán aplicarse una o varias de las siguientes medidas:

- Amonestación verbal o escrita.
- Capacitación obligatoria en protección de datos personales.
- Llamado de atención registrado en el expediente institucional.

5.2 Sanciones por infracciones graves: Podrán aplicarse, según la gravedad y normativa interna:

- Amonestación escrita agravada.
- Suspensión temporal de funciones o actividades académicas.
- Pérdida de acceso a sistemas de información institucionales.
- Inicio de acciones administrativas, civiles o penales, cuando corresponda.
- Comunicación del hecho a la Autoridad de Protección de Datos Personales, conforme a la ley.
- Suspensión temporal de funciones relacionadas con el tratamiento de datos.
- Terminación de contratos con terceros.

6. Principios aplicables al procedimiento sancionatorio: El procedimiento se regirá por los principios de:

- Legalidad
- Debido proceso
- Proporcionalidad
- Responsabilidad proactiva
- Presunción de inocencia
- Confidencialidad

7. Registro y seguimiento

Toda sanción impuesta será registrada por la unidad correspondiente y dará lugar a acciones correctivas y preventivas orientadas a fortalecer la cultura institucional de protección de datos personales.



8. Disposición final

El presente procedimiento es de cumplimiento obligatorio y forma parte integrante de la Política Institucional de Protección de Datos Personales de la ECMI, vinculando a estudiantes, docentes, personal administrativo, proveedores y terceros relacionados con el instituto.

DISPOSICIÓN FINAL

El presente documento entrará en vigor a partir de su aprobación por el órgano competente de la Escuela de Formación Conductores No Profesionales Miguel Iturralde (ECMI) y será revisado periódicamente para garantizar su actualización conforme a la Ley Orgánica de Protección de Datos Personales (LOPD) y demás normativa aplicable.

Dado y firmado en la ciudad de Quito, a los 10 días del mes de febrero del 2026.

Elaborado:	Revisado por:	Aprobado por:
 Abg. Mariuxi Ochoa, MSc.	 Ing. Wilfrido Trujillo, MSc.	 Licd. Danilo Naranjo
Fecha: 26/01/2026	Fecha: 28/01/2026	Fecha: 10/02/2026