

**POLÍTICA DE PROTECCIÓN DE
DATOS PERSONALES**

2026



PROCESOS DEL SISTEMA DE GESTIÓN

Tipo de Gestión	Gestión de Seguridad de la Información
Proceso	Habilitante de Asesoría

INFORMACIÓN GENERAL DEL DOCUMENTO

Título	Política de Protección de Datos Personales		
Código	PO-GSI-02	Versión	1.0
Instancia responsable del documento	Unidad de Seguridad de la Información		
Nivel de seguridad de la información	Pública		

LISTA DE CAMBIOS DEL DOCUMENTO

Versión	Fecha dd/mm/aa	Descripción
1.0	05-03-2026	Creación de la Política de protección de datos personales

Aprobado mediante RESOLUCIÓN No. 020-SG-SO-006-CU-IKIAM-2026 de 3 de junio de 2026

LEGALIZACIÓN

ELABORACIÓN

Instancia	Nombre	Cargo	Firma
Unidad de Seguridad de la Información	Carlos Fernando Pilco Zúñiga	Oficial de Seguridad de la Información Encargado	

REVISIÓN

Instancia	Nombre	Cargo	Firma
Dirección de Aseguramiento de la Calidad	Pablo Alejandro López Corrales	Especialista de Aseguramiento de la Calidad	
Dirección de Aseguramiento de la Calidad	Paúl Alejandro Morillo Medina	Director de Aseguramiento de la Calidad	
Unidad de Seguridad de la Información	Tania Alexandra Acosta Tamayo	Delegado de Protección de Datos Personales	

VALIDACIÓN

Instancia	Nombre	Cargo	Firma
Comité de Seguridad de la Información	Zayra Cecibel Moreno Carlosama	Presidenta	

APROBACIÓN

Instancia	Nombre	Cargo	Firma
Consejo Universitario	María Victoria Reyes Vargas	Presidenta	

TABLA DE CONTENIDOS

1.	Marco referencial	6
1.1.	Objetivo	6
1.2.	Alcance	6
1.3.	Glosario de términos	6
1.4.	Abreviaturas	7
2.	Normativa	8
2.1.	Constitución de la Republica del Ecuador	8
2.2.	Ley Orgánica de Educación Superior	8
2.3.	Ley Orgánica de Protección de Datos Personales.....	9
2.4.	Reglamento General de la Ley Orgánica de Protección de Datos Personales	16
2.5.	Esquema Gubernamental de Seguridad de la Información	18
2.6.	Modelo de Evaluación Externa con fines de Acreditación para el Aseguramiento de la Calidad de las Universidades y Escuelas Politécnicas.....	18
3.	Obligaciones y/o responsabilidades	18
3.1.	Oficial de Seguridad de la Información.....	18
3.2.	Delegado de Protección de Datos Personales	19
3.3.	Director/a de Comunicación.....	19
3.4.	Director/a de Tecnologías de la Información	19
3.5.	Comité de Seguridad de la Información	19
3.6.	Consejo Universitario	19
3.7.	Responsable del tratamiento de datos personales	19
4.	Desarrollo de la Política	20
4.1.	Compromiso institucional.....	20
4.2.	Fines del tratamiento de datos personales	20
4.3.	Base legal para el tratamiento de datos personales	20
4.4.	Tipos de tratamiento de datos personales	21
4.5.	Medidas para la protección de la seguridad de datos personales	21
4.6.	Tiempo de conservación de los datos personales	21
4.7.	Bases de datos personales.....	21
4.8.	Origen de los datos personales	21
4.9.	Tratamiento de datos personales ulteriores	21
4.10.	Contactos.....	21
4.11.	Transferencias o comunicaciones.....	22
4.12.	Consecuencias de la entrega o negativa para el tratamiento de datos personales	22
4.13.	Datos personales inexactos o erróneos.....	22
4.14.	Mecanismo para revocar un consentimiento.....	23
4.15.	Mecanismo para el ejercicio de derechos de los titulares de los datos personales.....	23

4.16.	Derecho a la portabilidad	23
4.17.	Reclamos	23
4.18.	Valoraciones y decisiones automatizadas	24
4.19.	Derecho a la información	24
4.20.	Mecanismos de seguimiento, control y evaluación	24

1. Marco referencial

1.1. Objetivo

Establecer los lineamientos institucionales que regulan el tratamiento de datos personales en la Universidad Regional Amazónica Ikiam, garantizando el respeto de los derechos de los titulares y el cumplimiento del marco normativo vigente.

1.2. Alcance

Aplica a todos los tratamientos de datos personales realizados por la Universidad Regional Amazónica Ikiam en sus funciones de gestión, docencia, investigación y vinculación con la sociedad.

1.3. Glosario de términos

Autoridad de Protección de Datos Personales: Autoridad pública independiente encargada de supervisar la aplicación de la Ley Orgánica de Protección de Datos Personales, su Reglamento y resoluciones que ella dicte, con el fin de proteger los derechos y libertades fundamentales de las personas naturales, en cuanto al tratamiento de sus datos personales, en el Ecuador asume este rol la Superintendencia de Protección de Datos Personales.

Dato personal: Dato que identifica o hace identificable a una persona natural, directa o indirectamente.

Datos sensibles: Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, 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.

Delegado de protección de datos: Persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la Autoridad de Protección de Datos Personales, sirviendo como punto de contacto entre esta y la entidad responsable del tratamiento de datos.

Destinatario: Persona natural o jurídica que ha sido comunicada con datos personales.

Elaboración de perfiles: Todo tratamiento de datos personales que permite evaluar, analizar o predecir aspectos de una persona natural para determinar comportamientos o estándares relativos a: rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, ubicación, movimiento físico de una persona, entre otros.

Fuente accesible al público: Bases de datos que pueden ser consultadas por cualquier persona, cuyo acceso es público, incondicional y generalizado.

Persona Identificable: se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando esto no requiera plazos o actividades desproporcionadas.

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

finalidad y el tratamiento de datos personales, en la presente política este rol lo asume la Universidad Regional Amazónica Ikiam.

Tercero: Persona natural o jurídica, autoridad pública, servicio u organismo distinto del titular, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable.

Titular: Persona natural cuyos datos son objeto de tratamiento.co

Transferencia o comunicación: Manifestación, declaración, entrega, consulta, interconexión, cesión, transmisión, difusión, divulgación o cualquier forma de revelación de datos personales realizada a una persona distinta al titular, responsable o encargado del tratamiento de datos personales. Los datos personales que comuniquen deben ser exactos, completos y actualizados.

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 recogida, 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

1.4. Abreviaturas

CU: Consejo Universitario

CSI: Comité de Seguridad de la Información

DPD: Delegado de Protección de Datos Personales

EGSI: Esquema Gubernamental de Seguridad de la Información

ETDP: Encargado del Tratamiento de Datos Personales

LOPDP: Ley Orgánica de Protección de Datos Personales

OSI: Oficial de Seguridad de la Información

RAT: Registro de Actividades de Tratamiento de Datos Personales

RGLOPDP: Reglamento General de la Ley Orgánica de Protección de Datos Personales

RTDP: Responsable del Tratamiento de Datos Personales

SPDP: Superintendencia de Protección de Datos Personales

URAI: Universidad Regional Amazónica Ikiam

2. Normativa

2.1. Constitución de la Republica del Ecuador

“Art. 66.- Se reconoce y garantizará a las personas:

19. El derecho a la protección de datos 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 ley”:

“Art. 92.- Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.

Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.

La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados.”

“Art. 417.- Los tratados internacionales ratificados por el Ecuador se sujetarán a lo establecido en la Constitución. En el caso de los tratados y otros instrumentos internacionales de derechos humanos se aplicarán los principios pro ser humano, de no restricción de derechos, de aplicabilidad directa y de cláusula abierta establecidos en la Constitución.”

“Art. 424.- La Constitución es la norma suprema y prevalece sobre cualquier otra del ordenamiento jurídico. Las normas y los actos del poder público deberán mantener conformidad con las disposiciones constitucionales; en caso contrario carecerán de eficacia jurídica.

La Constitución y los tratados internacionales de derechos humanos ratificados por el Estado que reconozcan derechos más favorables a los contenidos en la Constitución, prevalecerán sobre cualquier otra norma jurídica o acto del poder público. “

2.2. Ley Orgánica de Educación Superior

“Art. 17.- Reconocimiento de la autonomía responsable. - El Estado reconoce a las universidades y escuelas politécnicas autonomía académica, administrativa, financiera y orgánica, acorde con los principios establecidos en la Constitución de la República. En el ejercicio de autonomía responsable, las universidades y escuelas politécnicas mantendrán relaciones de reciprocidad y cooperación entre ellas y de estas con el Estado y la sociedad; además observarán los principios de justicia, equidad, solidaridad, participación ciudadana, responsabilidad social y rendición de cuentas. Se reconoce y garantiza la naturaleza jurídica propia y la especificidad de todas las universidades y escuelas politécnicas.

“Art. 18.- Ejercicio de la autonomía responsable.- La autonomía responsable que ejercen las instituciones de educación superior consiste en: (...)

e) La libertad para gestionar sus procesos internos (...)”

2.3. Ley Orgánica de Protección de Datos Personales

“Art. 12.- Derecho a la información. - El titular de datos personales tiene derecho a ser informado conforme los principios de lealtad y transparente por cualquier medio sobre:

- 1) Los fines del tratamiento;
- 2) La base legal para el tratamiento;
- 3) Tipos de tratamiento;
- 4) Tiempo de conservación;
- 5) La existencia de una base de datos en la que constan sus datos personales;
- 6) El origen de los datos personales cuando no se hayan obtenido directamente del titular;
- 7) Otras finalidades y tratamientos ulteriores;
- 8) Identidad y datos de contacto del responsable del tratamiento de datos personales, que incluirá: dirección del domicilio legal, número de teléfono y correo electrónico;
- 9) Cuando sea del caso, identidad y datos de contacto del delegado de protección de datos personales, que incluirá: dirección domiciliaria, número de teléfono y correo electrónico;
- 10) Las transferencias o comunicaciones, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y sus clases, así como las finalidades que motivan la realización de estas y las garantías de protección establecidas;
- 11) Las consecuencias para el titular de los datos personales de su entrega o negativa a ello;
- 12) El efecto de suministrar datos personales erróneos o inexactos;
- 13) La posibilidad de revocar el consentimiento;
- 14) La existencia y forma en que pueden hacerse efectivos sus derechos de acceso, eliminación, rectificación y actualización, oposición, anulación, limitación del tratamiento y a no ser objeto de una decisión basada únicamente en valoraciones automatizadas.
- 15) Los mecanismos para hacer efectivo su derecho a la portabilidad, cuando el titular lo solicite;
- 16) Dónde y cómo realizar sus reclamos ante el responsable del tratamiento de datos personales y la Autoridad de Protección de Datos Personales, y;
- 17) La existencia de valoraciones y decisiones automatizadas, incluida la elaboración de perfiles.

En el caso que los datos se obtengan directamente del titular, la información deberá ser comunicada de forma previa a este, es decir, en el momento mismo de la recogida del dato personal.

Cuando los datos personales no se obtuvieren de forma directa del titular o fueren obtenidos de una fuente accesible al público, el titular deberá, ser informado dentro de los siguientes treinta (30) días o al momento de la primera comunicación con el titular, cualquiera de las dos circunstancias que ocurra primero. Se le deberá proporcionar información expresa, inequívoca, transparente, inteligible, concisa, precisa y sin barreras técnicas.

La información proporcionada al titular podrá transmitirse de cualquier modo comprobable en un lenguaje claro, sencillo y de fácil comprensión, de preferencia propendiendo a que pueda ser accesible en la lengua de su elección.

En el caso de productos o servicios dirigidos, utilizados o que pudieran ser utilizados por niñas, niños y adolescentes, la información a la que hace referencia el presente artículo será, proporcionada a su representante legal conforme a lo dispuesto en la presente Ley.”

“Art. 13.- Derecho de acceso.- El titular tiene derecho a conocer y a obtener, gratuitamente, del responsable de tratamiento acceso a todos sus datos personales y a la información detallada en

el artículo precedente, sin necesidad de presentar justificación alguna. El responsable del tratamiento de datos personales deberá establecer métodos razonables que permitan el ejercicio de este derecho, el cual deberá ser atendido dentro del plazo de quince (15) días

El derecho de acceso no podrá ejercerse de forma tal que constituya abuso del derecho.”

“Art. 14.- Derecho de rectificación y actualización.- El titular tiene el derecho a obtener del responsable del tratamiento la rectificación y actualización de sus datos personales inexactos o incompletos.

Para tal efecto, el titular deberá presentar los justificativos del caso, cuando sea pertinente. El responsable de tratamiento deberá atender el requerimiento en un plazo de quince (15) días y en este mismo plazo, deberá informar al destinatario de los datos, de ser el caso, sobre la rectificación, a fin de que lo actualice.”

“Art. 15.- Derecho de eliminación.- El titular tiene derecho a que el responsable del tratamiento suprima sus datos personales, cuando:

- 1) El tratamiento no cumpla con los principios establecidos en la presente ley;*
- 2) El tratamiento no sea necesario o pertinente para el cumplimiento de la finalidad;*
- 3) Los datos personales hayan cumplido con la finalidad para la cual fueron recogidos o tratados;*
- 4) Haya vencido el plazo de conservación de los datos personales;*
- 5) El tratamiento afecte derechos fundamentales o libertades individuales;*
- 6) Revoque el consentimiento prestado o señale no haberlo otorgado para uno o varios fines específicos, sin necesidad de que medie justificación alguna; o,*
- 7) Exista obligación legal.*

El responsable del tratamiento de datos personales implementará métodos y técnicas orientadas a eliminar, hacer ilegible, o dejar irreconocibles de forma definitiva y segura los datos personales. Esta obligación la deberá cumplir en el plazo de quince (15) días de recibida la solicitud por parte del titular y será gratuito.”

“Art. 16.- Derecho de oposición.- El titular tiene el derecho a oponerse o negarse al tratamiento de sus datos personales, en los siguientes casos:

- 1) No se afecten derechos y libertades fundamentales de terceros, la ley se lo permita y no se trate de información pública, de interés público o cuyo tratamiento está ordenado por la ley.*
- 2) El tratamiento de datos personales tenga por objeto la mercadotecnia directa; el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles; en cuyo caso los datos personales dejarán de ser tratados para dichos fines.*
- 3) Cuando no sea necesario su consentimiento para el tratamiento como consecuencia de la concurrencia de un interés legítimo, previsto en el artículo 7, y se justifique en una situación concreta personal del titular, siempre que una ley no disponga lo contrario.*

El responsable de tratamiento dejará de tratar los datos personales en estos casos, salvo que acredite motivos legítimos e imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del titular, o para la formulación, el ejercicio o la defensa de reclamaciones.

Esta solicitud deberá ser atendida dentro del plazo de quince (15) días”

“Art. 17.- Derecho a la portabilidad.- El titular tiene el derecho a recibir del responsable del tratamiento, sus datos personales en un formato compatible, actualizado, estructurado, común, inter-operable y de lectura mecánica, preservando sus características; o a transmitirlos a otros responsables. La Autoridad de Protección de Datos Personales deberá dictar la normativa para el ejercicio del derecho a la portabilidad.

El titular podrá solicitar que el responsable del tratamiento realice la transferencia o comunicación de sus datos personales a otro responsable del tratamiento en cuanto fuera técnicamente posible y sin que el responsable pueda aducir impedimento de cualquier orden con el fin de ralentizar el acceso, la transmisión o reutilización de datos por parte del titular o de otro responsable del tratamiento. Luego de completada la transferencia de datos, el responsable que lo haga procederá a su eliminación, salvo que el titular disponga su conservación. El responsable que ha recibido la información asumirá las responsabilidades contempladas en esta Ley.

Para que proceda el derecho a la portabilidad de datos es necesario que se produzca al menos una de las siguientes condiciones:

- 1) Que el titular haya otorgado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. La transferencia o comunicación se hará entre responsables del tratamiento de datos personales cuando la operación sea técnicamente posible; en caso contrario los datos deberán ser transmitidos directamente al titular.
- 2) Que el tratamiento se efectúe por medios automatizados;
- 3) Que se trate de un volumen relevante de datos personales, según los parámetros definidos en el reglamento de la presente ley; o,
- 4) Que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos del responsable o encargado del tratamiento de datos personales, o del titular en el ámbito del derecho laboral y seguridad social

Esta transferencia o comunicación debe ser económica y financieramente eficiente, expedita y sin trabas.

No procederá este derecho cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable del tratamiento de datos personales con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.”

“Art. 18.- Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad.- Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad. No proceden los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad, en los siguientes casos;

- 1) Si el solicitante no es el titular de los datos personales o su representante legal no se encuentre debidamente acreditado;
- 2) Cuando los datos son necesarios para el cumplimiento de una obligación legal o contractual;
- 3) Cuando los datos son necesarios para el cumplimiento de una orden judicial, resolución o mandato motivado de autoridad pública competente;
- 4) Cuando los datos son necesarios para la formulación, ejercicio o defensa de reclamos o recursos;
- 5) Cuando se pueda causar perjuicios a derechos o afectación a intereses legítimos de terceros y ello sea acreditado por el responsable de la base de datos al momento de dar respuesta al titular a su solicitud de ejercicio del derecho respectivo;

6) Cuando se pueda obstaculizar actuaciones judiciales o administrativas en curso, debidamente notificadas;

7) Cuando los datos son necesarios para ejercer el derecho a la libertad de expresión y opinión;

8) Cuando los datos son necesarios para proteger el interés vital del interesado o de otra persona natural;”

“Art. 19.- Derecho a la suspensión del tratamiento.- El titular tendrá derecho a obtener del responsable del tratamiento la suspensión del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

1) Cuando el titular impugne la exactitud de los datos personales, mientras el responsable de tratamiento verifica la exactitud de los mismos;

2) El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

3) El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; y.

4) Cuando el interesado se haya opuesto al tratamiento en virtud del artículo 31 de la presente ley; mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

De existir negativa por parte del responsable o encargado del tratamiento de datos personales y el titular recurra por dicha decisión ante la Autoridad de Protección de Datos Personales, esta suspensión se extenderá hasta la resolución del procedimiento administrativo.

Cuando el titular impugne la exactitud de los datos personales, mientras el responsable de tratamiento verifica la exactitud de los mismos, deberá colocarse en la base de datos, en donde conste la información impugnada, que ésta ha sido objeto de inconformidad por parte del titular.

El responsable de tratamiento podrá tratar los datos personales, que han sido objeto del ejercicio del presente derecho por parte del titular, únicamente, en los siguientes supuestos; para la formulación, el ejercicio o la defensa de reclamaciones; con el objeto de proteger los derechos de otra persona natural o jurídica o por razones de interés público importante.”

“Art. 20.- Derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas.- El titular tiene derecho a no ser sometido a una decisión basada única o parcialmente en valoraciones que sean producto de procesos automatizados, incluida la elaboración de perfiles, que produzcan efectos jurídicos en el o que atenten contra sus derechos y libertades fundamentales, para lo cual podrá:

a. Solicitar al responsable del tratamiento una explicación motivada sobre la decisión tomada por el responsable o encargado del tratamiento de datos personales;

b. Presentar observaciones;

c. Solicitar los criterios de valoración sobre el programa automatizado; o,

d. Solicitar al responsable información sobre los tipos de datos utilizados y la fuente de la cual han sido obtenidos los mismos; e impugnar la decisión ante el responsable o encargado del tratamiento

No se aplicará este derecho cuando

1. La decisión es necesaria para la celebración o ejecución de un contrato entre el titular y el responsable o encargado del tratamiento de datos personales;

2. Está autorizada por la normativa aplicable, orden judicial, resolución o mandato motivado de autoridad técnica competente para lo cual se deberá establecer medidas adecuadas para salvaguardar los derechos fundamentales y libertades del titular; o,
3. Se base en el consentimiento explícito del titular.
4. La decisión no conlleve impactos graves o riesgos verificables para el titular.

No se podrá exigir la renuncia a este derecho en forma adelantada a través de contratos de adhesión masivos. A más tardar en el momento de la primera comunicación con el titular de los datos personales, para informar una decisión basada únicamente en valoraciones automatizadas, este derecho le será informado explícitamente por cualquier medio idóneo”

“Art. 21.- Derecho de niñas, niños y adolescentes a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas.- Además de los presupuestos establecidos en el derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas, no se podrán tratar datos sensibles o datos de niñas, niños y adolescentes a menos que se cuente con la autorización expresa del titular o de su representante legal; o, cuando, dicho tratamiento esté destinado a salvaguardar un interés público esencial, el cual se evalúe en atención a los estándares internacionales de derechos humanos, y como mínimo satisfaga los criterios de legalidad, proporcionalidad y necesidad, y además incluya salvaguardas específicas para proteger los derechos fundamentales de los interesados.

Los adolescentes, en ejercicio progresivo de sus derechos, a partir de los 15 años, podrán otorgar, en calidad de titulares, su consentimiento explícito para el tratamiento de sus datos personales, siempre que se les especifique con claridad sus fines.”

“Art. 22.- Derecho de consulta.- Las personas tienen derecho a la consulta pública y gratuita ante el Registro Nacional de Protección de Datos Personales, de conformidad con la presente Ley”

“Art. 23.- Derecho a la educación digital.- Las personas tienen derecho al acceso y disponibilidad del conocimiento, aprendizaje, preparación, estudio, formación; capacitación, enseñanza e instrucción relacionados con el uso y manejo adecuado, sano, constructivo, seguro y responsable de las tecnologías de la información y comunicación, en estricto apego a la dignidad e integridad humana, los derechos fundamentales y libertades individuales con especial énfasis en la intimidad, la vida privada, autodeterminación informativa, identidad y reputación en línea, ciudadanía digital y el derecho a la protección de datos personales, así como promover una cultura sensibilizada en el derecho de protección de datos personales.

El derecho a la educación digital tendrá un carácter inclusivo sobre todo en lo que respecta a las personas con necesidades educativas especiales.

El sistema educativo nacional, incluyendo el sistema de educación superior, garantizará la educación digital no solo a favor de los estudiantes de todos los niveles sino también de los docentes, debiendo incluir dicha temática en su proceso de formación.”

“Art. 24.- Ejercicio de derechos.- El Estado, entidades educativas, organizaciones de la sociedad civil, proveedores de servicios de la sociedad de la información y el conocimiento, y otros entes relacionados, dentro del ámbito de sus relaciones, están obligados a proveer información y capacitación relacionadas con el uso y tratamiento responsable, adecuado y seguro de datos personales de niñas, niños y adolescentes, tanto a sus titulares como a sus representantes

legales, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales.

Los adolescentes mayores de doce (12) años y menores de quince (15) años, así como las niñas y niños, para el ejercicio de sus derechos necesitarán de su representante legal. Los adolescentes mayores de quince (15) años y menores de dieciocho (18) años, podrán ejercerlos de forma directa ante la Autoridad de Protección de Datos Personales o ante el responsable de la base de datos personales del tratamiento.

Los derechos del titular son irrenunciables. Será nula toda estipulación en contrario.”

“Art. 31.- Tratamiento de datos relativos a la salud.- Todo tratamiento de datos relativos a la salud deberá cumplir con los siguientes parámetros mínimos y aquellos que determine la Autoridad de Protección de Datos Personales en la normativa emitida para el efecto:

1. Los datos relativos a la salud generados en establecimientos de salud públicos o privados, serán tratados cumpliendo los principios de confidencialidad y secreto profesional. El titular de la información deberá brindar su consentimiento previo conforme lo determina esta Ley, salvo en los casos en que el tratamiento sea necesario para proteger intereses vitales del interesado, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento; o sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico,, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base de la legislación especializada sobre la materia o en virtud de un contrato con un profesional sanitario. En este último caso el tratamiento sólo podrá, ser realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con la legislación especializada sobre la materia o con las demás normas que al respecto pueda establecer la Autoridad.
2. Los datos relativos a la salud que se traten, siempre que sea posible, deberán ser previamente anonimizados o seudonimizados, evitando la posibilidad de identificar a los titulares de los mismos.
3. Todo tratamiento de datos de salud anonimizados deberá ser autorizado previamente por la Autoridad de Protección de Datos Personales. Para obtener la autorización mencionada, el interesado deberá presentar un protocolo técnico que contenga los parámetros necesarios que garanticen la protección de dichos datos y el informe previo favorable emitido por la Autoridad Sanitaria.”

“Art. 32.- Tratamiento de datos de salud por entes privados y públicos con fines de investigación.- Los datos relativos a salud que consten en las instituciones que conforman el Sistema Nacional de Salud, podrán ser tratados por personas naturales y jurídicas privadas y públicas con fines de investigación científica, siempre que según el caso encuentren anonimizados, o dicho tratamiento sea autorizado por la Autoridad de Protección de Datos Personales, previo informe de la Autoridad Sanitaria Nacional.”

“Art. 33.- Transferencia o comunicación de datos personales.- Los datos personales podrán transferirse o comunicarse a terceros cuando se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del responsable y del destinatario, cuando la transferencia se encuentre configurada dentro de una de las causales de legitimidad establecidas en esta Ley, y se cuente, además, con el consentimiento del titular.

Se entenderá que el consentimiento es informado cuando para la transferencia o comunicación de datos personales el Responsable del tratamiento haya entregado información suficiente al titular que le permita conocer la finalidad a que se destinarán sus datos y el tipo de actividad del tercero a quien se pretende transferir o comunicar dichos datos.”

“Art. 34.- Acceso a datos personales por parte del encargado.- No se considerará transferencia o comunicación en el caso de que el encargado acceda a datos personales para la prestación de un servicio al responsable del tratamiento de datos personales. El tercero que ha accedido legítimamente a datos personales en estas consideraciones, será considerado encargado del tratamiento.

El tratamiento de datos personales realizado por el encargado deberá estar regulado por un contrato, en el que se establezca de manera clara y precisa que el encargado del tratamiento de datos personales tratará únicamente los mismos conforme las instrucciones del responsable y que no los utilizará para finalidades diferentes a las señaladas en el contrato, ni que los transferirá o comunicará ni siquiera para su conservación a otras personas.

Una vez que se haya cumplido la prestación contractual, los datos personales deberán ser destruidos o devueltos al responsable del tratamiento de datos personales bajo la supervisión de la Autoridad de Protección de Datos Personales.”

“Art. 38.- Medidas de seguridad en el ámbito del sector público.- El mecanismo gubernamental de seguridad de la información deberá incluir las medidas que deban implementarse en el caso de tratamiento de datos personales para hacer frente a cualquier riesgo, amenaza, vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita en el tratamiento de los datos conforme al principio de seguridad de datos personales.

El mecanismo gubernamental de seguridad de la información abarcará y aplicará a todas las instituciones del sector público, contenidas en el artículo 225 de la Constitución de la República de Ecuador, así como a terceros que presten servicios públicos mediante concesión, u otras figuras legalmente reconocidas. Estas, podrán incorporar medidas adicionales al mecanismo gubernamental de seguridad de la información”

“Art. 47.- Obligaciones del responsable y encargado del tratamiento de datos personales.- El responsable del tratamiento de datos personales está obligado a:

- 1) 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;
- 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, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia;
- 3) 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;
- 4) Implementar políticas de protección de datos personales afines al tratamiento de datos personales en cada caso en particular;

- 5) Utilizar metodologías de análisis y gestión de riesgos adaptadas a las particularidades del tratamiento y de las partes involucradas;
- 6) Realizar evaluaciones de adecuación al nivel de seguridad previas al tratamiento de datos personales;
- 7) Tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas;
- 8) 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;
- 9) Implementar la protección de datos personales desde el diseño y por defecto;
- 10) 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;
- 11) 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;
- 12) 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;
- 13) Designar al Delegado de Protección de Datos Personales, en los casos que corresponda;
- 14) 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,
- 15) 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.

El encargado de tratamiento de datos personales tendrá las mismas obligaciones que el responsable de tratamiento de datos personales, en lo que sea aplicable, de acuerdo a la presente ley y su reglamento”

“Art. 55.- Transferencia o comunicación internacional de datos personales.- La transferencia o comunicación internacional de datos personales será posible si se sujeta a lo previsto en el presente capítulo, la presente Ley o la normativa especializada en la materia, propendiendo siempre al efectivo ejercicio del derecho a la protección de datos personales.”

2.4. Reglamento General de la Ley Orgánica de Protección de Datos Personales

“Art. 12.- Medios para el ejercicio de los derechos.- Para efectivizar el ejercicio de los derechos establecidos en la Ley Orgánica de Protección de Datos Personales, el responsable habilitará, preferentemente, herramientas o canales informáticos simplificados de fácil acceso para el titular, con la finalidad de receptar y atender oportunamente las solicitudes o peticiones formuladas que permitan y garanticen una interacción segura, fiable y rápida entre el responsable y el titular, sin perjuicio de que también puedan ser presentadas por medios físicos.

Por lo tanto, se podrán habilitar plataformas digitales, centros de contacto, líneas telefónicas u otros mecanismos tecnológicos que se consideren idóneos para la presentación de las solicitudes por parte de los titulares.

En todos los casos, el requirente deberá demostrar la titularidad o la representación legal para ejercer el derecho.”.

“Art. 13.- Contenido de la solicitud.- En la solicitud para el ejercicio de los derechos consagrados en la Ley, se hará constar:

1. Los nombres y apellidos completos del titular, número de cédula de identidad o pasaporte y dirección domiciliaria o electrónica para notificaciones. Cuando se actúa en calidad de representante legal, se hará constar también los datos de la o del representado;
2. De ser posible, la descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados y cualquier otro elemento o documento que facilite la localización de los datos personales;
3. Relación de lo que solicita expuesto de manera clara y precisa;
4. Derecho o derechos que desea ejercer; y,
5. A la solicitud se acompañará los documentos que acrediten la identidad o, en su caso, la representación legal o convencional del titular.”

“Art. 14.- Requerimiento de información adicional.- En caso de que la información constante en la solicitud requiera ser aclarada o ampliada, el responsable podrá requerir al titular, por una sola vez y dentro del término de cinco (5) días de recibida la solicitud, que la aclare o complete.

El titular emplazado contará con el término de diez (10) días contados a partir del día siguiente en el que haya sido notificado, para aclarar o completar la solicitud.

Si el titular aclara o completa la solicitud dentro del término concedido, el responsable le dará la debida atención, caso contrario, la archivará notificando este particular al titular con las razones de su decisión. El archivo del requerimiento inicial no impedirá la presentación de una nueva solicitud.”

“Art. 15.- Registro de solicitudes.- El responsable deberá registrar todas las solicitudes de ejercicio de derechos, incluyendo el detalle de la atención dada a las mismas. La Autoridad de Protección de Datos determinará el contenido de dichos registros.”

“Art. 16.- Reclamo ante la Autoridad de Protección de Datos Personales.- El titular de datos personales que encuentre motivos para creer que se han vulnerado sus derechos con la respuesta que el responsable ha dado a su solicitud, o que no haya recibido respuesta en el plazo establecido, podrá acudir a la Autoridad de Protección de Datos a presentar su reclamo, el cual se sustanciará conforme al procedimiento previsto en el Código Orgánico Administrativo y en la normativa complementaria que, para el efecto, emita la Autoridad de Protección de Datos.

El procedimiento de reclamo contemplará la debida notificación al responsable a fin de que ejerza su derecho a la defensa.”

“Art. 38.- Registro de actividades de tratamiento.- El responsable del tratamiento que cuente con cien o más trabajadores, llevará un registro de todas las actividades de tratamiento de datos personales que sean de su competencia.

Este registro contendrá la siguiente información:

1. El nombre y los datos de contacto del responsable del tratamiento y, en su caso, del responsable que actúa conjuntamente con el responsable del tratamiento de datos personales, así como el nombre y los datos de contacto del delegado de protección de datos;

2. Los fines del tratamiento;
3. Las categorías de destinatarios a los que se han comunicado o se comunicarán los datos personales;
4. Identificar a los titulares y las categorías de datos personales de los titulares;
5. En su caso, el uso de perfiles;
6. En su caso, definir las transferencias de datos personales a organismos de un tercer país o a una organización internacional;
7. Descripción de las bases legitimadoras que facultan el tratamiento;
8. Los plazos de retención previstos para la supresión o la revisión de la necesidad de conservar las diferentes categorías de datos personales; y.
9. Una descripción general de las medidas técnicas, jurídicas, administrativas y organizativas.

El registro se llevará por escrito o electrónicamente. Los responsables pondrán a disposición de la Autoridad de Protección de Datos Personales los registros de actividades cuando ésta lo solicite.”

2.5. Esquema Gubernamental de Seguridad de la Información

“Artículo 1.- Expedir el Esquema Gubernamental de Seguridad de la Información – EGSi que se encuentra como Anexo al presente Acuerdo Ministerial, el cual es el mecanismo para implementar el Sistema de Gestión de Seguridad de la Información en el Sector Público.”

“Artículo 2.- El EGSi es de implementación obligatoria en las entidades, organismos e instituciones del sector público, de conformidad con lo establecido en el artículo 225 de la Constitución de la República del Ecuador y los artículos 7 literal o), y 20 de la Ley Orgánica para la Transformación Digital y Audiovisual; y, además, es de implementación obligatoria para terceros que presten servicios públicos mediante concesión, u otras figuras legalmente reconocidas, quienes podrán incorporar medidas adicionales de seguridad de la información.”

2.6. Modelo de Evaluación Externa con fines de Acreditación para el Aseguramiento de la Calidad de las Universidades y Escuelas Politécnicas

Indicador 4: Infraestructura Física y Tecnológica (...)

Elementos fundamentales:

1. La institución cuenta con una instancia responsable de la planificación de su infraestructura física y tecnológica para garantizar el desarrollo de las funciones sustantivas y adjetivas.

3. Obligaciones y/o responsabilidades

3.1. Oficial de Seguridad de la Información

El OSI tiene la responsabilidad de administrar este documento y de velar por su cumplimiento y actualización, así como de evaluar y mejorar la Política de Protección de Datos Personales, a fin de dar cumplimiento a la LOPDP, su reglamento y demás normativa emitida por la SPDP.

3.2. Delegado de Protección de Datos Personales

El DPD tiene la responsabilidad, en coordinación con el OSI, de asesorar y supervisar de manera independiente, en el cumplimiento, actualización, evaluación y mejora continua de la Política de Protección de Datos Personales, a fin de dar cumplimiento a la LOPDP, su reglamento y demás normativa emitida por la SPDP.

3.3. Director/a de Comunicación

El Director/a de Comunicación tiene la responsabilidad, en coordinación con el OSI, de difundir la presente política mediante los medios de comunicación digitales e impresos que dispone la URAI, implementado mecanismos de información por capas, utilizando un lenguaje accesible, claro y sencillo.

3.4. Director/a de Tecnologías de la Información

El Director/a de Tecnologías de la Información tiene la responsabilidad, en coordinación con el OSI, de implementar mecanismos técnicos para la difusión y aceptación la presente política por parte de los usuarios de las aplicaciones informáticas, implementado mecanismos de información por capas, utilizando un lenguaje accesible, claro y sencillo.

3.5. Comité de Seguridad de la Información

El CSI tiene la responsabilidad de validar la presente política.

3.6. Consejo Universitario

El CU tiene la responsabilidad de aprobar la presente política.

3.7. Responsable del tratamiento de datos personales

El RPTDP es la URAI, conforme el artículo 57 de la LOPDP, esta institución de educación superior y su personal tiene la responsabilidad de:

- 1) Tratar datos personales en estricto apego a los principios y derechos desarrollados en LOPDP, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la SPDP, o normativa sobre la materia;
- 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 LOPDP, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la SPDP, o normativa sobre la materia;
- 3) 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;
- 4) Implementar políticas de protección de datos personales afines al tratamiento de datos personales en cada caso en particular;
- 5) Utilizar metodologías de análisis y gestión de riesgos adaptadas a las particularidades del tratamiento y de las partes involucradas;

- 6) Realizar evaluaciones de adecuación al nivel de seguridad previas al tratamiento de datos personales;
- 7) Tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas;
- 8) Notificar a la SPDP 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;
- 9) Implementar la protección de datos personales desde el diseño y por defecto;
- 10) Suscribir contratos de confidencialidad y manejo adecuado de datos personales con el ETDP y el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales;
- 11) Asegurar que el ETDP ofrezca mecanismos suficientes para garantizar el derecho a la protección de datos personales conforme a lo establecido en la LOPDP, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la SPDP, normativa sobre la materia y las mejores prácticas a nivel nacional o internacional;
- 12) Registrar y mantener actualizado el Registro Nacional de Protección de Datos Personales, de conformidad a lo dispuesto en la LOPDP, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la SPDP;
- 13) Designar al DPD;
- 14) Permitir y contribuir a la realización de auditorías o inspecciones, por parte de un auditor acreditado por la SPDP; y,
- 15) Los demás establecidos en la presente LOPDP, en su reglamento, en directrices, lineamientos, regulaciones emitidas por la SPDP y normativa sobre la materia.

4. Desarrollo de la Política

4.1. Compromiso institucional

La Universidad Regional Amazónica Ikiam protege la privacidad y los datos personales, de cualquier persona natural, que son tratados por esta institución de educación superior para la ejecución de actividades de gestión, docencia, investigación y vinculación con la sociedad.

El personal de la Universidad Regional Amazónica Ikiam que trata datos personales se compromete a proteger los derechos de los titulares y garantizar la seguridad de los datos personales.

4.2. Fines del tratamiento de datos personales

La URAI trata datos personales en la ejecución de las actividades de gestión, docencia, investigación y vinculación con la sociedad, cuyas finalidades legítimas se encuentran registradas en el RAT levantado por cada unidad organizacional, en cumplimiento al artículo 38 del RGLOPDP.

4.3. Base legal para el tratamiento de datos personales

La URAI trata los datos personales de manera lícita, utilizando las bases legales determinadas en el artículo 7 de la LOPDP y, en el caso de tratamiento de datos sensibles, observando lo dispuesto en el artículo 26 de LOPDP, lo cual es registrado en el RAT levantado por cada unidad organizacional, en cumplimiento al artículo 38 del RGLOPDP.

4.4. Tipos de tratamiento de datos personales

La URAI gestiona el ciclo de vida del dato, a fin de mantener la seguridad de datos personales y proteger los derechos y libertades de los titulares de los datos personales, lo cual es registrado en el RAT levantado por cada unidad organizacional, en cumplimiento al artículo 38 del RGLOPDP.

4.5. Medidas para la protección de la seguridad de datos personales

La URAI conforme a lo dispuesto en el artículo 38 de la LOPDP implementa el EGSI, además de otras medidas jurídicas, organizativas, administrativas, físicas y técnicas para proteger la seguridad de los datos personales.

4.6. Tiempo de conservación de los datos personales

La URAI conserva los datos durante el tiempo necesario para cumplir con las finalidades de tratamiento registradas en el RAT levantado por cada unidad organizacional, en cumplimiento al artículo 38 del RGLOPDP.

La conservación ampliada del tratamiento de datos personales se realiza únicamente para los fines descritos en el numeral i) del artículo 10 de la LOPDP.

4.7. Bases de datos personales

La URAI registra y almacena los datos personales en formato físico y digital, para lo cual implementa medidas jurídicas, organizativas, administrativas, físicas y técnicas que permitan proteger la seguridad de datos personales, lo cual es registrado en el RAT levantado por cada unidad organizacional, en cumplimiento al artículo 38 del RGLOPDP.

4.8. Origen de los datos personales

La URAI recolecta los datos personales directamente del titular y mediante terceros que facilitan la gestión de la información, lo cual es registrado en el RAT levantado por cada unidad organizacional, en cumplimiento al artículo 38 del RGLOPDP.

4.9. Tratamiento de datos personales ulteriores

La URAI realiza tratamiento de datos personales ulteriores bajo el principio de finalidad descrito en el literal d) del artículo 10 de la LOPDP, lo cual es registrado en el RAT levantado por cada unidad organizacional, en cumplimiento al artículo 38 del RGLOPDP.

4.10. Contactos

La URAI como RTDP mantiene los siguientes datos de contacto:

- **Responsable del Tratamiento de Datos Personales:** Universidad Regional Amazónica Ikiam
- **Dirección:** Napo, Tena, parroquia Muyuna, vía Alto Tena Km 7, a un kilómetro del Puente de Alto Tena.
- **Número de teléfono:** 06 370 0040 ext. 202
- **Correo electrónico:** rectorado@ikiam.edu.ec

El DPD de la URAI mantiene los siguientes datos de contacto:

- **Delegado de Protección de Datos Personales:** Tania Alexandra Acosta Tamayo
- **Dirección:** Pichincha, Quito, parroquia Conocoto, calle Checoslovaquia E9-28 y calle Suiza, a dos cuadras del Parque la Carolina.
- **Número de teléfono:** 098 456 0453
- **Correo electrónico:** dpdp.ikiam@ikiam.edu.ec

4.11. Transferencias o comunicaciones

La URAI comunica datos personales a sus ETDP y terceros nacionales observando lo dispuesto en los artículos 33, 34 y 35 de la LOPDP, lo cual es registrado en el RAT levantado por cada unidad organizacional, en cumplimiento al artículo 38 del RGLOPDP.

La URAI también realiza transferencias internacionales de datos personales observando lo dispuesto en los artículos 55, 56 y 57 de la LOPDP, lo cual es registrado en el RAT levantado por cada unidad organizacional, en cumplimiento al artículo 38 del RGLOPDP.

4.12. Consecuencias de la entrega o negativa para el tratamiento de datos personales

La mayoría de los tratamientos de datos personales que realiza la URAI son necesarios para la ejecución de las actividades de gestión, docencia, investigación y vinculación con la sociedad, lo cual está enmarcado en su misión institucional y las competencias que le han sido conferidas por la Constitución de la República del Ecuador, la Ley Orgánica de Educación Superior, la Ley de Creación de la Universidad Regional Amazónica Ikiam y demás obligaciones legales que rigen al sector público.

Los titulares entregan sus datos personales para acceder a los servicios y productos que entrega la URAI, lo cual es registrado en el RAT levantado por cada unidad organizacional, en cumplimiento al artículo 38 del RGLOPDP.

Sin embargo, existen actividades de tratamiento de datos personales que se basan en el consentimiento otorgado por el titular, que cumple con lo dispuesto en el artículo 8 de la LOPDP, lo cual es registrado en el RAT levantado por cada unidad organizacional, en cumplimiento al artículo 38 del RGLOPDP.

4.13. Datos personales inexactos o erróneos

La correcta ejecución de las actividades de gestión, docencia, investigación y vinculación con la sociedad que se realizan en la URAI depende en gran medida de la exactitud de los datos personales recolectados, por esta razón se realizan validaciones mediante la presentación de documentos y de interconexión con sistemas de información.

Los datos personales recolectados son accesibles al titular para su verificación, a fin de evitar vulneraciones de sus derechos y libertades.

4.14. Mecanismo para revocar un consentimiento

El titular de datos personales que ha entregado su consentimiento para el tratamiento de datos personales, puede revocarlo en cualquier momento de acuerdo con lo dispuesto en el artículo 8 de la LOPDP, la URAI recibe estas solicitudes mediante el correo pdp.ikiam@ikiam.edu.ec

4.15. Mecanismo para el ejercicio de derechos de los titulares de los datos personales

El titular de los datos personales puede ejercer sus derechos de:

- Acceso, conforme lo dispuesto en el artículo 13 de la LOPDP
- Rectificación y actualización, conforme lo dispuesto en el artículo 14 de la LOPDP
- Eliminación, conforme lo dispuesto en el artículo 15 de la LOPDP
- Oposición, conforme lo dispuesto en el artículo 16 de la LOPDP
- Portabilidad, conforme lo dispuesto en el artículo 17 de la LOPDP
- Suspensión, conforme lo dispuesto en el artículo 19 de la LOPDP.
- A no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas, conforme a lo dispuesto en el artículo 20 de la LOPDP.

Conforme el procedimiento descrito en los artículos 12, 13, 14 y 15 del RGLOPDP, los titulares de los datos personales presentarán el formato **FO-GSI-10 “Solicitud para el ejercicio de derechos protección de datos personales”** conforme las instrucciones señaladas en el mismo, las solicitudes serán atendidas dentro de los plazos previstos en la LOPDP, en caso de existir alguna excepción, la misma será comunicada al titular de los datos personales conforme el artículo 18 de la LOPDP.

4.16. Derecho a la portabilidad

La URAI utiliza formatos digitales estructurados e interoperables para el registro y almacenamiento de datos personales, cuando sea técnicamente posible se comunicarán o transferirán los datos personales a otro responsable de tratamiento de datos personales de acuerdo con la solicitud del titular de los datos personales, caso contrario se entregarán directamente a éste conforme el artículo 17 de la LOPDP.

Mediante el correo pdp.ikiam@ikiam.edu.ec se receptorán y atenderán las solicitudes de ejercicio del derecho de portabilidad.

4.17. Reclamos

Los titulares de datos personales pueden presentar sus reclamos mediante el correo pdp.ikiam@ikiam.edu.ec, la URAI, en calidad de RTDP atenderá las solicitudes en los plazos establecidos en la LOPDP, conforme el procedimiento descrito en los artículos 12, 13, 14 y 15 del RGLOPDP, sin embargo, conforme el artículo 16 del RGLOPDP, una vez agotada esta instancia y que el titular encuentre motivos para creer que se han vulnerado sus derechos con la respuesta que ha recibido de la URAI, o que no haya recibido respuesta en el plazo establecido, puede presentar su reclamo ante la SPDP mediante los mecanismos dispuestos por esta en su sitio web (<https://spdp.gob.ec/>).

4.18. Valoraciones y decisiones automatizadas

Existen actividades de la URAI que realizan valoraciones y decisiones automatizadas, incluido la elaboración de perfiles, lo cual es registrado en el RAT levantado por cada unidad organizacional, en cumplimiento al artículo 38 del RGLOPDP.

4.19. Derecho a la información

La Política de Protección de Datos Personales será difundida a todos los titulares de datos personales mediante los mecanismos de comunicación que ha implementado la URAI, conforme lo dispuesto en el artículo 12 de la LOPDP.

La información será proporcionada mediante esquemas de capas, manteniendo un lenguaje claro, accesible y sencillo.

4.20. Mecanismos de seguimiento, control y evaluación

El OSI informará al Comité de Seguridad de la Información de manera semestral el seguimiento, control y evaluación del cumplimiento de la Política de Protección de Datos Personales de la Universidad Regional Amazónica Ikiam, conforme el formato **FO-GSI-11 “Informe semestral de avance en la implementación y mejora continua de la LOPDP y del EGSi”**, el CSI será quién valide el informe presentado y presente al CU para su conocimiento.

Los RAT levantados se encuentran publicados en el inventario de RAT (<https://rat.ikiam.edu.ec>), en cumplimiento al artículo 12 de la LOPDP, el mismo que es actualizado de manera anual o cuando existe un cambio relevante en el tratamiento de los datos personales.

5. Formatos

Código	Nombre
FO-GSI-10	Solicitud para el ejercicio de derechos protección de datos personales
FO-GSI-11	Informe semestral de avance en la implementación y mejora continua de la LOPDP y del EGSi