



# MANUAL INTERNO PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

Versión 01

PROCURADURÍA SÍNDICA

	MANUAL INTERNO PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Fecha: 09-04-2025
		Versión: 1.0
	Proceso: Procuraduría Síndica	Página 1 de 32

# UNIDAD EDUCATIVA PARTICULAR BILINGÜE ECOMUNDO MANUAL INTERNO PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

CONTROL DE EMISIÓN Y APROBACIÓN DEL DOCUMENTO		
Elaborado por:	Revisado por:	Aprobado por:
Abogados Baccamedina	Delegada	Rectora
Firma:  <div style="text-align: center;"><b><i>Germán Bacca</i></b></div> Abg. Germán Bacca	Firma:  <div style="text-align: center;"></div> Ing. Sara Layana Molina, Mgs.	Firma:  <div style="text-align: center;"></div> Econ. Raquel Maquilón, Mgtr.
Fecha: 09-04-2025	Fecha: 09-04-2025	Fecha: 09-04-2025

	MANUAL INTERNO	Fecha: 09-04-2025
	PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Versión: 1.0
	Proceso: Procuraduría Síndica	Página 2 de 32

# 1 CONTENIDO

---

2	INTRODUCCIÓN.....	4
3	ASPECTOS GENERALES .....	4
3.1	MARCO NORMATIVO .....	4
3.2	DEFINICIONES.....	4
3.3	PRINCIPIOS RECTORES.....	6
4	OFICIAL DE PROTECCIÓN DE DATOS.....	8
4.1	COMPROMISO DE LA ORGANIZACIÓN.....	8
4.2	OFICIAL DE PROTECCIÓN DE DATOS Y COMITÉ DE PROTECCIÓN DE DATOS PERSONALES.....	8
4.3	RESPONSABILIDADES.....	8
4.4	DEBERES COMO RESPONSABLE DEL TRATAMIENTO .....	10
5	CONSENTIMIENTO.....	11
5.1	REVOCATORIA .....	13
6	AVISO DE PRIVACIDAD .....	14
7	BASES DE DATOS .....	14
7.1	LINEAMIENTOS DE TRATAMIENTO DE LA INFORMACIÓN .....	16
7.1.1	Política de Tratamiento de Datos Personales .....	16
7.1.2	Registro de Actividades de Tratamiento.....	18
7.2	ADMINISTRACIÓN DEL INVENTARIO DE BASES DE DATOS .....	19
7.3	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN .....	19
7.3.1	Definición de la Política .....	20
7.3.2	Análisis de Riesgos (RA) .....	20
7.3.3	Gestión del Riesgo .....	20
7.3.4	Selección de los Controles a Implementar.....	21
7.3.5	Declaración de Aplicabilidad.....	21
7.3.6	Revisión del Sistema .....	21
8	ENCARGADO DEL TRATAMIENTO .....	21
8.1	DEBERES Y OBLIGACIONES EN CALIDAD DE ENCARGADO DEL TRATAMIENTO.....	22
8.2	LISTADO.....	23

	MANUAL INTERNO	Fecha: 09-04-2025
	PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>3</b> de <b>32</b>

9	TRANSFERENCIA NACIONAL O INTERNACIONAL .....	23
10	ATENCIÓN DE REQUERIMIENTOS .....	24
10.1	DERECHOS .....	24
10.2	ATENCIÓN DE REQUERIMIENTOS .....	25
11	GESTIÓN DE RIESGOS .....	26
12	GESTIÓN DE INCIDENTES .....	27
13	GESTIÓN DE RECURSOS HUMANOS.....	28
13.1	LINEAMIENTOS GENERALES .....	29
13.2	CAPACITACIÓN Y COMUNICACIONES .....	29
13.3	CAPACITACIÓN .....	30
13.4	COMUNICACIONES .....	30
14	EVALUACIÓN Y SEGUIMIENTO.....	30
14.1	PLAN DE REVISIÓN, EVALUACIÓN Y MEJORAMIENTO .....	31
14.2	INFORMES .....	31
15	glosario.....	32

	MANUAL INTERNO PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Fecha: 09-04-2025
		Versión: 1.0
	Proceso: Procuraduría Síndica	Página 4 de 32

## 2 INTRODUCCIÓN

---

Como parte de su compromiso con el cumplimiento del Régimen de Protección de Datos Personales, la UNIDAD EDUCATIVA PARTICULAR BILINGÜE ECOMUNDO, -en adelante la Unidad Educativa- ha elaborado el presente documento, el cual es de manejo interno. En él se explican en detalle las acciones necesarias para dar cumplimiento a lo expresado en la Política de Tratamiento de Datos Personales de la Unidad Educativa, cuyo fin es el de garantizar el derecho constitucional *“a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión requerirán la autorización del titular o el mandato de ley”* (Artículo 66 numeral 19 de la Constitución). Así mismo, desarrolla las actividades en torno al cumplimiento de lo establecido en la Ley Orgánica de Protección de Datos Personales - en adelante LOPDP - y demás normas relacionadas, para todas aquellas personas de quienes la Unidad Educativa administre o conserve información de carácter personal.

## 3 ASPECTOS GENERALES

---

### 3.1 MARCO NORMATIVO

Este Manual se encuentra ajustado a la legislación ecuatoriana y, en particular, por la Constitución de la República del Ecuador, la LOPDP, su reglamento y demás normativa secundaria aplicable que les complemente o adicione.

Las normas y disposiciones contenidas en la LOPDP aplican al tratamiento de datos personales contenidos en cualquier tipo de soporte, automatizados o no, así como a toda modalidad de uso posterior. Son accesibles al público y susceptibles de tratamiento los datos personales referentes al contacto de profesionales y los datos de comerciantes, representantes y socios y accionistas de personas jurídicas y servidores públicos, siempre y cuando se refieran al ejercicio de su profesión, oficio, giro de negocio, competencias, facultades, atribuciones o cargo y se trate de nombres y apellidos, funciones o puestos desempeñados, dirección postal o electrónica, y, número de teléfono profesional.

### 3.2 DEFINICIONES

	MANUAL INTERNO	Fecha: 09-04-2025
	PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Versión: 1.0
	Proceso: Procuraduría Síndica	Página 5 de 32

Para el desarrollo y aplicación de este manual se tendrán en cuenta las siguientes definiciones:

- **AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES:** Autoridad pública independiente encargada de supervisar la aplicación de la LOPDP, 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.
- **ANONIMIZACIÓN:** La aplicación de medidas dirigidas a impedir la identificación o reidentificación de una persona natural, sin esfuerzos desproporcionados.
- **BASE DE DATOS O FICHERO:** Conjunto estructurado de datos cualquiera que fuera la forma, modalidad de creación, almacenamiento, organización, tipo de soporte, tratamiento, procesamiento, localización o acceso, centralizado, descentralizado o repartido de forma funcional o geográfica.
- **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 permite o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre otros.
- **DATO GENÉTICO:** Dato personal único relacionado a características genéticas heredadas o adquiridas de una persona natural que proporcionan información única sobre la fisiología o salud de un individuo.
- **DATO PERSONAL:** Dato que identifica o hace 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 RELATIVOS A LA 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, 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.

	MANUAL INTERNO	Fecha: 09-04-2025
	PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Versión: 1.0
	Proceso: Procuraduría Síndica	Página 6 de 32

- **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 cuenta de un responsable de tratamiento de datos personales.
- **FUENTE ACCESIBLE AL PÚBLICO:** Bases de datos que pueden ser consultadas por cualquier persona, cuyo acceso es público, incondicional y generalizado.
- **OFICIAL DE PROTECCIÓN DE DATOS:** Persona asignada para la definición, implementación y seguimiento de las acciones requeridas para garantizar este derecho a los Titulares de datos personales en poder de la Unidad Educativa
- **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.
- **SEUDONIMIZACIÓN:** Tratamiento de datos personales de manera tal que ya no puedan atribuirse a un titular sin utilizar información adicional, siempre que dicha información adicional, figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.
- **TITULAR:** Persona natural cuyos datos son objeto de tratamiento.
- **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.

### 3.3 PRINCIPIOS RECTORES

Es compromiso de la Unidad Educativa en desarrollo de su gestión, entender y aplicar de manera armónica los siguientes principios establecidos en la LOPDP:

- a) **JURIDICIDAD.** Los datos personales deben tratarse con estricto apego y cumplimiento a los principios, derechos y obligaciones establecidas en la constitución, los instrumentos internacionales, la LOPDP, su Reglamento y la demás normativa y jurisprudencia aplicable.

	MANUAL INTERNO	Fecha: 09-04-2025
	PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Versión: 1.0
	Proceso: Procuraduría Síndica	Página 7 de 32

- b) **LEALTAD.** El tratamiento deberá ser leal, por lo que para los titulares debe quedar claro que se están recogiendo, utilizando, consultando o tratando de otra manera, datos personales que les conciernen, así como las formas en que dichos datos son o serán tratados.
- c) **TRANSPARENCIA.** El tratamiento deberá ser transparente, por lo que toda información o comunicación relativa a este tratamiento deberá ser fácilmente accesible y fácil de entender y se deberá utilizar un lenguaje sencillo y claro.
- d) **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.
- e) **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.
- f) **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.
- g) **CONFIDENCIALIDAD.** El tratamiento de datos personales debe concebirse sobre la base del debido sigilo y secreto.
- h) **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.
- i) **CONSERVACIÓN.** Los datos personales serán conservados durante un tiempo no mayor al necesario para cumplir con la finalidad de su tratamiento.
- j) **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.
- k) **RESPONSABILIDAD PROACTIVA Y DEMOSTRADA.** El responsable del tratamiento de datos personales acreditará el haber implementado mecanismos para la protección de datos personales; es decir, el cumplimiento de los principios, derechos y obligaciones establecidos en la LOPDP.
- l) **APLICACIÓN FAVORABLE AL TITULAR.** En caso de duda sobre el alcance de las disposiciones del ordenamiento jurídico o contractuales, aplicables a la protección de datos personales, los funcionarios judiciales y administrativos las interpretarán y aplicarán en el sentido más favorable al titular de dichos datos.
- m) **INDEPENDENCIA DEL CONTROL.** La Autoridad de Protección de Datos Personales, deberá ejercer un control independiente, imparcial y autónomo, así como llevar a cabo las respectivas acciones de prevención, investigación y sanción.



	MANUAL INTERNO PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Fecha: 09-04-2025
		Versión: 1.0
	Proceso: Procuraduría Síndica	Página 8 de 32

## 4 OFICIAL DE PROTECCIÓN DE DATOS

---

### 4.1 COMPROMISO DE LA ORGANIZACIÓN

Para el desarrollo e implementación del Programa Integral de Gestión de Datos Personales, la alta dirección ha decidido establecer, entre otras, las siguientes acciones:

- Designar el rol de Oficial de Protección de Datos Personales (OPD)
- Nombrar al responsable de la función de Oficial de Protección de Datos Personales (OPD)
- Crear un Comité de Protección de Datos Personales liderado por el OPD y conformado por representantes de diferentes áreas de la Unidad Educativa.
- Implementar un plan de capacitación y de comunicaciones orientado a fomentar la cultura de protección de datos.
- Implementar el proceso de atención de requerimientos.

### 4.2 OFICIAL DE PROTECCIÓN DE DATOS Y COMITÉ DE PROTECCIÓN DE DATOS PERSONALES

De acuerdo con la LOPDP y considerando el volumen, naturaleza, alcance y finalidades de los datos que son tratados, la Unidad Educativa no está obligada a designar un *“Delegado de protección de datos personales”*. Sin embargo, se ha decidido crear el rol de Oficial de Protección de Datos (OPD).

Este rol está asignado a Ing. Sara Layana Molina, Mgtr., quien tendrá a cargo la definición, coordinación, implementación y seguimiento de las acciones requeridas para garantizar este derecho a los Titulares de datos personales en poder de la Unidad Educativa, de acuerdo con la regulación vigente. Posteriormente, según lo establezca la alta dirección, se podrá asignar este rol a un tercero.

Adicionalmente, el Oficial contará con el apoyo de un Comité específico para el tema de protección de datos personales, del cual harán parte: Rectoría, Vicerrectoría, Inspección General, Secretaría General, Sistemas, Admisiones, Talento Humano, entre otras. En conjunto con el OPD desarrollarán las iniciativas y acciones necesarias según lo establecido.

### 4.3 RESPONSABILIDADES

Entre las responsabilidades del Oficial de Protección de Datos y el Comité de Protección de Datos Personales, se encuentran:

	MANUAL INTERNO	Fecha: 09-04-2025
	PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Versión: 1.0
	Proceso: Procuraduría Síndica	Página 9 de 32

- a. Administrar el Programa Integral de Gestión de Datos Personales.
- b. Promover la elaboración e implementación de un sistema que permita administrar los riesgos del tratamiento de datos personales.
- c. Coordinar la definición e implementación de los controles del Programa Integral de Gestión de Datos Personales.
- d. Servir de enlace y coordinador con las áreas para asegurar una implementación transversal del Programa Integral de Gestión de Datos Personales.
- e. Impulsar una cultura de protección de datos.
- f. Mantener un inventario centralizado de las bases de datos personales y clasificarlas según su tipo. (Alumnos, empleados, proveedores, etc.)
- g. Registrar y mantener actualizado el Registro Nacional de Protección de Datos Personales, de conformidad con lo dispuesto en la LOPDP, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales.
- h. Permitir y contribuir a la realización de auditorías o inspecciones, por parte de un auditor acreditado por la Autoridad de Protección de Datos Personales.
- i. Revisar y suscribir el contenido de los contratos de transferencia internacional de datos que se establezcan con Encargados no residentes en Ecuador.
- j. En conjunto con el área de Recursos Humanos:
  - Analizar las responsabilidades de cada cargo de la organización para diseñar un programa de entrenamiento en protección de datos personales específico para cada uno de ellos.
  - Realizar un entrenamiento general en protección de datos personales para todos los empleados.
  - Realizar el entrenamiento necesario a los nuevos empleados que tengan acceso a datos personales.
  - Monitorear la participación y el desempeño en los entrenamientos de protección de datos.
- k. Integrar las políticas de protección de datos dentro de las actividades de las áreas.
- l. Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de las políticas de tratamiento de la información personal.
- m. Realizar seguimiento continuo al Programa Integral de Gestión de Datos Personales.
- n. Informar periódicamente a la Dirección de la Unidad Educativa sobre la ejecución del Programa Integral de Protección de Datos Personales.
- o. Ofrecer mecanismos suficientes para garantizar el derecho a la protección de datos personales a los Titulares.
- p. Si llegara a presentarse una vulneración de seguridad, deberá notificar a la Autoridad de Protección de Datos Personales y la Agencia de Regulación y Control de las Telecomunicaciones de acuerdo con lo establecido en la Ley.
- q. Incorporar los cambios regulatorios según corresponda.
- r. Todas aquellas que le sean asignadas por sus jefes superiores en relación con esta función.

	MANUAL INTERNO PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Fecha: 09-04-2025
		Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>10</b> de <b>32</b>

#### 4.4 DEBERES COMO RESPONSABLE DEL TRATAMIENTO

Como Responsable del tratamiento, la Unidad Educativa está obligada a:

1. Tratar datos personales en estricto apego a los principios y derechos desarrollados en la LOPDP, 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 LOPDP, 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 en la LOPDP; excepto en los casos igualmente allí contenidos.
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 LOPDP 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 LOPDP, 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,

	MANUAL INTERNO PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Fecha: 09-04-2025
		Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>11</b> de <b>32</b>

15. Los demás establecidos en la LOPDP en su reglamento, en directrices, lineamientos, regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

Además, deberá:

1. Garantizar la calidad y exactitud de los datos personales que traten los encargados;
2. Establecer plazos para supresión o revisión periódica de los datos personales;
3. Acreditar el haber implementado mecanismos para la protección de datos personales; es decir, el cumplimiento de los principios, derechos y obligaciones establecidos en la LOPDP;
4. Rendir cuentas sobre el tratamiento al titular y a la Autoridad de Protección de Datos Personales;
5. Establecer métodos razonables que permitan el ejercicio del derecho de acceso;
6. Implementar métodos y técnicas orientadas a eliminar, hacer ilegible, o dejar irreconocibles de forma definitiva y segura los datos personales cuando proceda la eliminación;
7. Dejar de tratar los datos personales cuando proceda la oposición;
8. Suspender el tratamiento cuando el titular impugne la exactitud de los datos personales, colocando en la base de datos, en donde conste la información impugnada, que ésta ha sido objeto de inconformidad por parte del titular;
9. Utilizar para el análisis de riesgo, amenazas y vulnerabilidades una metodología que considere, entre otras: 1) Las particularidades del tratamiento; 2) Las particularidades de las partes involucradas; y, 3) Las categorías y el volumen de datos personales objeto de tratamiento;
10. Realizar una evaluación de impacto del tratamiento de datos personales cuando se haya identificado la probabilidad de que dicho tratamiento, por su naturaleza, contexto o fines, conlleve un alto riesgo para los derechos y libertades del titular o cuando la Autoridad de Protección de Datos Personales lo requiera;
11. Observar las obligaciones previstas en la LOPDP en caso de que se llegue a requerir la existencia de un delegado de protección de datos personales en la Unidad Educativa, y;
12. Respetar las políticas de protección de datos personales de los terceros para quienes actúe en calidad de Encargado, así como, cumplir las obligaciones que para el efecto se prevén en la LOPDP y su reglamentación complementaria.

## 5 CONSENTIMIENTO

---

Sin perjuicio de las excepciones previstas en la Ley, la Unidad Educativa se compromete a tratar y comunicar datos personales únicamente cuando cuente con la manifestación de la voluntad del titular para hacerlo, para lo cual el consentimiento será válido, cuando la manifestación de la voluntad sea:

1. Libre, es decir, cuando se encuentre exenta de vicios del consentimiento;

	MANUAL INTERNO PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Fecha: 09-04-2025
		Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>12</b> de <b>32</b>

2. Específica, en cuanto a la determinación concreta de los medios y fines del tratamiento;
3. Informada, de modo que cumpla con el principio de transparencia y efectivice el derecho a la transparencia,
4. Inequívoca, de manera que no presente dudas sobre el alcance de la autorización otorgada por el titular.

Se podrán recolectar los datos de los Titulares de manera electrónica o física.

La Unidad Educativa no requerirá del consentimiento del Titular para la transferencia o comunicación de datos personales, cuando:

1. Los datos hayan sido recogidos de fuentes accesibles al público;
2. El tratamiento responda a la libre y legítima aceptación de una relación jurídica entre el responsable y el titular, cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con base de datos. En este caso la transferencia o comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique;
3. Los datos personales deban proporcionarse a autoridades administrativas o judiciales en virtud de solicitudes y órdenes amparadas en competencias atribuidas en la norma vigente;
4. Cuando la comunicación se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando dichos datos se encuentren debidamente disociados o a lo menos anonimizados, y,
5. La comunicación de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que implique intereses vitales de su titular y este se encuentre impedido de otorgar su consentimiento.
6. La comunicación de datos de carácter personal relativos a la salud sea necesaria para realizar los estudios epidemiológicos de interés público, dando cumplimiento a los estándares internacionales en la materia de derechos humanos, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad. El tratamiento deberá ser de preferencia anonimizado, y en todo caso agregado, una vez pasada la urgencia de interés público.

Cuando la Unidad Educativa se encuentre frente a alguna de estas situaciones, lo dejará claramente revelado y en todo caso cumplirá con las demás disposiciones contenidas en la Ley.

El almacenamiento, uso, circulación, supresión o cualquier otro tratamiento que se dé a los datos recolectados se establecerá en el inventario de bases de datos. Es responsabilidad de cada "propietario" de una base de datos mantener esta información actualizada en el inventario, lo cual estará a cargo del Oficial de Protección de Datos.

Cuando se recolecten datos personales se tendrá en cuenta lo siguiente:

- En los formularios de recolección de datos se solicitarán únicamente los pertinentes y adecuados para la finalidad que estará descrita de manera clara y precisa.

	MANUAL INTERNO PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Fecha: 09-04-2025
		Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>13</b> de <b>32</b>

- La recolección de los datos corresponderá a un proceso documentado.
- Toda recolección contará con un consentimiento que cumpla con las características descritas en este capítulo y las establecidas en el Anexo Modelo - Consentimiento.
- El consentimiento de los datos personales que se recolecten de forma electrónica quedará registrado también electrónicamente y de manera explícita en la aplicación donde se recolecten los datos personales o, físicamente, a cargo del responsable del proceso.
- Los datos personales deben ser almacenados en las bases de datos que se registren en el Inventario de Bases de Datos o, en caso de generar una nueva base de datos, esta debe cumplir con todos los requisitos establecidos para su administración (Ver Numeral 7. Bases de Datos) y ser incluida en el inventario.
- Se mantendrá un registro de cada nueva versión de consentimiento.
- De cada consentimiento otorgado debe quedar prueba de su aceptación por parte del Titular.

Respecto a los sistemas de videovigilancia, se informará a los Titulares que se encuentran en una zona de monitoreo y observación; adicionalmente, se obtendrá su consentimiento a través de señales o avisos distintivos visibles y legibles, ubicados en los accesos principales a las zonas monitoreadas.

La Unidad Educativa conservará la prueba del consentimiento otorgado por los Titulares de los datos personales para su tratamiento, para lo cual adoptará las acciones necesarias para mantener registros o mecanismos técnicos o tecnológicos idóneos con el fin de determinar cuándo y cómo obtuvo ésta, de acuerdo con lo establecido por la ley.

La Unidad Educativa obtendrá del Titular un nuevo consentimiento cuando en la Política de Tratamiento haya un cambio sustancial respecto a la finalidad.

## 5.1 REVOCATORIA

Ante la Unidad Educativa podrá presentarse, en cualquier momento, la revocatoria del consentimiento, a través del correo electrónico: [dpd@ecomundo.edu.ec](mailto:dpd@ecomundo.edu.ec) o en la siguiente dirección: Plaza Parque, Km 12,5 Av. León Febres Cordero, Guayas. No se exigirá justificación alguna al titular para el efecto, y se establecerán mecanismos que garanticen celeridad, eficiencia, eficacia y gratuidad, así como un procedimiento sencillo, similar al proceder con el cual recabó el consentimiento. El tratamiento que se lleve a cabo antes de que el titular revoque el consentimiento es lícito. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste que dicho consentimiento se otorga para todas ellas.

Para el efecto se atenderá el término previsto para la atención de requerimientos, incluido en la Política y en el presente manual.

	MANUAL INTERNO	Fecha: 09-04-2025
	PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>14</b> de <b>32</b>

## 6 AVISO DE PRIVACIDAD

---

Adicionalmente, y con el fin de poner a disposición del Titular las Políticas de Tratamiento de Datos Personales en otros canales, se informará por medio de un Aviso de Privacidad al Titular sobre la existencia de tales políticas y la forma de acceder a las mismas, previamente y en todo caso a más tardar al momento de la recolección de los datos personales.

Se entiende por Aviso de Privacidad una comunicación escrita generada por el Responsable, y dirigida al Titular para el Tratamiento de sus datos personales en la que se le informa acerca de la existencia de las políticas de Tratamiento de la información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.

La referencia al Aviso de Privacidad será incluida en los formatos de recolección de datos y contratos pertinentes.

El anuncio indicará la responsabilidad de los Titulares respecto de la actualización de su información para el cumplimiento óptimo de los deberes de la Unidad Educativa. En cualquier caso, la Política de Tratamiento de Datos Personales estará publicada en el siguiente sitio web para su consulta: <https://ecomundo.edu.ec>

## 7 BASES DE DATOS

---

Los datos personales que administra la Unidad Educativa, como responsable, están organizados en un conjunto de bases de datos, físicas y electrónicas, relacionadas en el inventario de bases de datos.

Cualquier colección de datos personales que pueda ser considerada una base de datos, que no esté relacionada en el inventario, debe ser reportada al Oficial de Protección de Datos Personales para determinar si es necesaria, en cuyo caso se deberán ajustar los procesos para describir y controlar su tratamiento, y así ser incluida en el inventario; o, si se puede reemplazar por alguna de las que se encuentra inventariada y administrada.

Siempre que se determine un nuevo tratamiento de datos personales se hará una evaluación para establecer el impacto de este y posibles riesgos.

Todas las bases de datos deben considerar los principios de:

- **Confidencialidad:** La información contenida allí sólo debe ser accedida por las personas que tienen derecho a ella.

	MANUAL INTERNO PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Fecha: 09-04-2025
		Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>15</b> de <b>32</b>

- **Integridad:** La información debe mantener su veracidad y sólo ser modificada por personas autorizadas.
- **Disponibilidad:** La información debe estar disponible oportunamente (de acuerdo con los niveles de servicio ofrecidos) a las personas autorizadas.

Para lo anterior, el área de sistemas implementará los procesos de gestión tecnológica, basados en mejores prácticas de gestión de tecnología (ej. ITIL), con el fin de que se puedan cumplir estos principios en las bases de datos electrónicas.

En el caso de las bases de datos constituidas por documentos físicos, el Oficial de Protección de Datos definirá los lineamientos de control y manejo de documentos para garantizar los principios mencionados.

Por integridad y gobierno de datos, el objetivo es mantener el mínimo número de bases de datos y evitar su replicación. En este sentido, se evaluará permanentemente cómo se pueden revisar y ajustar los procesos para la reutilización y consolidación de las bases de datos. Así mismo, en el diseño y ajuste de procesos se incorporarán solo los datos personales requeridos para su objeto (protección por defecto) y se considerarán las medidas técnicas y organizacionales necesarias para garantizar la protección de los datos personales y de esta forma el cumplimiento de las obligaciones de ley y los requisitos planteados en el presente manual (protección por diseño).

Igualmente, se procurará administrar las bases de datos en sistemas de información estructurados, que permitan manejar el acceso, integridad, uso y respaldo de la información. Sin embargo, también hay bases de datos en archivos no integrados a estos sistemas, como hojas de cálculo o documentos electrónicos en plataformas como Google. En este caso, es muy importante considerar que:

- Todos los archivos que contengan bases de datos personales se deben almacenar en las herramientas institucionales de administración de información.
- Su acceso debe estar restringido a los usuarios determinados por los procesos que utilizan la base de datos y de acuerdo con los accesos de información definidos por los perfiles de cargo. En el caso de acceso remoto a bases de datos personales se debe tener un registro especial en la descripción de acceso del perfil de cargo y adicionalmente el área de sistemas entregará un documento con compromisos específicos para el manejo de estos datos.
- Estos archivos no se pueden transmitir por correo electrónico; en caso de requerir compartir esta información, en el marco de los procesos permitidos, se puede dar acceso y/o enviar el enlace al archivo.
- El administrador del repositorio de archivos debe garantizar el control de accesos y registro de versiones, de forma que haya trazabilidad para verificar alineación con los procesos.



	MANUAL INTERNO PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Fecha: 09-04-2025
		Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>16</b> de <b>32</b>

Eventualmente se manejarán bases de datos almacenadas físicamente, como documentos históricos o registros documentales físicos, entre otros. En este caso, se deben tener en cuenta todos los controles de protección de documentos, seguridad física y gestión de riesgos ambientales. En cuanto a seguridad física se deben considerar los principios de control de acceso y generación de barreras:

- ❖ **Disuasión:** Es el primer nivel de defensa, en que se evita el acceso por medio de avisos, procesos o áreas restringidas.
- ❖ **Negación:** Es la negación física del acceso, con puertas cerradas con llave, candados u otro tipo de bloqueos.
- ❖ **Detección:** Si el acceso se da, es importante poder detectarlo y notificarlo, bien sea con cámaras de vigilancia, alarmas y otros mecanismos que cubran este propósito.
- ❖ **Demora:** Finalmente, si se da el acceso a los documentos, se debe buscar un último elemento de demora que permita la acción de control, como vigilantes, que hayan sido notificados por los mecanismos de detección.

El Oficial de Protección de Datos deberá revisar, en conjunto con los responsables o proveedores de instalaciones físicas, el plan de control de accesos a las áreas en dónde se almacenen bases de datos personales físicas; este plan será revisado periódicamente para la identificación y gestión de riesgos.

## 7.1 LINEAMIENTOS DE TRATAMIENTO DE LA INFORMACIÓN

### 7.1.1 Política de Tratamiento de Datos Personales

Cuando se realice algún cambio sustancial en el contenido de la Política de Tratamiento, es decir, referidos a la identificación del Responsable y a la finalidad del Tratamiento de los datos personales, (los cuales puedan afectar el contenido del consentimiento) el Oficial de Protección de Datos debe asegurar que dichos cambios se comuniquen a los Titulares antes de o a más tardar al momento de implementar la nueva Política. Además, cuando el cambio se refiera a la finalidad del Tratamiento, se deberá obtener del Titular un nuevo consentimiento.

Todo tratamiento de datos personales debe considerar lo siguiente:

- ❖ Estar articulado en un proceso.
- ❖ Sólo se pueden tratar datos personales para las finalidades que tienen objetivos institucionales y que están cubiertas en los consentimientos de recolección.
- ❖ No se deben recolectar ni tratar datos personales cuya finalidad no esté claramente definida.
- ❖ Todas las bases de datos deben considerar las siguientes condiciones en el tratamiento:

	MANUAL INTERNO	Fecha: 09-04-2025
	PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>17</b> de <b>32</b>

- ✓ **Recolección:** Consentimiento de acuerdo con lo definido en el numeral 5 de este documento. Adicionalmente, se debe procurar que la información que se recolecte sea veraz y de calidad; con validaciones de formato y contenido, en el caso de los sistemas de información, o formularios explícitos con opciones claras y sin ambigüedades, en el caso de recolección física. Como parte de la gestión de riesgo, se evaluará semestralmente la calidad de los datos recolectados, se identificarán los aspectos que generan riesgos en la calidad de estos y se desarrollarán correctivos para mejorar la calidad de la información.
  - ✓ **Almacenamiento:** Se deben almacenar en medios que cuenten con los controles de seguridad necesarios. Así mismo, deben tener mecanismos de respaldo. En el caso de las bases de datos en archivos no integrados (Word, Excel), se debe contar con las herramientas provistas por la Unidad Educativa para garantizar su respaldo.
  - ✓ **Uso:** Deben tener los controles necesarios para que sólo sean utilizadas por las personas autorizadas de acuerdo con los procesos.
  - ✓ **Circulación:** Siempre se debe verificar la circulación de estos datos contra las autorizaciones de tratamiento y los procesos. Se aplicará el lineamiento de la menor circulación posible.
  - ✓ **Supresión:** Todas las bases de datos deben tener los mecanismos automatizados o manuales para la supresión, de acuerdo con los requerimientos de ley y los procesos. El proceso de supresión debe estar claramente documentado y debe dejar registro de la operación. En caso de administrar archivos físicos, se evaluará la implementación de tablas de retención documental.
- ❖ En caso del tratamiento de datos personales de niñas, niños y adolescentes, se tendrá particular cuidado para:
- ✓ Responder y respetar el interés superior de los niños, niñas y/o adolescentes.
  - ✓ Asegurar el respeto de sus derechos fundamentales.
  - ✓ Contar con el consentimiento expreso del titular (menores 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 especifiquen con claridad sus fines) o de su representante legal.
  - ✓ Implementar medidas adecuadas para garantizar una protección reforzada de esta información.
  - ✓ Asegurar que se informa al titular o responsable, acerca de que no hay obligación de suministrar datos sensibles.
  - ✓ No será necesario el consentimiento cuando dicho tratamiento esté destinado a salvaguardar un interés público esencial en los términos de la LOPDP.

	MANUAL INTERNO PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Fecha: 09-04-2025
		Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>18</b> de <b>32</b>

- ❖ En el tratamiento de datos de salud y datos de personas con discapacidad, se tendrá particular cuidado para:
  - ✓ Tratar los datos relativos a la salud cumpliendo los principios de confidencialidad y secreto profesional.
  - ✓ Contar con el consentimiento previo del titular para su tratamiento salvo cuando el tratamiento sea necesario para proteger intereses vitales del interesado, si este no está 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 caso este en el que el tratamiento sólo se hará por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad.
  
- ❖ En caso de estar tratando datos crediticios, se tendrá particular cuidado para:
  - ✓ Permitir de forma gratuita el acceso de forma personal a la información del titular cuantas veces lo requiera, respecto de la información que sobre sí mismos esté registrada ante los prestadores de servicios de referencia crediticia y a través de los siguientes mecanismos: a) Observación directa a través de pantallas; b) Entrega de impresiones de los reportes.
  - ✓ Elaborar el reporte de crédito de tal forma que permita conocer de manera clara y precisa la condición en que se encuentra el historial crediticio del titular, si la Unidad Educativa elabora tal documento.
  - ✓ Actualizar, rectificar y eliminar las fuentes de información, según el caso, de la información que fuese ilícita, falsa, inexacta, errónea, incompleta o caduca,
  - ✓ Atender en los términos de la LOPDP la solicitud de actualización, rectificación o eliminación de la información admitiéndola o rechazándola motivadamente, y;
  - ✓ Certificar el proceso de revisión, en los reportes de crédito que emitan, que la información materia de la solicitud está siendo revisada a pedido del titular.
  
- ❖ En caso de estar tratando datos sensibles, se tendrá particular cuidado para:
  - ✓ Requerir el consentimiento previo,
  - ✓ Informar al titular que el consentimiento para su tratamiento es facultativo,
  - ✓ Especificar en el consentimiento qué tipo de dato sensible se recolecta y;
  - ✓ Precisar e informar la finalidad del tratamiento.

### 7.1.2 Registro de Actividades de Tratamiento

	MANUAL INTERNO PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Fecha: 09-04-2025
		Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>19</b> de <b>32</b>

Se llevará un registro de todas las actividades de tratamiento de datos personales con la siguiente información:

1. El nombre de la Unidad Educativa como responsable del tratamiento y, de ser el caso del responsable que actúe conjuntamente con la Unidad Educativa, así como el nombre y los datos de contacto del oficial 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. El uso de perfiles de ser el caso,
6. De ser el 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.

## 7.2 ADMINISTRACIÓN DEL INVENTARIO DE BASES DE DATOS

- ❖ El inventario de Bases de Datos estará administrado por el Oficial de Protección de Datos Personales.
- ❖ Los responsables de las bases de datos deberán comunicarle al Oficial de Protección de Datos sobre cualquier modificación en la información del inventario.
- ❖ Si hay una modificación en la naturaleza de la base de datos (naturaleza de los datos, almacenamiento, etc.) se debe verificar qué impacto tiene en los procesos y actualizarlos de ser necesario.
- ❖ Periódicamente se realizará una revisión de los procesos que tienen datos personales sensibles.
- ❖ El Oficial de Protección de Datos realizará evaluaciones periódicas de la calidad del inventario, así como de los procesos operativos; generará reportes y definirá acciones preventivas y correctivas tendientes a garantizar que la información en este sea precisa y refleje todo el tratamiento de datos personales que se realiza.

## 7.3 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

	MANUAL INTERNO	Fecha: 09-04-2025
	PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>20</b> de <b>32</b>

El Sistema de Gestión de la Seguridad de la Información de la Unidad Educativa, podrá basarse en los lineamientos contenidos en la norma ISO27001, de los cuales la siguiente figura detalla los hitos a implementar:



### 7.3.1 Definición de la Política

- ✓ **Objetivo:** Proteger la información de la Unidad Educativa, de cualquier amenaza, de forma tal que se garantice en todo momento los pilares de la triada de información: Confidencialidad, Integridad y Disponibilidad.
- ✓ **Alcance:** La definición de las políticas de seguridad de la información están dirigida para (personal administrativo, educadores, estudiantes, terceros) que hagan uso de los sistemas de información y/o aplicaciones que la Unidad Educativa defina.

### 7.3.2 Análisis de Riesgos (RA)

- ✓ Identificar los activos de Información (clasificación).
- ✓ Identificar, evaluar y priorizar los riesgos, amenazas de los sistemas de información objeto de la política.
- ✓ Definir amenazas o vulnerabilidades.

### 7.3.3 Gestión del Riesgo

	MANUAL INTERNO	Fecha: 09-04-2025
	PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>21</b> de <b>32</b>

- ✓ Definir el grado de aseguramiento requerido.
- ✓ Definir amenazas o vulnerabilidades.

#### 7.3.4 Selección de los Controles a Implementar

- ✓ Uso de credenciales y claves con cierto grado de dificultad.
- ✓ Uso de doble factor de autenticación.
- ✓ Controles propuestos por la norma.

#### 7.3.5 Declaración de Aplicabilidad

- ✓ Controles seleccionados.

#### 7.3.6 Revisión del Sistema

- ✓ Valoración de las medidas preventivas.
- ✓ Medidas Correctivas.
- ✓ Propuestas de Mejora.

La Unidad Educativa adelantará auditorías periódicas que se realicen en el marco de la política de seguridad de la información para verificar y evaluar la eficiencia, eficacia y efectividad de las medidas técnicas, organizaciones y de proceso implementadas para garantizar la seguridad en el tratamiento de datos personales.

El Inventario de Bases de Datos deberá contener la relación de cada base de datos y el detalle de la información personal que administra la Unidad Educativa.

## 8 ENCARGADO DEL TRATAMIENTO

---

La LOPDP señala que el Encargado es la 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. Para el desarrollo de su labor los Encargados podrán eventualmente designar a una persona o área que asuma la función de protección de datos personales que dará trámite a las solicitudes de los Titulares.

	MANUAL INTERNO PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Fecha: 09-04-2025
		Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>22</b> de <b>32</b>

## 8.1 DEBERES Y OBLIGACIONES EN CALIDAD DE ENCARGADO DEL TRATAMIENTO

El Encargado que solo o conjuntamente con otros trate datos personales a nombre y por cuenta del responsable del tratamiento de datos personales deberá cumplir con las siguientes obligaciones de conformidad con lo previsto en el artículo 47 de la LOPDP:

- ✓ Tratar datos personales en estricto apego a los principios y derechos desarrollados en la LOPDP, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia;
- ✓ 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 Autoridad de Protección de Datos Personales, o normativa sobre la materia;
- ✓ 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;
- ✓ Implementar políticas de protección de datos personales afines al tratamiento de datos personales en cada caso en particular;
- ✓ Utilizar metodologías de análisis y gestión de riesgos adaptadas a las particularidades del tratamiento y de las partes involucradas;
- ✓ Realizar evaluaciones de adecuación al nivel de seguridad previas al tratamiento de datos personales;
- ✓ Tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas;
- ✓ 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 en la LOPDP; excepto en los casos igualmente allí contenidos;
- ✓ Implementar la protección de datos personales desde el diseño y por defecto;
- ✓ Suscribir contratos de confidencialidad y manejo adecuado de datos personales con el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales;
- ✓ 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 Autoridad de Protección de Datos Personales;
- ✓ Designar al Delegado de Protección de Datos Personales, en los casos que corresponda;
- ✓ 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,

	MANUAL INTERNO PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Fecha: 09-04-2025
		Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>23</b> de <b>32</b>

- ✓ Los demás establecidos en la LOPDP en su reglamento, en directrices, lineamientos, regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

El tratamiento de datos personales realizado por terceros se regulará por un contrato, en el que se establecerá de manera clara y precisa que el encargado del tratamiento de datos personales tratará únicamente los mismos conforme las instrucciones de la Unidad Educativa 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. (Ver Anexo Modelo - Contrato con Encargados).

## 8.2 LISTADO

El Oficial de Protección de Datos creará un listado de “Encargados-Terceros” donde se consigne la identificación de los terceros que manejan datos personales en desarrollo de su relación con la Unidad Educativa.

## 9 TRANSFERENCIA NACIONAL O INTERNACIONAL

---

La Unidad Educativa podrá transferir la información de los datos personales a terceros cuando se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas de la Unidad Educativa y del destinatario, cuando la transferencia se encuentre configurada dentro de una de las causales de legitimidad establecidas en la LOPDP y cuente con el consentimiento previo del titular del dato quien debe haber sido informado de forma suficiente sobre la finalidad a la que se destinarán sus datos y el tipo de actividad del tercero a quien se pretende transferir o comunicar dichos datos.

La transferencia de datos personales que se realice observará las reglas que para tal efecto disponga la legislación vigente, la LOPDP y los decretos y reglamentos que la modifiquen o adicionen.

Especialmente se tendrán en cuenta los siguientes lineamientos:

Cuando se trate de transferencias nacionales de datos personales, la Unidad Educativa o sus encargados exigirán el cumplimiento de los requisitos de la legislación de protección de datos vigente y las medidas de protección al responsable destinatario, según sea el caso, lo cual quedará debidamente documentando.



	MANUAL INTERNO	Fecha: 09-04-2025
	PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>24</b> de <b>32</b>

Cuando se trate de transferencias internacionales, la Unidad Educativa podrá transferir o comunicar datos personales a países declarados con nivel adecuado de protección o, en su defecto, cuando el responsable del tratamiento de datos personales ofrezca garantías adecuadas para el titular, para lo cual se deberá observar lo siguiente:

- ✓ Garantizar el cumplimiento de principios, derechos y obligaciones en el tratamiento de datos personales en un estándar igual o mayor a la normativa ecuatoriana vigente.
- ✓ Efectiva tutela del derecho a la protección de datos personales, a través de la permanente de acciones administrativas o judiciales; y,
- ✓ El derecho a solicitar la reparación integral, de ser el caso.

Estas deberán constar por escrito en un instrumento jurídico vinculante que cumpla como mínimo con los parámetros establecidos en el Capítulo IX de la LOPDP.

## 10 ATENCIÓN DE REQUERIMIENTOS

---

### 10.1 DERECHOS

La Unidad Educativa garantiza el ejercicio de los siguientes derechos contenidos en la LOPDP y que se resumen así:

- ✓ **A la información:** ser informado sobre, los fines, tipo de tratamiento, conservación, contacto del Responsable, transferencias, entre otros.
- ✓ **De acceso:** conocer y obtener acceso a todos sus datos personales.
- ✓ **De rectificación y actualización:** sobre los datos inexactos o incompletos.
- ✓ **De eliminación:** en unas condiciones establecidas (ej. El tratamiento no cumple con la finalidad, no es pertinente, existe obligación legal, etc.)
- ✓ **De oposición:** oponerse o negarse al tratamiento en ciertos casos (ej. Mercadotecnia directa, incluida la elaboración de perfiles).
- ✓ **A la portabilidad:** recibir de la Unidad Educativa sus datos personales en un formato compatible, actualizado, estructurado de acuerdo con la regulación que para el efecto expida la Autoridad de Protección de Datos Personales.
- ✓ **A la suspensión del Tratamiento:** en determinadas situaciones tales como cuando el tratamiento es ilícito, o que el Responsable ya no necesite los datos por haber agotado la finalidad para la cual fueron recolectados, entre otros.
- ✓ **A no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas:** Incluye la elaboración de perfiles.

	MANUAL INTERNO	Fecha: 09-04-2025
	PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>25</b> de <b>32</b>

- ✓ **Derecho de niñas, niños y adolescentes:** A no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas y a contar con el consentimiento para datos sensibles.
- ✓ **De consulta:** Pública y gratuita ante el “Registro Nacional de Protección de Datos Personales”.
- ✓ **Derechos especiales para titulares de datos crediticios:** Las Unidad Educativa garantiza los siguientes derechos adicionales para dichos datos: a) Acceder de forma personal a la información de la cual son titulares; b) Que el reporte de crédito permita conocer de manera clara y precisa la condición en que se encuentra su historial crediticio; y, c) Que las fuentes de información actualicen, rectifiquen o eliminen, según el caso, la información que fuese ilícita, falsa, inexacta, errónea, incompleta o caduca.

En ningún caso se solicitará o aceptará la renunciabilidad de los anteriores derechos por parte de su titular y tendrá por nula toda estipulación en contrario. La Unidad Educativa respetará y velará por el pleno ejercicio de los derechos de los Titulares. Todos los derechos serán tramitados de conformidad con la LOPDP.

## 10.2 ATENCIÓN DE REQUERIMIENTOS

Para el adecuado ejercicio de los derechos descritos, el Oficial de Protección de Datos será el encargado de recibir, gestionar y dar respuesta a los requerimientos, peticiones, quejas o reclamaciones que presenten los Titulares o los titulares de derechos sucesorios (de las personas fallecidas) o apoderados. 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 el responsable del tratamiento.

Para el efecto, se han dispuesto los canales de contacto correo electrónico: [dpd@ecomundo.edu.ec](mailto:dpd@ecomundo.edu.ec) o en la siguiente dirección: Plaza Parque, Km 12,5 Av. León Febres Cordero, Guayas, Ecuador, para que los Titulares ejerzan los derechos que le asisten.

Una vez presentado el requerimiento, se contará con un término de diez (10) días para contestar afirmativa o negativamente, notificar y ejecutar lo que corresponda.

En caso de que la Unidad Educativa requiera ampliar o aclarar la petición formulada por un titular podrá requerirlo por una sola vez y dentro del término de cinco (5) días de recibida la solicitud. El titular contará con diez (10) días a partir del día siguiente en que haya sido notificado para aclarar o completar la solicitud, vencido el cual y recibida respuesta la Unidad Educativa dará debida atención. De no recibirse respuesta se archivará la solicitud notificando dicho acto al titular.

	MANUAL INTERNO	Fecha: 09-04-2025
	PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>26</b> de <b>32</b>

El Oficial de Protección de Datos elaborará un registro de todas las solicitudes de ejercicio de derechos y la atención dada de acuerdo con lo que para el efecto establezca la Autoridad de Protección de Datos Personales.

## 11 GESTIÓN DE RIESGOS

---

Con el fin de fortalecer los procesos y actividades relacionadas con el Tratamiento de datos personales de sus Titulares, se adopta un Sistema de Gestión de Riesgos, a través del cual se identificarán, medirán y controlarán todas aquellas situaciones o hechos que puedan generar alguna afectación de los derechos de habeas data.

Para el análisis de riesgos, amenazas y vulnerabilidades, se deberán considerar:

1. Las particularidades del tratamiento.
2. Las partes involucradas.
3. Las categorías y volumen de los datos tratados.

Este sistema será administrado por el Oficial de Protección de Datos quien coordinará los recursos necesarios para gestionar adecuadamente los riesgos identificados. Este sistema considera los siguientes aspectos:

- **Identificación del riesgo:** Clara identificación del riesgo que se está gestionando.
- **Impacto:** Evaluación del impacto directo y consecuencias colaterales si el riesgo se materializa. Este impacto se debe evaluar desde la perspectiva del negocio, así como en el posible incumplimiento de la Ley de Protección de Datos y otras normativas.
- **Base de Datos y Datos Comprometidos**
- **Categoría y volumen** de los datos tratados
- **Titulares**
- **Particularidades del Tratamiento:** Observaciones sobre el tratamiento relevantes a la evaluación del riesgo.
- **Otras partes involucradas:** Áreas, procesos o terceros relacionados en el tratamiento de los datos o con el riesgo identificado.
- **Probabilidad de ocurrencia:** Porcentaje estimado de ocurrencia del riesgo.
- **Peso del riesgo:** Es el producto de multiplicar el impacto por la probabilidad; esto facilita la priorización de riesgos para su atención.
- **Acciones frente al riesgo:**
  - **Mitigación:** Acciones para reducir el impacto o probabilidad de ocurrencia.
  - **Transferencia:** Asignación del riesgo a una tercera parte que lo asuma y exima a la Unidad Educativa de su impacto o consecuencias.
  - **Evitación:** Eliminación de las acciones que generaron el riesgo.
  - **Aceptación:** Aceptación del riesgo y su impacto. Planeación para su manejo.

	MANUAL INTERNO	Fecha: 09-04-2025
	PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>27</b> de <b>32</b>

- **Responsable de las acciones:** Persona que llevará acabo las acciones definidas.
- **Evaluación de las acciones:** Evaluación del cumplimiento del objetivo de las acciones propuestas en la gestión de riesgos.

El Oficial de Protección de Datos convocará periódicamente o cuando lo considere pertinente tanto al Comité de Protección de Datos Personales como a las personas responsables de la evaluación y toma de decisiones sobre los diferentes riesgos e informará a la Dirección de la Unidad Educativa sobre su gestión y avance.

Así mismo, deberán identificar y llevar a cabo iniciativas tendientes a gestionar proactivamente los riesgos.

## 12 GESTIÓN DE INCIDENTES

---

El Oficial de Protección de Datos es el responsable de manejar los incidentes o vulneraciones a los sistemas de información donde se gestionan datos personales y a los archivos físicos.

*“Incidente”* se refiere a cualquier evento en los sistemas de información o bases de datos manuales o sistematizadas, que atente contra la seguridad de los datos personales en ellos almacenados.

En caso de presentarse un incidente o vulneración de los datos se llevarán a cabo los siguientes pasos:

1. Contener el incidente de seguridad y hacer una evaluación preliminar.
2. Evaluar los riesgos e impactos asociados con el incidente de seguridad.
3. Identificar los daños para las personas, organizaciones y público en general.
4. Notificar a la Autoridad de Protección de Datos en un término máximo de cinco (5) días.
5. Comunicar a los Titulares de la información. Esta notificación considerará el plazo máximo de tres (3) días, dependiendo de las condiciones definidas en la LOPDP y las determinaciones que tome la Autoridad de Protección de Datos.
6. Prevenir futuros incidentes de seguridad en cuanto a Datos Personales.

En particular se debe tener presente lo siguiente:

1. El área involucrada debe reportar al Oficial de Protección de Datos el incidente presentado.
2. Recopilar los datos del incidente: fecha de ocurrencia, fecha en la que se tuvo conocimiento, sistema o base de datos vulnerada, número de titulares afectados, causal, tipo de datos personales comprometidos y responsables.
3. Registrar el incidente en la Base de Datos de Incidentes.
4. Analizar con las personas involucradas las posibles causas y consecuencias del incidente. Formalizar el análisis y generar las acciones correspondientes.
5. Reportar detalles del incidente a la Dirección de la Unidad Educativa.

	MANUAL INTERNO PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Fecha: 09-04-2025
		Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>28</b> de <b>32</b>

6. Periódicamente, evaluar en conjunto con el Comité de Protección de Datos Personales, el impacto de las acciones correctivas en el riesgo y ocurrencia de nuevos incidentes, dentro del plan de revisión, evaluación y mejoramiento.
7. Generar el plan de comunicación para los Titulares afectados incluyendo herramientas para minimizar el daño potencial o causado.

La notificación a la autoridad de datos personales se deberá efectuar siempre que sea probable que dicha violación constituye un riesgo para los derechos y libertades de las personas naturales, esto es cuando concurra cualquiera de las siguientes causales:

- ✓ Cuando los datos fueron destruidos, ya no existen o no están disponibles de una forma que sea de utilidad para el responsable del tratamiento;
- ✓ Cuando los datos personales han sido alterados, corrompidos o dejan de estar completos,
- ✓ Cuando el responsable ha perdido el control o acceso a los datos o ya no obran en su poder, o
- ✓ Cuando el tratamiento no ha sido autorizado o es ilícito lo cual incluye la divulgación de datos personales o el acceso por parte de destinatarios que no están autorizados a recibir o acceder a los datos o cualquier otra forma de tratamiento que se ejecuta contrariando la Ley.

La notificación de vulneración de seguridad a la autoridad deberá contener lo siguiente:

- ✓ La naturaleza y tipo de vulneración;
- ✓ Identificar los titulares o interesados afectados,
- ✓ El detalle inicial de los sistemas vulnerados,
- ✓ La causa presunta de la vulneración,
- ✓ El volumen y tipo de datos expuestos o comprometidos,
- ✓ Las medidas adoptadas y previstas para responder y remediar la vulneración con la finalidad de mitigar las consecuencias presuntas;
- ✓ La evaluación del riesgo que la vulneración implica para los derechos y libertados de los titulares y;
- ✓ Aquellos aspectos adicionales que determine la Autoridad de Protección de Datos Personales.

## 13 GESTIÓN DE RECURSOS HUMANOS

---

Se han definido acciones específicas con el propósito de fortalecer la cultura de protección de datos personales en todos los empleados de la Unidad Educativa.

	MANUAL INTERNO PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Fecha: 09-04-2025
		Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>29</b> de <b>32</b>

Así mismo, dado que los empleados son también titulares de datos personales, el manejo de esta información es responsabilidad de la Dirección de Talento Humano bajo los lineamientos estipulados en este manual y los requisitos de ley exigidos.

### 13.1 LINEAMIENTOS GENERALES

Todos los empleados deben conocer la Política de Protección de Datos Personales.

Cuando corresponda, en la descripción del perfil de cargo se incluirá una responsabilidad relacionada con el acceso o uso de datos personales similar a esta:

*“Manejar la información de acuerdo con lo establecido en la Política de Protección de Datos Personales, el Manual Interno y los demás lineamientos que determine la Unidad Educativa”.*

Los contratos laborales de los empleados deben incluir:

- ✓ Cláusula relacionada con el tratamiento de información confidencial (específica respecto de datos personales) y el conocimiento y compromiso con la aplicación de la Política de Tratamiento de Datos Personales. (Ver Anexo – Modelo Cláusula contratos laborales).
- ✓ Consentimiento de Tratamiento de Datos Personales y de Datos Sensibles. (Se dejará un registro de todos los consentimientos otorgados por los empleados).

Los procesos de ingreso y retiro del personal deben considerar las condiciones de acceso a la información y el bloqueo a la misma cuando sea pertinente (por suspensión, retiro, etc.).

La Dirección de Talento Humano, en conjunto con el Oficial de Protección de Datos y el Comité de Protección de Datos, determinarán para cada cargo el nivel de acceso a la información de datos personales teniendo en cuenta: las responsabilidades, funciones y procesos, entre otros. Dicho acceso se basará en la matriz definida para tal fin (Anexo Perfiles de cargo – accesos de información). En el formato de descripción del perfil de cargo también se agregará un ítem para referirse a dicha matriz.

### 13.2 CAPACITACIÓN Y COMUNICACIONES

En concordancia con el ítem anterior, el desarrollo de planes de capacitación y/o de comunicaciones será apoyo fundamental para el fortalecimiento de la cultura de protección de datos personales. Por lo tanto, la Dirección de Talento Humano y el Oficial de Protección de Datos deberán diseñar, implementar y hacer seguimiento trimestral a los planes definidos con el fin de garantizar el cumplimiento de la Política de Tratamiento de Datos Personales y del presente Manual.

	MANUAL INTERNO	Fecha: 09-04-2025
	PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>30</b> de <b>32</b>

### 13.3 CAPACITACIÓN

Tal y como se enunció en el ítem 13.1, todos los empleados de la Unidad Educativa deben conocer la Política de Tratamiento de Datos Personales.

- ❖ Se programará al menos una sesión de capacitación general sobre el tema para todo el personal.
- ❖ Además, aquellas personas que tienen a cargo bases de datos con información personal tendrán al menos una sesión adicional con énfasis en conocer y asegurar el cumplimiento de sus deberes respecto a dicha información.
- ❖ Toda capacitación realizada sobre este tema debe dejar una evidencia de registro de asistencia a la misma. Dicho registro debe guardarse para una posterior consulta, en caso de requerirse.

### 13.4 COMUNICACIONES

#### Comunicación externa:

- ✓ El Oficial de Protección de Datos es el responsable de modificar, entregar y/o publicar los textos de avisos y notificaciones que deban divulgarse, garantizando que éstos se mantienen actualizados. Además, debe conservar el registro y la trazabilidad de dichos documentos.
- ✓ Las comunicaciones dirigidas a los Titulares deben ser claras y comprensibles. Se debe procurar que los titulares de datos personales conozcan sus derechos y los mecanismos que tienen a disposición para ejercerlos.

#### Comunicación interna:

- ✓ Como complemento a la capacitación, se podrán utilizar otros medios de comunicación disponibles (videos, carteles, entre otros) con el fin de reforzar la información relacionada con protección de datos personales al interior de la Unidad Educativa.
- ✓ Los empleados directos, que a su vez son titulares de datos personales, podrán informarse a través de estos medios acerca de sus derechos, los programas de control implementados y los mecanismos que tienen a disposición para ejercer tales derechos.

## 14 EVALUACIÓN Y SEGUIMIENTO

---

	MANUAL INTERNO PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Fecha: 09-04-2025
		Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>31</b> de <b>32</b>

El Oficial de Protección de Datos realizará un seguimiento continuo a la ejecución del Programa con el fin de garantizar su pertinencia, eficacia permanente y el cumplimiento de los requisitos de ley vigentes.

## 14.1 PLAN DE REVISIÓN, EVALUACIÓN Y MEJORAMIENTO

### Plan de revisión:

Cada año, el Oficial de Protección de Datos elaborará un plan que incluirá los temas, fechas e indicadores para la revisión integral del Programa.

### Evaluación y mejoramiento:

Los temas para revisar y evaluar deben incluir como mínimo:

- ✓ Nuevas amenazas y riesgos detectados.
- ✓ Requerimientos, peticiones, quejas o reclamaciones presentadas durante el período evaluado.
- ✓ Incidentes o vulneraciones de seguridad presentadas durante el período evaluado.
- ✓ Informe de seguimiento a los resultados y acciones identificadas en las auditorías de seguridad de la información.
- ✓ Resultados de las acciones de correctivas generadas a partir de los requerimientos o incidentes.
- ✓ Ejecución de los procesos.
- ✓ Cumplimiento de las políticas y lineamientos.
- ✓ Desempeño de los indicadores.
- ✓ Resultados de los planes de capacitación y comunicaciones.
- ✓ Nueva regulación o mejores prácticas.

De acuerdo con el análisis realizado y los resultados obtenidos, el Oficial de Protección de Datos determinará un plan de acción especificando las actividades, responsables y fechas de ejecución.

Una vez cumplida la evaluación, informará a la Dirección de la Unidad Educativa acerca de los resultados, avances y en general, la evolución del Programa.

## 14.2 INFORMES

El seguimiento al desempeño y evolución del Programa Integral de Gestión de Datos Personales se realizará mediante la generación y análisis periódico de informes e indicadores.



	MANUAL INTERNO PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES	Fecha: 09-04-2025
		Versión: 1.0
	Proceso: Procuraduría Síndica	Página <b>32</b> de <b>32</b>

### TABLA DE INFORMES

NOMBRE	DESCRIPCIÓN	MÉTRICA/INDICADOR
Inventario de Bases de Datos	Número de bases de datos existentes y condiciones con respecto a los requerimientos de la Política.	- Número de bases de datos - Número de titulares por cada base de datos.
Inventario de Encargados y Terceros	Listado de Encargados de Tratamiento y terceros y estado con respecto a los requerimientos.	- Número de encargados y terceros. - Cumple / No Cumple (con la Ley)
Requerimientos	Reporte de gestión de las diferentes solicitudes recibidas.	- Cantidad por tipo de solicitud (requerimientos, peticiones, quejas o reclamaciones) - Causales - Tiempos de atención
Incidentes/Vulneraciones de seguridad	Consolidado de incidentes en un período determinado. Reporte obligatorio a la Autoridad de Protección de Datos Personales y a la Agencia de Regulación y Control de las Telecomunicaciones en caso de presentarse algún incidente o vulneración de datos.	- Número de incidentes por período. - Tipo de incidentes, fecha de ocurrencia y de conocimiento; causal, tipo de datos personales comprometidos y cantidad de titulares afectados.
Capacitación	Informe de ejecución y resultados de los planes de capacitación y comunicaciones.	- Cantidad de personas capacitadas/Total de empleados. - Cantidad de acciones ejecutadas.
Estado de proyectos relacionados con el PIGDP	Informe de estado de los proyectos asociados a la implementación del Programa Integral de Gestión de Datos Personales.	-Porcentaje de cumplimiento de actividades planeadas.

## 15 GLOSARIO

- LOPDP: Ley Orgánica de Protección de Datos Personales
- OPD: Oficial de Protección de Datos
- PIGDP: Programa Integral de Gestión de Datos Personales