

**RESOLUCIÓN Nro. 005-DIGERCIC-CGAJ-DPyN-2026**

Mgs. Ottón José Rivadeneira González  
**DIRECCIÓN GENERAL DE REGISTRO CIVIL,  
IDENTIFICACIÓN Y CEDULACIÓN**

**CONSIDERANDO:**

- Que,** el numeral 2 del artículo 18 de la Constitución de la República del Ecuador, establece: *"Todas las personas, en forma individual o colectiva, tienen derecho a: (...) 2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley (...)"*;
- Que,** los numerales 11 y 19 del artículo 66 de la Constitución de la República del Ecuador, disponen: *"Se reconoce y garantizará a las personas: (...) 11. El derecho a guardar reserva sobre sus convicciones. Nadie podrá ser obligado a declarar sobre las mismas. En ningún caso se podrá exigir o utilizar sin autorización del titular o de sus legítimos representantes, la información personal o de terceros sobre sus creencias religiosas, filiación o pensamiento político; ni sobre datos referentes a su salud y vida sexual, salvo por necesidades de atención médica; y, (...) 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley (...)"*;
- Que,** el artículo 82 de la Constitución de la República del Ecuador, señala: *"El derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídica previas, claras, públicas y aplicadas por las autoridades competentes"*;
- Que,** el artículo 83 de la Constitución de la República del Ecuador, determina que son deberes y responsabilidades de las ecuatorianas y los ecuatorianos, sin perjuicio de otros previstos en la Constitución y la ley: *"1. Acatar y cumplir la Constitución, la ley y las decisiones legítimas de autoridad competente. (...)"*;
- Que,** el artículo 84 de la Constitución de la República del Ecuador, prevé: *"(...) todo órgano con potestad normativa tendrá la obligación de adecuar, formal y materialmente, las leyes y demás normas jurídicas a los derechos previstos en la Constitución y los tratados internacionales, y los que sean necesarios para garantizar la dignidad del ser humano o de las comunidades, pueblos y nacionalidades. En ningún caso, la reforma de la Constitución, las leyes, otras normas jurídicas ni los actos del poder público atentarán contra los derechos que reconoce la Constitución."*;
- Que,** el artículo 92 de la Constitución de la República del Ecuador manifiesta: *"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 (...)"*;

- Que,** el artículo 225 de la Constitución de la República del Ecuador establece: *“El sector público comprende: 1. Los organismos y dependencias de las funciones Ejecutiva, Legislativa, Judicial, Electoral y de Transparencia y Control Social. 2. Las entidades que integran el régimen autónomo descentralizado. 3. Los organismos y entidades creados por la Constitución o la ley para el ejercicio de la potestad estatal, para la prestación de servicios públicos o para desarrollar actividades económicas asumidas por el Estado. 4. Las personas jurídicas creadas por acto normativo de los gobiernos autónomos descentralizados para la prestación de servicios públicos”;*
- Que,** el artículo 226 de la Constitución de la República del Ecuador prescribe: *“(…) Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la Ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución (…)”;*
- Que,** el artículo 227 de la Constitución de la República del Ecuador señala: *“La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación”;*
- Que,** el artículo 233 de la Constitución de la República del Ecuador determina: *“Ninguna servidora ni servidor público estará exento de responsabilidades por los actos realizados en el ejercicio de sus funciones, o por sus omisiones, y serán responsables administrativa, civil y penalmente por el manejo y administración de fondos, bienes o recursos públicos. (…)”;*
- Que,** el artículo 17 del Código Orgánico Administrativo señala: *“Principio de buena fe. Se presume que los servidores públicos y las personas mantienen un comportamiento legal y adecuado en el ejercicio de sus competencias, derechos y deberes”;*
- Que,** el artículo 128 del Código Orgánico Administrativo señala: *“Acto normativo de carácter administrativo.- Es toda declaración unilateral efectuada en ejercicio de una competencia administrativa que produce efectos jurídicos generales, que no se agota con su cumplimiento y de forma directa”;*
- Que,** el artículo 130 del Código Orgánico Administrativo dispone: *“Las máximas autoridades administrativas tienen competencia normativa de carácter administrativo únicamente para regular los asuntos internos del órgano a su cargo, salvo los casos en los que la ley prevea esta competencia para la máxima autoridad legislativa de una administración pública.”*
- Que,** el numeral 7 del artículo 3 de la Ley Orgánica de Gestión de la Identidad y Datos Civiles, señala: *“7. Propender a la simplificación, automatización e interoperabilidad de los procesos concernientes a los hechos y actos relativos al estado civil de las personas, de conformidad a la normativa legal vigente para el efecto”;*

- Que,** el artículo 5 de la Ley Orgánica de Gestión de la Identidad y Datos Civiles dispone: "*La Dirección General de Registro Civil, Identificación y Cedulación es una entidad de derecho público, desconcentrada, adscrita al ministerio rector del sector, con personalidad jurídica propia, dotada de autonomía administrativa, operativa y financiera. Será la encargada de la administración y provisión de servicios relacionados con la gestión de la identidad y de los hechos y actos relativos al estado civil de las personas (...)*";
- Que,** el artículo 8 de la Ley Orgánica de Gestión de la Identidad y Datos Civiles prescribe: "*El Director General es la máxima autoridad de la Dirección General de Registro Civil, Identificación y Cedulación. Su cargo será de libre nombramiento y remoción y su designación corresponde al Ministro rector del sector. Para ejercer este cargo se requerirá tener título académico de tercer nivel y demás requisitos establecidos en la ley que regula a los servidores públicos*";
- Que,** en el numeral 2 del artículo 9, de la Ley Orgánica de Gestión de la Identidad y Datos Civiles consta como atribución del Director General: "*Expedir actos administrativos y normativos, manuales e instructivos u otros de similar naturaleza relacionados con el ámbito de sus competencias*";
- Que,** el artículo 75 de la Ley Orgánica de Gestión de la Identidad y Datos Civiles, establece: "*Acceso y Protección de la información.- El acceso a los archivos físicos y electrónicos de los cuales es custodio la Dirección General de Registro Civil, Identificación y Cedulación que están sujetos al principio de confidencialidad y publicidad, derivada del derecho a la protección de datos de carácter personal, podrá darse únicamente por autorización de su titular, por el representante legal o por orden judicial*";
- Que,** el artículo 96 de la Ley Orgánica de Gestión de la Identidad y Datos Civiles, señala: "*Sistema informático.- Para los procesos de identificación y expedición de la cédula de identidad, se empleará la captura biométrica de las características personales y la captura de datos de los atributos de la persona, tales como nombre, nacionalidad, domicilio, estado civil, entre otros. Se lo realizará a través de sistemas tecnológicos que permitan obtener datos seguros, confiables y verídicos, que se implementen para el efecto. Su funcionamiento se lo realizará a través del sistema nacional de datos públicos. La información biométrica se podrá intercambiar a través del sistema antedicho. Esta información podrá ser consultada por entidades externas tanto públicas como privadas para fines de validación o identificación de las personas*";
- Que,** el artículo 99 de la Ley Orgánica de Gestión de la Identidad y Datos Civiles , determina: "*Fijación de tarifas.- La Dirección General de Registro Civil, Identificación y Cedulación tendrá facultad para establecer y actualizar las tarifas por los servicios que presta, de conformidad con los requisitos y procedimientos establecidos en la normativa aplicable*";
- Que,** el numeral 2 del artículo 21 de la Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos dispone: "*Sin perjuicio de lo establecido en la Ley del Sistema Nacional de Registro de Datos Públicos, todas las entidades reguladas por esta Ley deberán utilizar obligatoriamente la información que reposa en:*  
*1. Sus propias bases de datos, alimentadas por información proporcionada por el propio ciudadano o por terceros, con anterioridad a la fecha del trámite; y*

2. El Sistema Nacional de Registro de Datos Públicos, para lo cual deberán cumplir con el trámite establecido en la ley que lo regula y demás normativa pertinente. Para el efecto, dichas entidades tienen la obligación de integrar los registros y bases de datos que estén a su cargo al Sistema Nacional de Registro de Datos Públicos en el plazo y con las formalidades requeridas por la Ley del Sistema Nacional de Registro de Datos Públicos y la entidad que presida el Sistema Nacional de Registro de Datos Públicos.";

**Que,** el artículo 19 de la Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos dispone: "La entidad rectora de la simplificación de trámites tendrá a su cargo la administración del registro único de trámites administrativos, el cual, deberá integrarse entre otros, al Sistema Nacional de Registro de Datos Públicos. La información que conste en el registro será generada por las entidades reguladas por esta Ley y consolidada en una base de datos nacional que incorpore en forma ordenada y periódica la información sobre los diferentes trámites administrativos, incluida la base normativa que sustenta el trámite, los requisitos que se deben cumplir, el tiempo aproximado que toma la gestión del trámite, el lugar en el que se lo debe realizar y cualquier otra información que sea dispuesta por la entidad rectora de la simplificación de trámites. Esta información deberá ser la misma que conste en la página web institucional de las entidades reguladas por esta Ley. (...)";

**Que,** el artículo 2 de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos establece: "(...) rige para las instituciones del sector público y privado que actualmente o en el futuro administren bases o registros públicos, sobre las personas naturales o jurídicas, sus bienes o patrimonio y para las usuarias o usuarios de los registros públicos";

**Que,** el artículo 4 de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos manda: "(...) Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos son responsables de la integridad, protección y control de los registros y bases de datos a su cargo (...);

**Que,** el artículo 6 de la Ley del Sistema Nacional de Registro de Datos Públicos, establece: "Son confidenciales los datos de carácter personal. El acceso a estos datos, solo será posible cuando quien los requiera se encuentre debidamente legitimado, conforme a los parámetros previstos en la Ley Orgánica de Protección de Datos Personales, su respectivo reglamento y demás normativa emitida por la Autoridad de Protección de Datos Personales. (...) La Directora o Director Nacional de Registros Públicos, definirá los demás datos que integran el sistema nacional y el tipo de reserva y accesibilidad";

**Que,** el artículo 13 de la Ley del Sistema Nacional de Registro de Datos Públicos, determina: "Son registros de datos públicos: el Registro Civil, de la Propiedad, Mercantil, Societario, Vehicular, de naves y aeronaves, patentes, de propiedad intelectual, registros de datos crediticios y los que en la actualidad o en el futuro determine la Dirección Nacional de Registros Públicos, en el marco de lo dispuesto por la Constitución de la República y las leyes vigentes.

Los Registros son dependencias públicas, desconcentrados, con autonomía registral y administrativa en los términos de la presente ley, y sujetos al control, auditoría y vigilancia de la Dirección Nacional de Registros Públicos en lo relativo al cumplimiento de políticas, resoluciones y disposiciones para la interconexión e interoperabilidad de bases

*de datos y de información pública, conforme se determine en el Reglamento que expida la Dirección Nacional.”;*

- Que,** el artículo 14 de la Ley del Sistema Nacional de Registro de Datos Públicos, determina: *“Los registros públicos y demás oficinas que manejen información relacionada con el objeto de esta Ley administrarán sus bases de datos en coordinación con la Dirección Nacional de Registros Públicos. Sus atribuciones, responsabilidades y funciones serán determinadas por la ley pertinente a cada registro y por el Reglamento a la presente ley.”;*
- Que,** el artículo 22 de la Ley del Sistema Nacional de Registro de Datos Públicos, determina: *“La Dirección Nacional de Registros Públicos se encargará de organizar un sistema de interconexión cruzado entre los registros público y privado que en la actualidad o en el futuro administren bases de datos públicos, de acuerdo a lo establecido en esta Ley y en su Reglamento.”;*
- Que,** el artículo 28 de la Ley del Sistema Nacional de Registros Públicos, señala: *“Créase el Sistema Nacional de Registros Públicos con la finalidad de proteger los derechos constituidos, los que se constituyan, modifiquen, extingan y publiquen por efectos de la inscripción de los hechos, actos y/o contratos determinados por la presente Ley y las leyes y normas de registros; y con el objeto de coordinar el intercambio de información de los registros públicos. En el caso de que entidades privadas posean información que por su naturaleza sea pública, serán incorporadas a este sistema. (...)”;*
- Que,** el artículo 29 de la Ley del Sistema Nacional de Registro de Datos Públicos, determina: *“El Sistema Nacional de Registros Públicos estará conformado por los registros: civil, de la propiedad, mercantil, societario, datos de conectividad electrónica, vehicular, de naves y aeronaves, patentes, de propiedad intelectual, registros de datos crediticios y todos los registros de datos de las instituciones públicas y privadas que mantuvieron y administren por disposición legal información registral de carácter público. Será presidido por la Directora o Director Nacional de Registros Públicos, con las facultades que se determinan en la presente Ley y su respectivo reglamento.”;*
- Que,** el numeral 1 y 4 del artículo 7 de la Ley Orgánica de Protección de Datos Personales manifiesta: *“Tratamiento legítimo de datos personas.- El tratamiento será legítimo y lícito si se cumple con alguna de las siguientes condiciones: (...) 1) Por consentimiento del titular para el tratamiento de sus datos personales, para una o varias finalidades específicas; 4) Que el tratamiento de datos personales se sustente en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, derivados de una competencia atribuida por una norma con rango de ley, sujeto al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta ley y a los criterios de legalidad, proporcionalidad y necesidad”;*
- Que,** el artículo 10 de la Ley Orgánica de Protección de Datos Personales determina: *“Principios.- Sin perjuicio de otros principios establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, la presente Ley se regirá por los principios de: (...) 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 esta Ley. El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. Para ello, habrá de considerarse el contexto en el que se recogieron los datos, la información facilitada al titular en ese proceso y, en particular, las expectativas razonables del titular basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los titulares del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista.”;*

**Que,** el artículo 25 de la Ley Orgánica de Protección de Datos Personales señala: *“Categorías especiales de datos personales. - Se considerarán categorías especiales de datos personales, los siguientes: a) Datos sensibles; b) Datos de niñas, niños y adolescentes; c) Datos de salud; y, d) Datos de personas con discapacidad y de sus sustitutos, relativos a la discapacidad.”;*

**Que,** el artículo 26 de la Ley Orgánica de Protección de Datos Personales dispone: *“Tratamiento de datos sensibles.- Queda prohibido el tratamiento de datos personales sensibles salvo que concurra alguna de las siguientes circunstancias: a) El titular haya dado su consentimiento explícito para el tratamiento de sus datos personales, especificándose claramente sus fines. b) El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular en el ámbito del Derecho laboral y de la seguridad y protección social. c) El tratamiento es necesario para proteger intereses vitales del titular o de otra persona natural, en el supuesto de que el titular no esté capacitado, física o jurídicamente, para dar su consentimiento. d) El tratamiento se refiere a datos personales que el titular ha hecho manifiestamente públicos. e) El tratamiento se lo realiza por orden de autoridad judicial. f) El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular. g) Cuando el tratamiento de los datos de salud se sujete a las disposiciones contenidas en la presente Ley.”;*

**Que,** el artículo 33 de la Ley Orgánica de Protección de Datos Personales determina: *“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”;*

**Que,** el artículo 34 de la Ley Orgánica de Protección de Datos Personales manifiesta: *“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. El encargado será responsable de las infracciones derivadas del incumplimiento de las condiciones de tratamiento de datos personales establecidas en la presente ley.”;*

**Que,** el artículo 35 de la Ley Orgánica de Protección de Datos Personales determina: *“No se considerará transferencia o comunicación cuando el acceso a datos personales por un tercero sea necesario para la prestación de un servicio al responsable del tratamiento de datos personales. El tercero que ha accedido a datos personales en estas condiciones debió hacerlo legítimamente. El tratamiento de datos personales realizado por terceros 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. El tercero será responsable de las infracciones derivadas del incumplimiento de las condiciones de tratamiento de datos personales establecidas en la presente ley.”;*

**Que,** el artículo 37 de la Ley Orgánica de Protección de Datos Personales manifiesta: *“El responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos. El responsable o encargado del tratamiento de datos personales, deberá implementar un proceso de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole, implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales. El responsable o encargado del*

*tratamiento de datos personales deberá evidenciar que las medidas adoptadas e implementadas mitiguen de forma adecuada los riesgos identificados. Entre otras medidas, se podrán incluir las siguientes (...) 4) Los responsables y encargados del tratamiento de datos personales, podrán acogerse a estándares internacionales para una adecuada gestión de riesgos enfocada a la protección de derechos y libertades, así como para la implementación y manejo de sistemas de seguridad de la información o a códigos de conducta reconocidos y autorizados por la Autoridad de Protección de Datos Personales”;*

**Que,** el artículo 38 de la Ley Orgánica de Protección de Datos Personales dispone las medidas de seguridad que deben implementar las entidades del sector público para el tratamiento de datos personales, de la siguiente manera: *“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 abarca y aplicará a todas las instituciones del sector público (...)”;*

**Que,** el artículo 47 de la Ley Orgánica de Protección de Datos Personales dispone las obligaciones que corresponden al responsable y encargado del tratamiento de datos personales, entre otras, lo siguiente: *“(...) 2) Aplicar e implementar requisitos y herramientas administrativas, técnicas, física, 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 (...); 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; (...) 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”;*

**Que,** los literales a) y h) del artículo 22 de la Ley Orgánica del Servicio Público, establecen entre los deberes de las y los servidores públicos los siguientes: *“a) Respetar, cumplir y hacer cumplir la Constitución de la República, leyes, reglamentos y más disposiciones expedidas de acuerdo con la Ley; (...) h) Ejercer sus funciones con lealtad institucional, rectitud y buena fe. Sus actos deberán ajustarse a los objetivos propios de la institución en la que se desempeñe y administrar los recursos públicos con apego a los principios de legalidad, eficacia, economía y eficiencia, rindiendo cuentas de su gestión (...)”;*

**Que,** la Carta Iberoamericana de Gobierno Electrónico aprobada por la IX Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado, celebrada en Chile el 1 de junio de 2007, en la sección 24, recomienda a los gobiernos tomar en consideración la importancia de la interoperabilidad de las comunicaciones y servicios así como disponer las medidas necesarias, para que todas las entidades públicas, cualquiera que sea su nivel y con independencia del respeto a su autonomía, establezcan sistemas que sean interoperables;

- Que,** el artículo 33 del Reglamento a la Ley Orgánica de Protección de Datos Personales determina: *“Obligaciones del responsable del tratamiento. - El responsable del tratamiento deberá, tanto en el momento de la determinación de los medios para el tratamiento como en el momento mismo del procesamiento de datos personales, aplicar medidas apropiadas que sean adecuadas para la observancia efectiva de los principios de protección de datos, así como de los derechos reconocidos en la Ley. Para ello, tendrá en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, las circunstancias y los fines del tratamiento, así como la probabilidad y la gravedad de los riesgos para los intereses de los titulares.”;*
- Que,** el artículo 48 del Reglamento a la Ley Orgánica de Protección de Datos Personales dispone: *“Delegado de protección de datos.- El delegado de protección de datos personales es la persona natural que se encarga principalmente de asesorar, velar y supervisar, de manera independiente, el cumplimiento de las obligaciones legales imputables al responsable y al encargado del tratamiento de datos personales. Podrá realizar otras actividades relacionadas con la protección de datos personales que le sean encomendadas por el responsable, siempre que no supongan o exijan del delegado una preparación diversa ni exista un conflicto con las responsabilidades previamente adquiridas. El delegado de protección de datos personales desempeñará sus funciones de manera profesional, con total independencia del responsable y del encargado del tratamiento de datos personales, quienes estarán obligados a facilitar la asistencia, recursos y elementos que les sea oportunamente requeridos para garantizar el cumplimiento de los deberes, funciones y responsabilidades a cargo del delegado. Sin perjuicio de lo que disponga la Ley y este Reglamento, corresponderá a la Autoridad de Protección de Datos Personales emitir la normativa que garantice la independencia del delegado de protección de datos personales en el desempeño de sus funciones en relación con el responsable y encargado.”;*
- Que,** mediante Decreto Ejecutivo Nro. 1384 de 13 de diciembre de 2012, publicado en el Segundo Suplemento del Registro Oficial Nro. 860 de 2 de enero de 2013, en el artículo 1, se dispone: *“Establecer como política pública, el desarrollo de la interoperabilidad gubernamental, que consiste en el esfuerzo mancomunado y permanente de todas las entidades de la Administración Central, dependiente e institucional para compartir e intercambiar entre ellas, por medio de las tecnologías de la información y comunicación, datos e información electrónicos que son necesarios en la prestación de los trámites y servicios ciudadanos que prestan las entidades, así como en la gestión interna e interinstitucional”;* por su parte, en su artículo 2, determina: *“La interoperabilidad gubernamental entre todas las Entidades de la Administración Pública Central, dependiente e institucional, será gestionada y normada por el conjunto de principios, políticas, procesos, procedimientos y estándares en los ámbitos operativo, conceptual y tecnológico que para el efecto dicte la Secretaría Nacional de la Administración Pública”;*
- Que,** mediante Acuerdo Nro. MINTEL-MINTEL-2024-0002, el Dr. César Antonio Martín Moreno, Ministro de Telecomunicaciones y de la Sociedad de la Información, resolvió designar al Lcdo. Ottón José Rivadeneira González como Director General de Registro Civil, Identificación y Cedulación, desde el 08 de febrero de 2024;

- Que,** mediante Resolución Nro. 031-DIGERCIC-CGAJ-DPyN-2025 de 23 de diciembre de 2025 se expidió el *“REGLAMENTO PARA EL ACCESO Y VERIFICACIÓN DE DATOS DEL ESTADO CIVIL E IDENTIDAD DE LAS PERSONAS, A TRAVÉS DE LOS SERVICIOS DE INTEROPERABILIDAD DE LA DIRECCIÓN GENERAL DE REGISTRO CIVIL, IDENTIFICACIÓN Y CEDULACIÓN”*, el cual en sus artículos 28, 29, 30 y 31 establece el proceso para la determinación de segmentación de campos para la prestación de servicios de interoperabilidad, bajo criterios de pertinencia, minimización y proporcionalidad, la cual debe ser elaborada por la Dirección de Servicios Electrónicos, la Dirección de Soporte e Interoperabilidad, el Oficial de Seguridad de la Información y el Delegado de Protección de Datos Personales, contar con la revisión y sustento legal de la Coordinación General de Asesoría Jurídica respecto a la competencia y finalidad del acceso, para posteriormente formalizarse a través de un informe conjunto de la Dirección de Servicios Electrónicos, Dirección de Soporte e Interoperabilidad, el Oficial de Seguridad de la Información y la Dirección de Asesoría Jurídica, que sirva de base técnica y legal para el Catálogo Sectorizado, cuya aprobación corresponde a la Máxima Autoridad o su delegado mediante el instrumento administrativo pertinente para su observancia obligatoria;
- Que,** mediante Memorando Nro. DIGERCIC-CGS-2026-0093-M de 05 de febrero de 2026, la Coordinación General de Servicios remitió a la Máxima Autoridad Institucional el *“INFORME TÉCNICO Y LEGAL DE CATÁLOGO SECTORIZADO DE INFORMACIÓN”*, de febrero de 2026; documento que, en cumplimiento de los artículos 30 y 31 de la Resolución Nro. 031-DIGERCIC-CGAJ-DPyN-2025, recomienda la aprobación e implementación del esquema de segmentación de información por sector como una medida esencial para garantizar el cumplimiento de la Ley Orgánica de Protección de Datos Personales y prevenir tratamientos excesivos o incompatibles con las finalidades legalmente establecidas;
- Que,** mediante Memorando Nro. DIGERCIC-DIGERCIC-2026-0057-M de 19 de febrero de 2026, la Dirección General dispone a la Coordinación General de Asesoría Jurídica: *“(…) la elaboración del instrumento administrativo correspondiente para la aprobación del catálogo sectorizado; tal cual lo contempla el Art. 31 de la RESOLUCIÓN Nro. 031-DIGERCIC-CGAJ-DPyN-2025”*;

En ejercicio de las atribuciones conferidas por el artículo 9, numeral 2 de la Ley Orgánica de Gestión de la Identidad y Datos Civiles,

**RESUELVE:**

**Artículo 1.- APROBAR EL CATÁLOGO SECTORIZADO DE INFORMACIÓN**, el cual establece los campos de datos autorizados, cantidades y restricciones para los sectores de Comercio, Educación, Financiero, Salud, Seguros, Servicios, Tecnología y Telecomunicaciones, destinados a la prestación del servicio de interoperabilidad de la Dirección General de Registro Civil, Identificación y Cedulación.

**Artículo 2.- ADOPTAR** el contenido íntegro del catálogo detallado en el informe técnico y legal de soporte, mismo que se adjunta a la presente Resolución como Anexo, formando parte integrante de la misma y de cumplimiento obligatorio para todas las entidades requirentes de información.

**Artículo 3.- DISPONER** a la Dirección de Servicios Electrónicos y a la Dirección de Soporte e Interoperabilidad, la implementación técnica de este catálogo en los servicios de interoperabilidad, asegurando que las entidades consumidoras accedan exclusivamente a los campos autorizados para su sector respectivo.

**Artículo 4.- ENCARGAR** a la Dirección de Servicios Electrónicos el monitoreo constante de las estadísticas de uso y la pertinencia de los campos, de conformidad con lo establecido en el Reglamento General a la Ley Orgánica de Protección de Datos Personales y la normativa interna institucional.

**DISPOSICIÓN REFORMATORIA**

**ÚNICA.- REFORMAR** la Disposición Final Segunda de la Resolución Nro. 031-DIGERCIC-CGAJ-DPyN-2025 de 23 de diciembre de 2025, por el siguiente texto:

*"SEGUNDA.- El presente Reglamento entrará en vigencia al día siguiente de la notificación de la publicación en la página web de la DIGERCIC, de los formularios correspondientes al catálogo de segmentación de la información para los servicios de interoperabilidad, a los que podrán acceder las empresas con base en la actividad económica que desarrollan."*

**DISPOSICIÓN FINAL**

**ÚNICA.-** Por medio de la Unidad de Gestión de Secretaría de la DIGERCIC notifíquese el contenido de la presente Resolución, a la Subdirección General, Coordinaciones Generales, Direcciones Nacionales, Coordinaciones Zonales, Dirección de Servicios Electrónicos, Dirección de Soporte e Interoperabilidad, Oficial de Seguridad de la Información y Delegado de Protección de Datos Personales; así como, el envío al Registro Oficial para la publicación correspondiente.




La presente Resolución entrará en vigencia a partir de su suscripción, sin perjuicio de su publicación en el Registro Oficial.

Dado en esta ciudad de Quito, Distrito Metropolitano, a los veinte (20) días del mes de febrero de 2026.



Mgs. Ottón José Rivadeneira González

**DIRECTOR GENERAL DE REGISTRO CIVIL, IDENTIFICACIÓN Y CEDULACIÓN**

Acción	Nombre /Cargo	Firma
Elaborado por:	Abg. Andrea Johanna Altamirano Bastidas <b>ANALISTA DE NORMATIVA 2</b>	
Revisado por:	Abg. Víctor Andrés Oquendo Torres <b>DIRECTOR DE PATROCINIO Y NORMATIVA</b>	
Autorizado por:	Abg. María José Rentería Landívar <b>COORDINADORA GENERAL DE ASESORÍA JURÍDICA</b>	

**Dirección General de Registro Civil,  
Identificación y Cedulación**

---

***INFORME TÉCNICO Y LEGAL DE CATÁLOGO  
SECTORIZADO DE INFORMACIÓN***








***Resolución Nro. 031-DIGERCIC-CGAJ-DPyN-2025***

---

*Coordinación General de Servicios  
Dirección de Servicios Electrónicos  
Febrero - 2026*

**INFORME TÉCNICO Y LEGAL DE SEGMENTACIÓN DE INFORMACIÓN**

Dirección General de Registro Civil,  
Identificación y Cedulación

	<b>NOMBRES, APELLIDOS Y CARGO</b>	<b>FIRMA</b>
<b>Elaborado</b>	Mgs. Marilyn Nathaly Monge Pinto <b>ANALISTA DE ORGANIZACIÓN, SEGUIMIENTO Y CONTROL DE PROCESOS DE SERVICIOS ELECTRÓNICOS 3</b>	 Firmado electrónicamente por: <b>MARILYN NATHALY MONGE PINTO</b> Validar únicamente con FirmaEC
	Ab. Ryna Alexandra Andrade Arciniegas <b>ANALISTA DE DICTÁMENES JURÍDICOS 3</b>	 Firmado electrónicamente por: <b>RYNA ALEXANDRA ANDRADE ARCINIEGAS</b> Validar únicamente con FirmaEC
<b>Revisado y Aprobado</b>	Ing, Diego German Arias Torres <b>DELEGADO DE PROTECCIÓN DE DATOS DE LA DIRECCIÓN GENERAL DE REGISTRO CIVIL, IDENTIFICACIÓN Y CEDULACIÓN</b>	 Firmado electrónicamente por: <b>DIEGO GERMAN ARIAS TORRES</b> Validar únicamente con FirmaEC
	Ing, Fausto Eduardo Tabango Canchigña <b>OFICIAL DE SEGURIDAD DE LA INFORMACIÓN</b>	 Firmado electrónicamente por: <b>FAUSTO EDUARDO TABANGO CANCHIGÑA</b> Validar únicamente con FirmaEC
	Mgs. Héctor Efrén Espinosa Villarreal <b>DIRECTOR DE SERVICIOS ELECTRÓNICOS</b>	 Firmado electrónicamente por: <b>HECTOR EFREN ESPINOSA VILLARREAL</b> Validar únicamente con FirmaEC
	Lcdo. Carlos Julio Villalba Flor <b>DIRECTOR DE SOPORTE E INTEROPERABILIDAD</b>	 Firmado electrónicamente por: <b>CARLOS JULIO VILLALBA FLOR</b> Validar únicamente con FirmaEC
	Mgs. Myriam Andrea Olivo Carrion <b>DIRECTORA DE ASESORÍA JURÍDICA</b>	 Firmado electrónicamente por: <b>MYRIAM ANDREA OLIVO CARRION</b> Validar únicamente con FirmaEC

**CONTENIDO**

- 1. ANTECEDENTES.....
- 2. MARCO NORMATIVO PERTINENTE .....

  - 2.1. Constitución de la República del Ecuador .....
  - 2.2. Ley Orgánica de Gestión de la Identidad y Datos Civiles .....
  - 2.3. Ley Orgánica del Registro Nacional de Datos Públicos .....
  - 2.4. Ley Orgánica de Protección de Datos Personales.....
  - 2.5. Reglamento a la Ley Orgánica de Protección de Datos Personales .....
  - 2.6. Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos .....

- 3. OBJETIVO.....
- 4. METODOLOGÍA DE TRABAJO .....

  - 4.1. Ámbito Económico .....

    - 4.1.1. Escenario de Riesgos Potencial de Impacto Económico .....

  - 4.2. Ámbito de la Segmentación .....

    - 4.2.1. Vista Materializada .....

- 5. Seguridad de la Información - Segmentación de los servicios de interoperabilidad. ....
- 6. ANÁLISIS JURÍDICO.....

  - 6.1. Consentimiento del titular.....
  - 6.2. Finalidad, minimización, pertinencia y proporcionalidad.....
  - 6.3. Segmentación .....
  - 6.4. Matriz por sector.....

- 7. Protección de datos personales (RAT) .....
- 8. CONCLUSIONES .....
- 9. RECOMENDACIONES .....

**ÍNDICE DE TABLAS**

Tabla 1: Contratos Suscritos WEB SERVICE .....

Tabla 2: Contratos Suscritos SNIC.....

Tabla 3: Transacciones y Valores Facturados Web Service .....

Tabla 4: Transacciones y Valores Facturados SNIC.....

Tabla 5: Valores estimados Web Service .....

Tabla 6: Valores proyectados SNIC.....

Tabla 7 Segmentos y campos por servicio.....

Tabla 8 Análisis Jurídico de campos a entregar .....

## 1. ANTECEDENTES

De conformidad con el Estatuto Orgánico por Procesos de la Dirección General de Registro Civil, Identificación y Cedulación (DIGERCIC), la Dirección de Servicios Electrónicos tiene como misión gestionar y proveer productos y servicios electrónicos de calidad, basados en datos registrales y de identidad, orientados a la simplificación de trámites para la ciudadanía y al fortalecimiento del gobierno electrónico.

Entre sus atribuciones y responsabilidades constan, entre otras, la gestión de servicios electrónicos, la administración de convenios y contratos, la promoción y distribución de dichos servicios, así como el seguimiento a la facturación y recaudación derivada de los servicios de interoperabilidad.

El 23 de diciembre de 2025, la máxima autoridad institucional expidió la Resolución Nro. 031-DIGERCIC-CGAJ-DPyN-2025, mediante la cual se aprobó el Reglamento para el Acceso y Verificación de Datos del Estado Civil e Identidad de las Personas a través de los Servicios de Interoperabilidad de la DIGERCIC. Dicho reglamento establece, en su Capítulo IV, la obligación de realizar una segmentación técnica y jurídica de la información, diferenciando los campos de datos por sector, bajo criterios de pertinencia, minimización y proporcionalidad.

En cumplimiento de lo dispuesto en los artículos 27 y 28 del referido Reglamento, la Dirección de Servicios Electrónicos, en coordinación con la Dirección de Soporte e Interoperabilidad, el Oficial de Seguridad de la Información y el Delegado de Protección de Datos Personales, elaboran en conjunto la propuesta técnica de segmentación de información, cuya revisión jurídica constituye el objeto del presente informe.

## 2. MARCO NORMATIVO PERTINENTE

### 2.1. Constitución de la República del Ecuador

*“Artículo 66.- Se reconoce y garantizará a las personas: (...) 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley (...);”*

### 2.2. Ley Orgánica de Gestión de la Identidad y Datos Civiles

*“Artículo 75.- Acceso y Protección de la información.- El acceso a los archivos físicos y electrónicos de los cuales es custodio la Dirección General de Registro Civil, Identificación y Cedulación que están sujetos al principio de confidencialidad y publicidad, derivada del derecho a la protección de datos de carácter personal, podrá darse únicamente por autorización de su titular, por el representante legal o por orden judicial”;*

### 2.3. Ley Orgánica del Registro Nacional de Datos Públicos

*“Artículo 6.- Accesibilidad y confidencialidad.- Son confidenciales los datos de carácter personal. El acceso a estos datos, solo será posible cuando quien los requiera se encuentre debidamente legitimado, conforme a los parámetros previstos en la Ley Orgánica de Protección de Datos Personales, su respectivo reglamento y demás normativa emitida por la Autoridad de Protección de Datos Personales.*

*Al amparo de esta Ley, para acceder a la información sobre el patrimonio de las personas cualquier solicitante deberá justificar y motivar su requerimiento, declarar el uso que hará del mismo y consignar sus datos básicos de identidad, tales como nombres y apellidos completos, número del documento de identidad o ciudadanía, dirección domiciliaria y los demás datos que mediante el respectivo reglamento se determinen.*

*Un uso distinto al declarado dará lugar a la determinación de responsabilidades, sin perjuicio de las acciones legales que el titular de la información pueda ejercer. La Directora o Director Nacional de Registros Públicos, definirá los demás datos que integran el sistema nacional y el tipo de reserva y accesibilidad.”*

#### 2.4. Ley Orgánica de Protección de Datos Personales

**“Artículo 7.- Tratamiento legítimo de datos personas (sic).**- El tratamiento será legítimo y lícito si se cumple con alguna de las siguientes condiciones:

- 1) Por consentimiento del titular para el tratamiento de sus datos personales, para una o varias finalidades específicas;
- 2) Que sea realizado por el responsable del tratamiento en cumplimiento de una obligación legal;
- 3) Que sea realizado por el responsable del tratamiento, por orden judicial, debiendo observarse los principios de la presente Ley;
- 4) Que el tratamiento de datos personales se sustente en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, derivados de una competencia atribuida por una norma con rango de ley, sujeto al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta Ley y a los criterios de legalidad, proporcionalidad y necesidad;
- 5) Para la ejecución de medidas precontractuales a petición del titular o para el cumplimiento de obligaciones contractuales perseguidas por el responsable del tratamiento de datos personales, encargado del tratamiento de datos personales o por un tercero legalmente habilitado;
- 6) Para proteger intereses vitales del interesado o de otra persona natural, como su vida, salud o integridad;
- 7) Para tratamiento de datos personales que consten en bases de datos de acceso público; u,
- 8) Para satisfacer un interés legítimo del responsable de tratamiento o de tercero, siempre que no prevalezca el interés o derechos fundamentales de los titulares al amparo de lo dispuesto en esta norma.”

**“Artículo 9.- Interés legítimo.** - Cuando el tratamiento de datos personales tiene como fundamento el interés legítimo: a) Únicamente podrán ser tratados los datos que sean estrictamente necesarios para la realización de la finalidad. b) El responsable debe garantizar que el tratamiento sea transparente para el titular. c) La Autoridad de Protección de Datos puede requerir al responsable un informe con (sic) de riesgo para la protección de datos en el cual se verificará si no hay amenazas concretas a las expectativas legítimas de los titulares y a sus derechos fundamentales.”

**“Artículo 10.- Principios.**- Sin perjuicio de otros principios establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, la presente Ley se regirá por los principios de:

(...) **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 esta Ley. El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. Para ello, habrá de considerarse el contexto en el que se recogieron los datos, la información facilitada al titular en ese proceso y, en particular, las expectativas razonables del titular basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los titulares del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista.”

**“Artículo 25.- Categorías especiales de datos personales.** - Se considerarán categorías especiales de datos personales, los siguientes:

- a) Datos sensibles;
- b) Datos de niñas, niños y adolescentes;
- c) Datos de salud; y,
- d) Datos de personas con discapacidad y de sus sustitutos, relativos a la discapacidad.”

**“Artículo 26.- Tratamiento de datos sensibles.**- Queda prohibido el tratamiento de datos personales sensibles salvo que concurra alguna de las siguientes circunstancias: a) El titular haya dado su consentimiento explícito para el tratamiento de sus datos personales, especificándose claramente sus fines. b) El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular en el ámbito del Derecho laboral y de la seguridad y protección social. c) El tratamiento es necesario para proteger intereses vitales del titular o de otra persona natural, en el supuesto de que el titular no esté capacitado, física o jurídicamente, para dar su consentimiento. d) El tratamiento se refiere a datos personales que el titular ha hecho manifiestamente públicos. e) El tratamiento se lo realiza por orden de autoridad judicial. f) El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger

los intereses y derechos fundamentales del titular. g) Cuando el tratamiento de los datos de salud se sujete a las disposiciones contenidas en la presente Ley.”

**“Artículo 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”;

## 2.5. Reglamento a la Ley Orgánica de Protección de Datos Personales

**“Artículo 33.- Obligaciones del responsable del tratamiento.-** El responsable del tratamiento deberá, tanto en el momento de la determinación de los medios para el tratamiento como en el momento mismo del procesamiento de datos personales, aplicar medidas apropiadas que sean adecuadas para la observancia efectiva de los principios de protección de datos, así como de los derechos reconocidos en la Ley. Para ello, tendrá en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, las circunstancias y los fines del tratamiento, así como la probabilidad y la gravedad de los riesgos para los intereses de los titulares.”

**“Artículo 48.- Delegado de protección de datos.-** El delegado de protección de datos personales es la persona natural que se encarga principalmente de asesorar, velar y supervisar, de manera independiente, el cumplimiento de las obligaciones legales imputables al responsable y al encargado del tratamiento de datos personales. Podrá realizar otras actividades relacionadas con la protección de datos personales que le sean encomendadas por el responsable, siempre que no supongan o exijan del delegado una preparación diversa ni exista un conflicto con las responsabilidades previamente adquiridas. El delegado de protección de datos personales desempeñará sus funciones de manera profesional, con total independencia del responsable y del encargado del tratamiento de datos personales, quienes estarán obligados a facilitar la asistencia, recursos y elementos que les sea oportunamente requeridos para garantizar el cumplimiento de los deberes, funciones y responsabilidades a cargo del delegado. Sin perjuicio de lo que disponga la Ley y este Reglamento, corresponderá a la Autoridad de Protección de Datos Personales emitir la normativa que garantice la independencia del delegado de protección de datos personales en el desempeño de sus funciones en relación con el responsable y encargado.”

## 2.6. Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos

**“Artículo 19.-** La entidad rectora de la simplificación de trámites tendrá a su cargo la administración del registro único de trámites administrativos, el cual, deberá integrarse entre otros, al Sistema Nacional de Registro de Datos Públicos.

La información que conste en el registro será generada por las entidades reguladas por esta Ley y consolidada en una base de datos nacional que incorpore en forma ordenada y periódica la información sobre los diferentes trámites administrativos, incluida la base normativa que sustenta el trámite, los requisitos que se deben cumplir, el tiempo aproximado que toma la gestión del trámite, el lugar en el que se lo debe realizar y cualquier otra información que sea dispuesta por la entidad rectora de la simplificación de trámites. Esta información deberá ser la misma que conste en la página web institucional de las entidades reguladas por esta Ley. (...);

## 3. OBJETIVO

Presentar el informe técnico y legal de segmentación de información, identificando los campos de datos que deben ser habilitados por sector para la prestación de los servicios de interoperabilidad de la DIGERCIC, con el fin de obtener la aprobación del Catálogo Sectorizado de Información, garantizando el cumplimiento de los principios de protección de datos personales.

#### 4. METODOLOGÍA DE TRABAJO

De acuerdo al artículo 27 de la Resolución Nro. 031-DIGERCIC-CGAJ-DPyN-2025, que indica que se proceda a recopilar y analizar la información relativa a la provisión de servicios de interoperabilidad ofertados por la DIGERCIC, con el objetivo de realizar la segmentación, a continuación, se realiza las siguientes actividades para la obtención de dicha información: Conforme a la matriz de control de la Dirección de Servicios Electrónicos, del periodo comprendido entre el 05 de junio de 2025 al 31 de diciembre de 2025 (**ANEXO 1**), donde se identifica que actualmente se encuentran 185 entidades suscritas y con servicio activo en Web Service y en 48 suscritas y con servicio activo en SNIC; dando un total de 233 entidades autorizadas. Empresas seleccionadas debido a que, a pesar de ser entidades usuarias de los servicios de interoperabilidad desde el 2024, cuentan con un contrato de prestación de servicios amparado en el Convenio de Cooperación Interinstitucional 002-2025 suscrito el 5 de junio de 2025, mismo que se encuentra vigente hasta el 5 de junio de 2028.

Para definir los sectores de las entidades seleccionadas se consultó la actividad económica de acuerdo al registro de su razón social (RUC) y la naturaleza jurídica, así como de su imagen empresarial mayormente conocida (**ANEXO 2**), se considera los siguientes 8 segmentos que se definen a continuación:

- **Comercio:** La entrega de datos a las entidades del sector comercio tiene como finalidad verificar de manera certera la identidad de una persona, prevenir suplantaciones y garantizar la seguridad jurídica en las transacciones y servicios que dichas entidades prestan.

Se ha considerado este segmento para contemplar las actividades económicas tales como: Venta al por mayor y menor de artículos.

- **Educación:** Se ha considerado este segmento para contemplar las actividades económicas tales como: Educación de tercer nivel, destinado a la formación básica en una disciplina o a la capacitación para el ejercicio de una profesión.
- **Financiera:** Se ha considerado este segmento para contemplar las actividades económicas tales como: Actividades de intermediación monetaria realizada por la banca comercial.
- **Salud:** Se ha considerado este segmento para contemplar las actividades económicas tales como: Actividades a corto y a largo plazo de los hospitales especializados, es decir, actividades médicas, de diagnóstico y de tratamiento.
- **Seguros:** Se ha considerado este segmento para contemplar las actividades económicas tales como: Servicios de seguro en general incluido la medicina pre pagado.
- **Servicios:** Se ha considerado este segmento para contemplar las actividades económicas tales como: Prestación de asesoramiento, consultorías y ayuda a las empresas y las administraciones públicas en materia de planificación, organización, eficiencia y control, información administrativa, etcétera.
- **Tecnología:** Se ha considerado este segmento para contemplar las actividades económicas tales como: Adaptación de programas informáticos a las necesidades de los clientes, es decir, modificación y configuración de una aplicación existente para que pueda funcionar adecuadamente con los sistemas de información de que dispone el cliente.
- **Telecomunicaciones:** Se ha considerado este segmento para contemplar las actividades económicas tales como: proveedores de servicio de internet, telefonía celular y venta al por mayor de teléfonos y equipos de comunicación relacionados.

De acuerdo a los segmentos considerados, las 233 entidades seleccionadas para el presente análisis, han sido agrupadas como se evidencian en los siguientes resultados cuantitativos por servicio:

Tabla 1: Contratos Suscritos WEB SERVICE

SERVICIO WEB	
SEGMENTO	CONTRATOS SUSCRITOS
COMERCIO	18
EDUCACIÓN	7
FINANCIERA	111
SALUD	6
SEGUROS	11
SERVICIOS	12
TECNOLOGÍA	19
TELECOMUNICACIONES	1
<b>TOTAL</b>	<b>185</b>

Fuente: Dirección de Servicios Electrónicos

De acuerdo al análisis realizado, en la tabla Nro. 1, se presenta la segmentación del servicio web (Demográfico y Demográfico más Biométrico), se determinó que existe un total de 185 empresas.

Tabla 2: Contratos Suscritos SNIC

SERVICIO SNIC	
SEGMENTO	CONTRATOS SUSCRITOS
COMERCIO	4
EDUCACIÓN	1
FINANCIERA	36
SALUD	0
SEGUROS	0
SERVICIOS	5
TECNOLOGÍA	1
TELECOMUNICACIONES	1
<b>TOTAL</b>	<b>48</b>

Fuente: Dirección de Servicios Electrónicos

De acuerdo al análisis realizado, en la tabla Nro. 2, se presenta la segmentación del servicio Sistema Nacional de Identificación Ciudadana, el cual se ha recabado información de un total de 48 empresas.

#### 4.1. Ámbito Económico

El Ámbito Económico comprende el análisis de la facturación y recaudación generada por la prestación de servicios electrónicos (Web Service y SNIC). Su propósito es evaluar el impacto financiero actual y proyectar posibles riesgos de reducción en los ingresos de la institución derivados de la implementación de la segmentación de datos por sector.

Tabla 3: Transacciones y Valores Facturados Web Service

SERVICIO WEB					
SEGMENTO	CONTRATOS SUSCRITOS	CONSULTAS REALIZADAS WS 2024	VALOR FACTURADO 2024	CONSULTAS REALIZADAS WS 2025	VALOR FACTURADO 2025
COMERCIO	18	2.619.097	\$674.895,30	914390	\$131.707,06
EDUCACIÓN	7	142.433	\$11.396,62	312394	\$24.992,84
FINANCIERA	111	15.687.444	\$3.906.467,86	16492862	\$4.259.355,18

<b>SALUD</b>	6	355.181	\$28.414,48	485153	\$38.812,24
<b>SEGUROS</b>	11	328.547	\$26.284,20	558528	\$44.683,56
<b>SERVICIOS</b>	12	187.039	\$25.256,70	324321	\$63.889,08
<b>TECNOLOGÍA</b>	19	3.253.581	\$879.885,90	4278422	\$1.051.253,46
<b>TELECOMUNICACIONES</b>	1	1.720.183	\$137.614,64	1633804	\$130.704,32
<b>TOTAL</b>	<b>185</b>	<b>24.293.505</b>	<b>\$5.690.215,70</b>	<b>24.999.874</b>	<b>\$5.745.397,74</b>

Fuente: Dirección de Servicios Electrónicos

Tabla 4: Transacciones y Valores Facturados SNIC

SERVICIO SNIC					
SEGMENTO	CONTRATOS SUSCRITOS	CONSULTAS REALIZADAS WS 2024	VALOR FACTURADO 2024	CONSULTAS REALIZADAS SNIC 2025	VALOR FACTURADO 2025
COMERCIO	4	46.355	\$13.276,05	61.608	\$17.665,35
EDUCACIÓN	1			2	0,60
FINANCIERA	36	329.200	\$95.092,65	304.791	\$87.306,45
SALUD	0				
SEGUROS	0				
SERVICIOS	5	7.413	\$1.973,70	12.678	\$3.384,90
TECNOLOGÍA	1	3	\$0,90	56	\$14,10
TELECOMUNICACIONES	1	74	\$20,40	290	\$73,95
<b>TOTAL</b>	<b>48</b>	<b>383.045</b>	<b>\$110.363,70</b>	<b>379.425</b>	<b>\$108.445,35</b>

Fuente: Dirección de Servicios Electrónicos

A continuación, en la tabla Nro. 3 y Nro.4 se presenta el reporte de transacciones y valores facturados y recaudados por los servicios de interoperabilidad; tablas que se establecieron conforme a los siguientes criterios:

- La segmentación detallada corresponde a las entidades autorizadas de la matriz de distribución de servicios electrónicos (**ANEXO 1**).
- Los valores presentados corresponden a la recaudación de enero a diciembre de los años 2024 y 2025 de las entidades autorizadas que se detallan en el (**ANEXO 1**).
- Como se puede evidenciar en el servicio Web, la facturación y recaudación en el año 2024 ha sido de \$ 5.690.215,70 y en el 2025 de \$ 5.745.397,74, dando un total de \$11.435.613,44 dólares.
- Como se puede evidenciar en el servicio SNIC, la facturación y recaudación en el año 2024 ha sido de 110.363,70 y en el 2025 de \$ 108.445,35, dando un total de \$218,809,05 dólares.

#### 4.1.1. Escenario de Riesgos Potencial de Impacto Económico

Este apartado analiza el impacto económico conforme a la implementación de la segmentación de los campos por sector, se basa en la proyección de una posible disminución en el consumo de los servicios de interoperabilidad (Web Service y SNIC) por parte de las entidades autorizadas, lo que resultaría la baja en la recaudación de la Institución, tal como se evidencia en la tabla Nro. 5:

Tabla 5: Valores estimados Web Service

SERVICIO WEB							
SEGMENTO	2024	2025	10 %	20 %	30 %	40 %	50 %
COMERCIO	\$674.895,30	\$131.707,06	\$118.536,35	\$105.365,65	\$92.194,94	\$79.024,24	\$65.853,53
EDUCACIÓN	\$11.396,62	\$24.992,84	\$22.493,56	\$19.994,27	\$17.494,99	\$14.995,70	\$12.496,42

FINANCIERA	\$3.906.467,86	\$4.259.355,18	\$3.833.419,66	\$3.407.484,14	\$2.981.548,63	\$2.555.613,11	\$2.129.677,59
SALUD	\$28.414,48	\$38.812,24	\$34.931,02	\$31.049,79	\$27.168,57	\$23.287,34	\$19.406,12
SEGUROS	\$26.284,20	\$44.683,56	\$40.215,20	\$35.746,85	\$31.278,49	\$26.810,14	\$22.341,78
SERVICIOS	\$25.256,70	\$63.889,08	\$57.500,17	\$51.111,26	\$44.722,36	\$38.333,45	\$31.944,54
TECNOLOGÍA	\$879.885,90	\$1.051.253,46	\$946.128,11	\$841.002,77	\$735.877,42	\$630.752,08	\$525.626,73
TELECOMUNICACIONES	\$137.614,64	\$130.704,32	\$117.633,89	\$104.563,46	\$91.493,02	\$78.422,59	\$65.352,16
<b>TOTAL</b>	<b>\$ 5.690.215,70</b>	<b>\$ 5.745.397,74</b>	<b>\$5.170.857,97</b>	<b>\$4.596.318,19</b>	<b>\$4.021.778,42</b>	<b>\$3.447.238,64</b>	<b>\$2.872.698,87</b>

Fuente: Dirección de Servicios Electrónicos

El servicio de interoperabilidad a través de Web Service es el principal ingreso de la Dirección de Electrónicos, mostrando una estabilidad operativa, en el cual se mantiene los campos solicitados por las entidades autorizadas (20 campos).

Como se puede observar la recaudación total del Servicio Web pasó de \$5.690.215,70 en el año 2024 a \$5.745.397,74 para el año 2025, lo que representa un incremento neto de \$55.182,04, se considera que, al realizar un análisis de proyección, la implementación de la segmentación de campos por sector, existe un riesgo a la baja en un total de facturación estimado de \$ 2.872.698,87 anual.

Cabe mencionar que el sector Financiero cuenta con los valores más altos en la facturación, este segmento es el más crítico, aportando \$4.259.355,18 en el año 2025 (aproximadamente el 74% del total facturado).

Sector Tecnología: Presentó el crecimiento más dinámico, aumentando su facturación de \$879.885,90 a \$1.051.253,46, respectivamente por año, en este sector.

Sector Telecomunicaciones: Se observa una caída en la facturación de este sector, bajando de \$ 137.614,64 en el año 2024 a \$ 130.704,32 para el año 2025.

A continuación, en la tabla Nro. 6 se va a realizar la presentación del análisis de riesgo de baja de recaudación en caso de que se presente la implementación de la segmentación de la información y esto provoque una reducción de consumo.

Tabla 6: Valores proyectados SNIC

SERVICIO SNIC							
SEGMENTO	2024	2025	10 %	20 %	30 %	40 %	50 %
COMERCIO	\$ 13.276,05	\$ 17.665,35	\$15.898,80	\$ 14.308,00	\$ 12.878,05	\$11.590,20	\$ 10.431,20
EDUCACIÓN		\$ 0,60	\$ 0,60	\$ 0,60	\$ 0,60	\$ 0,60	\$ 0,30
FINANCIERA	\$ 95.092,65	\$ 87.306,45	\$ 78.575,80	\$ 70.718,00	\$ 63.646,40	\$ 57.281,75	\$ 51.553,60
SALUD							
SEGUROS							
SERVICIOS	\$ 1.973,70	\$ 3.384,90	\$ 3.046,40	\$ 2.741,80	\$2.467,60	\$ 2.220,80	\$ 1.998,75
TECNOLOGÍA	\$ 0,90	\$ 14,10	\$ 12,80	\$ 11,40	\$ 10,28	\$ 9,25	\$ 8,20
TELECOMUNICACIONES	\$ 20,40	\$ 73,95	\$ 66,55	\$ 59,90	\$ 53,90	\$ 48,50	\$ 43,70
<b>TOTAL</b>	<b>\$110.363,70</b>	<b>\$108.445,35</b>	<b>\$ 97.600,95</b>	<b>\$ 87.839,70</b>	<b>\$ 79.056,83</b>	<b>\$ 71.151,10</b>	<b>\$ 64.035,75</b>

Fuente: Dirección de Servicios Electrónicos

El Sistema Nacional de Identificación Ciudadana (SNIC) es una plataforma de consulta de datos de identidad (Demográfico y Demográfico más Biométrico) que permite la consulta de la información ciudadana, para prevenir posibles actos de suplantación de identidad.

Aunque cuenta con menos entidades suscritas que el Web Service (48 frente a 185), es una herramienta clave para sectores que requieren validaciones específicas de identidad, y un sistema obligatorio para las Notarías a nivel nacional por su ente rector al Consejo Nacional de la Judicatura.

Generalmente se aplica la tarifa base de \$0.30 (treinta centavos de dólar) por consulta, en el año 2025 registró 379,425 consultas, con una recaudación de \$108,445.35, considerando la segmentación de campos por sector, se puede evidenciar que existe una reducción con base a un análisis de riesgos por la visibilidad de los datos, es decir, que existiría una reducción de un total de facturación estimada de \$64.035,75.

#### 4.2. Ámbito de la Segmentación

Los criterios utilizados para este análisis son los siguientes:

- Las entidades pueden contar con datos básicos con los cuales puedan validar la identidad de las personas y minimizar riesgos de suplantación, falsificación de documentos y discriminación, tanto para la entidad autorizada como para el ciudadano.
- Las entidades pueden validar la información que presentan los ciudadanos con la que presenta la DIGERCIC como la encargada de la administración y provisión de los servicios relacionado con la gestión de la identidad y de los hechos y actos relativos al estado civil de las personas.
- Las entidades tienen la alternativa de minimizar el riesgo de fraude de identidad que las expondría a potenciales estafas económicas.

En este sentido, se detalla a continuación los campos de datos propuestos por cada segmento, a fin de permitir la validación de información por parte de las entidades:

##### 1. COMERCIO (10 campos propuestos)

1. **Condición de cedulado:** Permite confirmar que la persona cuenta con un documento de identidad vigente y válida, lo que constituye el primer filtro de autenticidad.
2. **Número de cédula:** Es el identificador único de la persona dentro del sistema nacional de identificación y permite la consulta y verificación inequívoca del ciudadano.
3. **Apellidos y nombres:** Facilitan la comparación y validación de la información declarada por el usuario frente a los registros oficiales.
4. **Fecha de nacimiento:** Contribuye a diferenciar homónimos y permite validar requisitos de edad para determinados actos o servicios reservados para personas mayores de edad.
5. **Nacionalidad:** Permite verificar la condición jurídica de la persona y su elegibilidad para acceder a ciertos servicios o productos.
6. **Estado civil:** Permite validar actos que generan efectos legales o patrimoniales, especialmente en operaciones financieras o contractuales.
7. **Nombre del cónyuge:** Resultan relevantes para validar actos que generan efectos legales o patrimoniales, especialmente en operaciones financieras o contractuales.
8. **Instrucción:** En determinados servicios, permite cumplir requisitos normativos o políticas internas de evaluación de clientes.
9. **Foto:** Es un elemento clave para la verificación biométrica y la comparación visual de la identidad, reduciendo riesgos de fraude o suplantación.
10. **Firma:** Permite contrastar la identidad en procesos que requieren aceptación expresa, autorización o suscripción de documentos.

Por ello, la segmentación por sector comercio debe asegurar que solo se habiliten los campos indispensables según el tipo de servicio, operación o transacción que la entidad requiera realizar, evitando accesos innecesarios a información personal.

##### 2. EDUCACIÓN (7 campos propuestos)

1. **Condición de cedulado:** Permite identificar a los estudiantes o personal educativo, garantizando que la información se asigne a la persona correcta.
2. **Número de cédula:** Son fundamentales para identificar de forma única a los estudiantes o personal educativo, garantizando que la información se asigne a la persona correcta.

3. **Apellidos y nombres:** Permiten la correcta identificación del estudiante, del personal o de los tutores, y son esenciales para la correcta administración académica.
4. **Fecha de nacimiento:** Es importante para verificar la edad del estudiante, cumpliendo con requisitos de admisión o de asignación de cursos según el nivel educativo.
5. **Nacionalidad:** Permiten determinar la elegibilidad para ciertos programas, becas o beneficios específicos.
6. **Instrucción:** Puede ser requerido para validar el nivel de educación, a fin de poder acceder a distintas ofertas educativas.
7. **Estado civil:** Pueden ser relevantes para determinar la elegibilidad para ciertos programas, becas o beneficios específicos.

### 3. FINANCIERO (10 campos propuestos)

1. **Condición de cedulado:** Son esenciales para identificar de manera única al cliente, evitando fraudes y asegurando que la información se asigne a la persona correcta.
2. **Número de cédula:** Son esenciales para identificar de manera única al cliente, evitando fraudes y asegurando que la información se asigne a la persona correcta.
3. **Apellidos y nombres:** Permiten la identificación precisa del cliente, lo cual es vital para la apertura de cuentas, la emisión de tarjetas y la realización de operaciones financieras.
4. **Fecha de nacimiento:** Ayuda a verificar la mayoría de edad del cliente, cumpliendo con requisitos legales para la apertura de cuentas y otros productos financieros.
5. **Nacionalidad:** Es clave para determinar la residencia y la elegibilidad para ciertos productos o servicios, así como para cumplir con normativas internacionales contra el lavado de dinero.
6. **Estado civil:** Es relevante para evaluar ciertos productos financieros, como créditos hipotecarios o seguros, ya que el estado civil puede influir en la capacidad crediticia y en los riesgos asociados, en consideración a si existe una sociedad conyugal legal establecida.
7. **Nombre del cónyuge:** Es relevante cuando las operaciones financieras generan efectos patrimoniales compartidos, especialmente en: Créditos hipotecarios o prendarios, apertura de cuentas conjuntas, otorgamiento de garantías o avales, permite verificar el régimen económico matrimonial, prevenir conflictos legales y garantizar la validez de los actos contractuales.
8. **Instrucción:** Puede ser requerido para: Evaluaciones de perfil del cliente, cumplimiento de políticas internas de conocimiento del cliente (KYC), Determinar la comprensión del cliente respecto a productos financieros complejos.
9. **Foto:** Es un elemento clave para la verificación biométrica y visual de la identidad del cliente, permitiendo comparar al titular con el documento de identidad y para reducir el riesgo de suplantación de identidad.
10. **Firma:** Es indispensable para validar la aceptación expresa de contratos, autorizaciones y consentimientos, verificar la identidad en la suscripción de documentos físicos o electrónicos.

La recopilación de estos datos en el sector financiero no solo cumple con requisitos legales y normativos, sino que también protege tanto a la entidad como al cliente de posibles riesgos y fraudes.

### 4. SALUD (8 campos propuestos)

1. **Condición de cedulado:** Permite verificar que la persona está debidamente identificada, evitando suplantación de identidad o errores en la asignación de atenciones médicas.
2. **Número de cédula:** Permiten identificar de manera única al paciente, evitando confusiones o errores en el historial médico.
3. **Apellidos y nombres:** Son esenciales para la correcta identificación del paciente y para evitar errores de atención o de prescripción.
4. **Fecha de nacimiento:** Es fundamental para determinar la edad del paciente, lo cual influye en el diagnóstico, el tratamiento y las dosis de medicamentos.
5. **Nacionalidad:** Puede ser relevante para acceder a ciertos servicios de salud, cumplir con regulaciones específicas, o para la atención de pacientes extranjeros.
6. **Sexo:** Es importante para personalizar la atención médica, ya que ciertos tratamientos, diagnósticos y medicamentos dependen del género del paciente.
7. **Foto:** Ayuda a verificar visualmente la identidad del paciente, evitando errores en la atención y reduciendo riesgos de suplantación.
8. **Firma:** Es esencial para el consentimiento informado, la aceptación de tratamientos, procedimientos y la autorización de uso de datos médicos.

**5. SEGUROS (11 campos propuestos)**

1. **Condición de cedulado:** Permite verificar que la persona cuenta con un documento de identidad válido y vigente, requisito indispensable para la contratación de una póliza y el ejercicio de derechos y obligaciones contractuales.
2. **Número de cédula:** Es el identificador único del asegurado, beneficiario o contratante, lo que permite evitar duplicidades o registros erróneos, prevenir suplantación de identidad, garantizar la trazabilidad de la información durante la vigencia de la póliza
3. **Apellidos y nombres:** Permiten identificar de forma precisa a la persona asegurada y contrastar la información declarada con los registros oficiales, asegurando la correcta emisión de pólizas y el pago de siniestros.
4. **Fecha de nacimiento:** Es fundamental para determinar la edad del asegurado, calcular primas y coberturas, verificar elegibilidad y vigencia de ciertos seguros (vida, salud, accidentes)
5. **Nacionalidad:** Permite establecer la condición jurídica del asegurado y verificar restricciones, coberturas o requisitos específicos según la normativa aplicable o el tipo de seguro contratado.
6. **Estado civil:** Resulta relevante para identificar beneficiarios legales, evaluar riesgos patrimoniales o familiares, Gestionar seguros con efectos económicos compartidos (vida, desgravamen, exequias)
7. **Nombre del cónyuge:** Es relevante cuando las operaciones financieras generan efectos patrimoniales compartidos, especialmente en: prestación de servicios diferenciados para la sociedad conyugal legalmente establecido.
8. **Instrucción:** Puede ser utilizado para evaluar el perfil del asegurado, garantizar la adecuada comprensión de las condiciones de la póliza
9. **Sexo:** Es un dato relevante para determinar coberturas específicas.
10. **Foto:** Constituye un elemento clave para verificación visual y biométrica de la identidad, prevención de fraudes y suplantación, fortalecer controles en procesos presenciales y no presenciales
11. **Firma:** Es indispensable para formalizar la aceptación de la póliza y sus condiciones, otorgar consentimiento expreso, garantizar la validez legal y probatoria de los contratos de seguro.

**6. SERVICIOS (9 campos propuestos)**

1. **Condición de cedulado:** Permite verificar si la cédula se encuentra vigente, válida o anulada, asegurando que la identidad del ciudadano sea auténtica antes de brindar el servicio.
2. **Número de cédula:** Es el identificador único del ciudadano. Se utiliza para localizar su registro y evitar duplicidades o suplantación de identidad.
3. **Apellidos y nombres:** Permiten la identificación nominal del ciudadano y la concordancia con el número de cédula en registros administrativos y contractuales.
4. **Fecha de nacimiento:** Sirve para verificar edad, validar capacidad legal y diferenciar a personas con nombres similares.
5. **Nacionalidad:** Determina el estatus legal del ciudadano y su elegibilidad para acceder a determinados servicios o beneficios.
6. **Estado civil:** Se utiliza cuando el servicio tiene implicaciones legales, patrimoniales o familiares (por ejemplo, contratos, beneficiarios, autorizaciones).
7. **Nombre del cónyuge:** Aplica únicamente cuando el servicio requiere verificación de vínculos familiares o conyugales, como en trámites administrativos específicos.
8. **Foto:** Permite la validación biométrica visual, reduciendo riesgos de fraude o suplantación durante la atención presencial o digital.
9. **Firma:** Se emplea para la aceptación expresa de términos, respaldo de trámites, contratos o autorizaciones, otorgando validez jurídica.

**7. TECNOLOGÍA (7 campos propuestos)**

1. **Condición de cedulado:** Permite verificar que la persona se encuentra oficialmente registrada y cuenta con un documento de identidad válido, lo cual es fundamental para el acceso seguro a plataformas tecnológicas y servicios digitales.
2. **Número de cédula:** Funciona como identificador único para autenticar al usuario, evitar duplicidades, prevenir fraudes y garantizar la trazabilidad de las transacciones o accesos a sistemas.

3. **Apellidos y Nombres:** Facilitan la identificación nominal del usuario dentro de los sistemas tecnológicos, permitiendo una correcta asociación de cuentas, perfiles y registros.
4. **Fecha de nacimiento:** Se utiliza para validar la identidad, verificar mayoría de edad cuando el servicio lo exige y aplicar controles de acceso según rangos etarios.
5. **Nacionalidad:** Permite cumplir con requisitos legales, normativos o contractuales, así como aplicar restricciones o habilitaciones según el país de origen.
6. **Foto:** Sirve como mecanismo adicional de autenticación y validación visual de identidad, especialmente en procesos de registro, enrolamiento o control de acceso digital.
7. **Firma:** Se emplea para la validación de consentimientos, aceptación de términos y condiciones, y suscripción de documentos electrónicos, otorgando validez jurídica a los procesos digitales.

**8. TELECOMUNICACIONES (7 campos propuestos)**

1. **Condición de cedulado:** Asegura que el usuario está debidamente registrado y cuenta con una identidad verificada, lo cual es esencial para la provisión de servicios de telecomunicaciones y la protección contra fraudes.
2. **Número de cédula:** Sirve como identificador único para autenticar a los usuarios y gestionar las cuentas de manera precisa.
3. **Apellidos y nombres:** Permiten la correcta identificación de los usuarios, facilitando la personalización de los servicios y la gestión de cuentas.
4. **Fecha de nacimiento:** Es utilizada para verificar la edad del usuario, aplicar restricciones de edad si es necesario, y adaptar los servicios a las necesidades del usuario.
5. **Nacionalidad:** Permite cumplir con normativas regulatorias y adaptar los servicios según el país de origen del usuario.
6. **Foto:** Se emplea para la verificación visual de identidad, especialmente en procesos de activación o control de acceso.
7. **Firma:** Es crucial para la validación de consentimientos, la aceptación de términos y condiciones, y la firma electrónica de contratos o servicios.

En el (ANEXO 3) podemos evidenciar los campos propuestos a entregar por segmento y su justificación:

La entrega no segmentada de estos datos a las entidades autorizadas y requirentes incrementa significativamente los riesgos legales, operativos, de seguridad tanto para los ciudadanos como para las entidades autorizadas.

En este contexto, la segmentación por sector permite habilitar únicamente los campos de información estrictamente necesarios, como se indica en la tabla Nro 7.

Tabla 7 Segmentos y campos por servicio

SEGMENTO	SERVICIO WEB		SERVICIO SNIC	
	DETALLE	NRO. DE CAMPOS	DETALLE	NRO. DE CAMPOS
COMERCIO	1. Condición de cedulado 2. Número de cédula 3. Apellidos y nombres 4. Fecha de nacimiento 5. Nacionalidad 6. Estado civil 7. Nombre del cónyuge 8. Instrucción 9. Foto 10. Firma	10	1. Condición de cedulado 2. Número único de identificación 3. Nombre del Ciudadano 4. Fecha de nacimiento 5. Nacionalidad 6. Estado civil 7. Cónyuge 8. Instrucción 9. Foto 10. Firma	10
EDUCACIÓN	1. Condición de cedulado 2. Número de cédula 3. Apellidos y nombres 4. Fecha de nacimiento 5. Nacionalidad 6. Instrucción 7. Estado civil	7	1. Condición de cedulado 2. Número único de identificación 3. Nombre del Ciudadano 4. Fecha de nacimiento 5. Nacionalidad 6. Instrucción 7. Estado civil	7

<b>FINANCIERA</b>	1. Condición de cedulado 2. Número de cédula 3. Apellidos y nombres 4. Fecha de nacimiento 5. Nacionalidad 6. Estado civil 7. Nombre del cónyuge 8. Instrucción 9. Foto 10. Firma	10	1. Condición de cedulado 2. Número único de identificación 3. Apellidos y nombres 4. Fecha de nacimiento 5. Nacionalidad 6. Estado civil 7. Cónyuge 8. Instrucción 9. Foto 10. Firma	10
<b>SALUD</b>	1. Condición de cedulado 2. Número de cédula 3. Apellidos y nombres 4. Fecha de nacimiento 5. Nacionalidad 6. Sexo 7. Foto 8. Firma	8	1. Condición de cedulado 2. Número único de identificación 3. Nombre del Ciudadano 4. Fecha de nacimiento 5. Nacionalidad 6. Sexo 7. Foto 8. Firma	8
<b>SEGUROS</b>	1. Condición de cedulado 2. Número de cédula 3. Apellidos y nombres 4. Fecha de nacimiento 5. Nacionalidad 6. Estado civil 7. Nombre del cónyuge 8. Instrucción 9. Sexo 10. Foto 11. Firma	11	1. Condición de cedulado 2. Número único de identificación 3. Nombre del Ciudadano 4. Fecha de nacimiento 5. Nacionalidad 6. Estado civil 7. Cónyuge 8. Instrucción 9. Sexo 10. Foto 11. Firma	11
<b>SERVICIOS</b>	1. Condición de cedulado 2. Número de cédula 3. Apellidos y nombres 4. Fecha de nacimiento 5. Nacionalidad 6. Estado civil 7. Nombre del cónyuge 8. Foto 9. Firma	9	1. Condición de cedulado 2. Número único de identificación 3. Nombre del Ciudadano 4. Fecha de nacimiento 5. Nacionalidad 6. Estado civil 7. Cónyuge 8. Foto 9. Firma	9
<b>TECNOLOGÍA</b>	1. Condición de cedulado 2. Número de cédula 3. Apellidos y Nombres 4. Fecha de nacimiento 5. Nacionalidad 6. Foto 7. Firma	7	1. Condición de cedulado 2. Número único de identificación 3. Nombre del Ciudadano 4. Fecha de nacimiento 5. Nacionalidad 6. Foto 7. Firma	7
<b>TELECOMUNICACIONES</b>	1. Condición de cedulado 2. Número de cédula 3. Apellidos y Nombres 4. Fecha de nacimiento 5. Nacionalidad 6. Foto 7. Firma	7	1. Condición de cedulado 2. Número único de identificación 3. Nombre del Ciudadano 4. Fecha de nacimiento 5. Nacionalidad 6. Foto 7. Firma	7

Fuente: Dirección de Servicios Electrónicos

#### 4.2.1. Vista Materializada

En lo referido a la segmentación para el servicio de Vista Materializada se diferencia de los servicios de Web Service y SNIC por estar orientado estrictamente para las instituciones públicas, servicio masivo requerido para el funcionamiento de las instituciones. Debido a que este servicio requiere la integración de datos para procesos del Estado, no es factible aplicar una segmentación de campos, ya que esto comprometería la eficacia de los trámites ciudadanos y el cumplimiento de los procesos establecidos en cada una de las instituciones.

Dado que las instituciones públicas operan bajo mandato de ley, requieren acceso a la totalidad de los datos pertinentes para ejercer sus competencias legales.

## 5. Seguridad de la Información - Segmentación de los servicios de interoperabilidad.

Los servicios de interoperabilidad que distribuye la Dirección General de Registro Civil, Identificación y Cedulación y que constan en la taxonomía de servicios, se encuentran sustentados como servicios que permiten prevenir la suplantación de identidad de los ciudadanos ecuatorianos o extranjeros, para acceder a estos servicios las instituciones deben tener un instrumento legal vigente por los servicios (Demográfico y/o Biométrico), Servicio del Sistema Nacional de Identificación Ciudadana (SNIC), Vista Materializada (Transferencia de Registros), con entidades del sector público, privado y notarías; estos servicios exigen controles de seguridad robustos que permitan prevenir la suplantación de identidad y proteger a ciudadanos ecuatorianos y extranjeros del mal uso de su información.

La verificación, segmentación de campos establecida por la Dirección de Servicios Electrónicos para los servicios de interoperabilidad, debe disponer un esquema integral basado en gobierno electrónico, controles técnicos, controles organizativos, cumplimiento normativo y monitoreo continuo, que de preferencia deben estar alineados con el Esquema Gubernamental de Seguridad de la Información (EGSI).

Considerando las atribuciones y responsabilidades establecidas en la normativa vigente para el Oficial de Seguridad de la Información es necesario señalar en este documento las siguientes generalidades para los servicios de interoperabilidad: La unidades administrativas de la DIGERCIC en relación a sus atribuciones y competencias establecidas en el Estatuto Orgánico por Procesos; son los responsables en disponer actualizado el modelo y arquitectura de interoperabilidad en el que se incluyan los componentes tecnológicos y organizacionales de la distribución de los servicios de interoperabilidad de la DIGERCIC, utilizando los principios de protección de datos personales (Privacy by Design), con el propósito para evitar riesgos en los derechos de los titulares de la información de acuerdo a los fines del tratamiento, así también para que los datos personales no sean por defecto accesibles a personas no autorizadas.

Los controles técnicos y organizacionales que pueden ser considerados y documentados para la distribución de los servicios de interoperabilidad pueden ser:

- Integración segura
- Cifrado de datos
- Parametrización de atributos
- API seguro para la consulta de la información
- Autenticación y autorización (MFA)
- Pruebas de vida en la identificación
- Protección en la integridad de datos
- Correlación de enlaces (IP)
- Monitoreo, registro y respuesta de incidentes
- Auditorías periódicas
- Capacitación y Concientización
- Gestión y evaluación de los riesgos en los servicios de interoperabilidad

## 6. ANÁLISIS JURÍDICO

### 6.1. Consentimiento del titular

El numeral 7.1 de la Ley Orgánica de Protección de Datos Personales establece al consentimiento del titular como una base legitimadora para el tratamiento de datos personales, siempre que este se otorgue para una o varias finalidades específicas. Este consentimiento constituye una manifestación expresa de la autodeterminación informativa y se vincula directamente con el derecho constitucional a la protección de datos personales, en cuanto permite al titular decidir de manera libre e informada sobre el uso de su información personal. En consecuencia, no se trata de una autorización general o indeterminada, sino de una habilitación jurídica limitada por la finalidad concreta previamente informada.

Desde una perspectiva jurídica, el consentimiento válido exige que sea previo, libre, específico, informado e inequívoco. La exigencia de finalidades específicas impide la utilización de cláusulas genéricas o abiertas que pretendan habilitar tratamientos futuros o incompatibles con la finalidad original. Asimismo, el consentimiento no exime al responsable del cumplimiento de los principios de finalidad, pertinencia, minimización y proporcionalidad, de modo que aun existiendo aceptación expresa del titular, el tratamiento puede resultar ilícito si los datos recolectados son excesivos o innecesarios respecto del fin declarado.

El consentimiento otorgado en virtud del numeral 7.1 es esencialmente revocable, sin necesidad de motivación y sin efectos retroactivos, lo que refuerza su carácter dinámico y controlable. Para el tratamiento de datos se debe acreditar no solo la obtención del consentimiento, sino su correspondencia exacta con la finalidad declarada. Cualquier ampliación, reutilización o cambio de finalidad sin nuevo consentimiento constituye una infracción a la Ley Orgánica de Protección de Datos Personales y una vulneración al derecho fundamental de protección de datos.

### **6.2. Finalidad, minimización, pertinencia y proporcionalidad.**

En adición a lo señalado en párrafos anteriores cabe señalar que conforme a la Ley Orgánica de Protección de Datos Personales, el principio de finalidad constituye el eje estructural que condiciona la aplicación de la pertinencia y minimización del tratamiento de datos personales. La exigencia de que las finalidades sean determinadas, explícitas, legítimas y previamente comunicadas al titular impide que se recolecte o conserve información bajo supuestos amplios o indeterminados. Desde esta perspectiva, la minimización opera como una consecuencia directa de la finalidad declarada, pues únicamente pueden tratarse aquellos datos que guarden una relación funcional y necesaria con el propósito específico informado, quedando proscrito cualquier tratamiento ulterior que no sea compatible con las expectativas razonables del titular y con el contexto en el que los datos fueron originalmente recopilados.

En este mismo sentido, el principio de pertinencia y minimización impone un deber jurídico activo de selección y restricción de los datos personales tratados. No basta con que el dato resulte útil o conveniente; es indispensable que sea estrictamente necesario para cumplir la finalidad legítima del tratamiento. Este principio exige una evaluación previa y continua que descarte la recolección masiva o preventiva de información, así como la conservación de datos redundantes o carentes de relevancia. En términos jurídicos, la carga de demostrar la necesidad de cada categoría de datos recae en quien va a tratar los datos, de modo que la ausencia de una justificación objetiva convierte el tratamiento en ilegítimo, aun cuando exista consentimiento del titular.

Finalmente, el principio de proporcionalidad del tratamiento actúa como un mecanismo de control material que integra y refuerza la finalidad y la minimización. La proporcionalidad exige que el tratamiento sea adecuado, necesario y no excesivo, atendiendo tanto a la finalidad perseguida como a la naturaleza de los datos, en especial cuando se trata de categorías especiales. Esto implica que se debe optar siempre por el medio menos invasivo disponible para alcanzar la finalidad declarada y evaluar las consecuencias del tratamiento sobre los derechos del titular. En este sentido, la recolección o el uso de datos que excedan lo estrictamente necesario, aun cuando estén relacionados con la finalidad, constituye una vulneración a la Ley y al derecho fundamental a la protección de datos personales.

### **6.3. Segmentación**

Desde una perspectiva jurídico-técnica, una propuesta de segmentación de la información por sectores resulta fundamental para garantizar el cumplimiento efectivo de los principios de finalidad, pertinencia, minimización y proporcionalidad previstos en la Ley Orgánica de Protección de Datos Personales. La interoperabilidad entre entidades públicas o privadas no constituye, por sí sola, una habilitación general para el intercambio irrestricto de datos, sino un mecanismo instrumental que debe limitarse estrictamente a los datos indispensables para la prestación del servicio o el ejercicio de competencias legalmente atribuidas. La segmentación permite identificar, de manera previa y objetiva, qué categorías de datos personales son necesarias en función del sector y del trámite específico, evitando accesos amplios, indeterminados o preventivos que carezcan de sustento legal.

Asimismo, la identificación clara de los datos efectivamente utilizados en cada sector fortalece la trazabilidad, la rendición de cuentas y la responsabilidad proactiva del responsable del tratamiento. Una segmentación técnica adecuadamente documentada permite demostrar que el intercambio de información responde a una necesidad concreta y verificable, reduce el riesgo de tratamientos excesivos o incompatibles y facilita el control administrativo y constitucional del uso de datos personales. En este sentido, la interoperabilidad basada en segmentación no solo optimiza la eficiencia del servicio, sino que constituye una garantía jurídica para la protección de los derechos de los titulares y un elemento clave para la defensa institucional frente a eventuales observaciones de la autoridad de control o acciones constitucionales.

#### 6.4. Matriz por sector

Desde una perspectiva jurídica y conforme a la Ley Orgánica de Protección de Datos Personales, no resulta jurídicamente viable ni técnicamente correcto elaborar una justificación general y abstracta por cada campo de datos personales, debido a que la legitimidad de su tratamiento depende necesariamente del contexto concreto, de la finalidad específica, del tipo de trámite o servicio, y de la base legal aplicable en cada caso. La normativa exige un análisis casuístico que permita verificar la necesidad, pertinencia y proporcionalidad del dato en relación con la finalidad perseguida, lo cual impide validaciones genéricas o apriorísticas. Cualquier intento de justificar de forma uniforme el tratamiento de determinados campos de información desconoce el carácter dinámico del principio de minimización y trasladaría el riesgo jurídico al responsable del tratamiento, al no poder demostrar la necesidad efectiva del dato en un escenario específico.

No obstante de lo anterior, resulta jurídicamente admisible establecer parámetros generales orientadores por sector, que permitan delimitar criterios mínimos de análisis sin sustituir la evaluación individual técnica que se deberá realizar en cada caso concreto. Sobre lo cual es importante enfatizar que quien solicite la elaboración de un contrato de interoperabilidad deberá justificar de manera clara y precisa los datos solicitados; tomando especial relevancia lo señalado en el artículo 66 numeral 19 de la Constitución de la República del Ecuador que establece: “(...) *La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley (...)*”; lo que obliga a la DIGERCIC establecer un adecuado proceso de control, que permita verificar el cumplimiento estricto de lo que determina la Carta Magna.

### 7. Protección de datos personales (RAT)

Las entidades autorizadas estarán obligadas a proceder a la supresión, anonimización o devolución de los datos personales, quedando prohibida su conservación indefinida o reutilización no autorizada, en relación a los derechos de acceso, rectificación, actualización, eliminación, oposición, portabilidad y limitación del tratamiento, conforme a la Ley Orgánica de Protección de Datos Personales, manteniéndose la responsabilidad primaria como responsable del tratamiento, mismas que deberán ser canalizadas a través de los mecanismos institucionales definidos por la DIGERCIC.

En base al análisis jurídico-técnico de riesgos sobre los tratamientos de datos personales, el cual cumple con los estándares de evaluación previa exigidos por la normativa vigente, se encuentran sujetos a controles de roles, perfiles, trazabilidad y auditoría, garantizando el uso exclusivo para competencias legalmente atribuidas.

Tabla 8 Análisis Jurídico de campos a entregar

SEGMENTO	NRO. DE CAMPOS	CONSIDERACIÓN GENERAL	LISTADO DE CAMPOS (WEB SERVICE)	LISTADO DE CAMPOS (SNIC)	Parámetros de pertinencia
COMERCIO	10	los datos deben vincularse estrictamente a la transacción comercial	<ol style="list-style-type: none"> <li>1. Condición de cedulado</li> <li>2. Número de cédula</li> <li>3. Apellidos y nombres</li> <li>4. Fecha de nacimiento</li> <li>5. Nacionalidad</li> <li>6. Estado civil</li> <li>7. Nombre del cónyuge</li> <li>8. Instrucción</li> <li>9. Foto</li> <li>10. Firma</li> </ol>	<ol style="list-style-type: none"> <li>1. Condición de cedulado</li> <li>2. Número único de identificación</li> <li>3. Nombre del Ciudadano</li> <li>4. Fecha de nacimiento</li> <li>5. Nacionalidad</li> <li>6. Estado civil</li> <li>7. Cónyuge</li> <li>8. Instrucción</li> <li>9. Foto</li> <li>10. Firma</li> </ol>	<ul style="list-style-type: none"> <li>• Datos pertinentes:                             <ul style="list-style-type: none"> <li>Identificación básica</li> <li>Datos de contacto</li> <li>Información de facturación</li> </ul> </li> <li>• Datos no pertinentes:                             <ul style="list-style-type: none"> <li>Información financiera detallada (si no hay crédito)</li> </ul> </li> </ul>
EDUCACIÓN	7	los datos deben vincularse a la gestión académica y protección reforzada de estudiantes	<ol style="list-style-type: none"> <li>1. Condición de cedulado</li> <li>2. Número de cédula</li> <li>3. Apellidos y nombres</li> <li>4. Fecha de nacimiento</li> <li>5. Nacionalidad</li> <li>6. Instrucción</li> <li>7. Estado civil</li> </ol>	<ol style="list-style-type: none"> <li>1. Condición de cedulado</li> <li>2. Número único de identificación</li> <li>3. Nombre del Ciudadano</li> <li>4. Fecha de nacimiento</li> <li>5. Nacionalidad</li> <li>6. Instrucción</li> <li>7. Estado civil</li> </ol>	<ul style="list-style-type: none"> <li>• Datos pertinentes:                             <ul style="list-style-type: none"> <li>Identificación del estudiante</li> <li>Historial académico</li> <li>Información socioeconómica (si involucra financiamiento)</li> <li>Datos no pertinentes:                                     <ul style="list-style-type: none"> <li>Información médica no relacionada</li> <li>Datos familiares sin justificación</li> </ul> </li> </ul> </li> </ul>
FINANCIERA	10	Los datos deben vincularse a obligaciones legales y análisis de riesgo financieros	<ol style="list-style-type: none"> <li>1. Condición de cedulado</li> <li>2. Número de cédula</li> <li>3. Apellidos y nombres</li> <li>4. Fecha de nacimiento</li> <li>5. Nacionalidad</li> <li>6. Estado civil</li> <li>7. Nombre del cónyuge</li> <li>8. Instrucción</li> <li>9. Foto</li> <li>10. Firma</li> </ol>	<ol style="list-style-type: none"> <li>1. Condición de cedulado</li> <li>2. Número único de identificación</li> <li>3. Apellidos y nombres</li> <li>4. Fecha de nacimiento</li> <li>5. Nacionalidad</li> <li>6. Estado civil</li> <li>7. Cónyuge</li> <li>8. Instrucción</li> <li>9. Foto</li> <li>10. Firma</li> </ol>	<ul style="list-style-type: none"> <li>• Datos pertinentes:                             <ul style="list-style-type: none"> <li>Identificación</li> <li>Información financiera necesaria</li> <li>Historial crediticio relevante</li> <li>Datos no pertinentes:                                     <ul style="list-style-type: none"> <li>Preferencias personales</li> <li>Información patrimonial no vinculada al producto</li> </ul> </li> </ul> </li> </ul>
SALUD	8	Datos vinculados a necesidades clínicas y de salud de las personas. Merece especial atención	<ol style="list-style-type: none"> <li>1. Condición de cedulado</li> <li>2. Número de cédula</li> <li>3. Apellidos y nombres</li> <li>4. Fecha de nacimiento</li> <li>5. Nacionalidad</li> <li>6. Sexo</li> <li>7. Foto</li> <li>8. Firma</li> </ol>	<ol style="list-style-type: none"> <li>1. Condición de cedulado</li> <li>2. Número único de identificación</li> <li>3. Nombre del Ciudadano</li> <li>4. Fecha de nacimiento</li> <li>5. Nacionalidad</li> <li>6. Sexo</li> <li>7. Foto</li> <li>8. Firma</li> </ol>	<ul style="list-style-type: none"> <li>• Historia clínica relevante</li> <li>• Datos biométricos necesarios</li> <li>• Información genética solo cuando sea imprescindible</li> <li>• Datos no pertinentes:                             <ul style="list-style-type: none"> <li>Datos familiares irrelevantes</li> <li>Datos médicos históricos sin utilidad clínica</li> </ul> </li> </ul>
SEGUROS	11	Datos vinculados a los riesgos del asegurado.	<ol style="list-style-type: none"> <li>1. Condición de cedulado</li> <li>2. Número de cédula</li> <li>3. Apellidos y nombres</li> <li>4. Fecha de nacimiento</li> </ol>	<ol style="list-style-type: none"> <li>1. Condición de cedulado</li> <li>2. Número único de identificación</li> <li>3. Nombre del Ciudadano</li> <li>4. Fecha de nacimiento</li> </ol>	<ul style="list-style-type: none"> <li>• Datos pertinentes:                             <ul style="list-style-type: none"> <li>Información médica vinculada al riesgo asegurado</li> </ul> </li> </ul>

			<p>5. Nacionalidad 6. Estado civil 7. Nombre del cónyuge 8. Instrucción 9. Sexo 10. Foto 11. Firma</p>	<p>5. Nacionalidad 6. Estado civil 7. Cónyuge 8. Instrucción 9. Sexo 10. Foto 11. Firma</p>	<ul style="list-style-type: none"> <li>● Datos del bien asegurado</li> <li>● Historial de siniestros</li> <li>● Datos no pertinentes:</li> <li>● Información médica general no relacionada</li> <li>● Datos financieros excesivos</li> <li>● Información de terceros sin vínculo contractual</li> </ul>
<b>SERVICIOS</b>	9	Los datos deben estar vinculados a prestación eficiente y legalmente atribuida del servicio.	<p>1. Condición de cedulado 2. Número de cédula 3. Apellidos y nombres 4. Fecha de nacimiento 5. Nacionalidad 6. Estado civil 7. Nombre del cónyuge 8. Foto 9. Firma</p>	<p>1. Condición de cedulado 2. Número único de identificación 3. Nombre del Ciudadano 4. Fecha de nacimiento 5. Nacionalidad 6. Estado civil 7. Cónyuge 8. Foto 9. Firma</p>	<p>Datos pertinentes:</p> <ul style="list-style-type: none"> <li>● Identificación del usuario</li> <li>● Datos de contacto</li> <li>● Información técnica necesaria (consumo, ubicación general)</li> <li>● Datos no pertinentes:</li> <li>● Geolocalización precisa permanente</li> <li>● Información familiar o patrimonial</li> </ul>
<b>TECNOLOGÍA</b>	7	Los datos deben vincularse a la actividad del sector	<p>1. Condición de cedulado 2. Número de cédula 3. Apellidos y Nombres 4. Fecha de nacimiento 5. Nacionalidad 6. Foto 7. Firma</p>	<p>1. Condición de cedulado 2. Número único de identificación 3. Nombre del Ciudadano 4. Fecha de nacimiento 5. Nacionalidad 6. Foto 7. Firma</p>	<p>Datos pertinentes:</p> <ul style="list-style-type: none"> <li>● Identificadores técnicos</li> <li>● Datos de uso anonimizados</li> <li>● Información estrictamente funcional</li> <li>● Datos no pertinentes:</li> <li>● Datos personales completos cuando basta anonimización</li> <li>● Recolección masiva sin finalidad clara</li> </ul>
<b>TELECOMUNICACIONES</b>	7	Los datos deben vincularse a la provisión de servicios de telecomunicaciones.	<p>1. Condición de cedulado 2. Número de cédula 3. Apellidos y Nombres 4. Fecha de nacimiento 5. Nacionalidad 6. Foto 7. Firma</p>	<p>1. Condición de cedulado 2. Número único de identificación 3. Nombre del Ciudadano 4. Fecha de nacimiento 5. Nacionalidad 6. Foto 7. Firma</p>	<p>Datos pertinentes:</p> <ul style="list-style-type: none"> <li>● Identificación del abonado</li> <li>● Datos técnicos de conexión</li> <li>● Información de facturación</li> <li>● Datos no pertinentes:</li> <li>● Contenido de comunicaciones</li> <li>● Metadatos históricos extensos sin causa legal</li> <li>● Geolocalización continua sin necesidad técnica</li> </ul>

Fuente: Dirección de Asesoría Jurídica

**Aspectos relevantes para considerar:**

1. Como se señaló en párrafos precedentes, se deberá realizar el análisis técnico respectivo en cada caso.
2. Los sectores que han sido técnicamente determinados, son referenciales, no son excluyentes entre sí.
3. Deberá considerarse los datos sensibles para cuando existan solicitudes al respecto.
4. Si un dato no es estrictamente necesario para cumplir la finalidad declarada o la obligación legal, no debe ser recolectado ni tratado.
5. Los datos deben ser adecuados, pertinentes y no excesivos.
6. El solicitante de los datos debe demostrar por qué cada dato es necesario.

**8. CONCLUSIONES**

La DIGERCIC se encuentra legalmente habilitada para entregar información de identidad a entidades usuarias de los servicios de interoperabilidad; sin embargo, dicha entrega no es irrestricta, sino que debe sujetarse obligatoriamente a los principios de: Finalidad legítima, necesidad, minimización de datos, y proporcionalidad.

Para todos los sectores es obligación aplicar segmentación de campos, minimización de datos y control de accesos diferenciados por sector, conforme a criterios de pertinencia y proporcionalidad.

De acuerdo a la propuesta realizada por las áreas técnicas se considera que, la DIGERCIC es la entidad pública legalmente competente para administrar el sistema nacional de identificación civil, lo que incluye la custodia, actualización, validación y certificación de los datos de identidad de los ciudadanos por lo que se encuentra jurídicamente habilitada para entregar información de identidad a entidades pertenecientes a determinados sectores económicos, siempre que dicha entrega se considere lo siguiente:

1. Se observe estrictamente lo que establece el Artículo 66 numeral 19 de la Constitución de la República del Ecuador, que señala: *"(...) La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley (...)"*.
2. Se realice dentro de su competencia legal como entidad rectora del sistema nacional de identificación;
3. Se responda a una finalidad específica, legítima y jurídicamente verificable, vinculada a la prestación de servicios esenciales o al cumplimiento de obligaciones legales;
4. Se observe estrictamente el principio de minimización, mediante la segmentación de los campos de información por sector económico; se ejecute bajo esquemas de interoperabilidad controlada, con medidas técnicas, jurídicas y organizativas de seguridad y trazabilidad.
5. De conformidad con la Ley Orgánica de Protección de Datos Personales, el tratamiento de datos debe limitarse estrictamente a aquellos adecuados, pertinentes y necesarios para cumplir la finalidad previamente definida.
6. Se habiliten únicamente los campos estrictamente necesarios por sector.
7. Se restrinja el acceso a datos sensibles a los casos debidamente justificados.
8. Se mantenga control contractual, técnico y administrativo del uso de la información.
9. La entrega de datos que no guarden relación directa con la finalidad específica del sector constituye un exceso en el tratamiento y vulnera el derecho constitucional a la protección de datos personales.
10. Conforme al muestreo de la Dirección de Servicios Electrónicos, se ha evidenciado 8 segmentos (Comercio, Educación, Financiera, Salud, Seguros, Servicios, Tecnología y Telecomunicaciones) con un número de campos de consulta que varía entre 7 y 11, adaptándose estrictamente a las necesidades operativas de cada uno.
11. La Dirección de Servicios Electrónicos determina que la regularización y segmentación de campos para el sector público se abordará mediante un instrumento técnico independiente, por la naturaleza específica de los servicios de consumo masivo (Vista Materializada), garantizando que la segmentación no comprometa las funciones legales y competencias institucionales del Estado.
12. La distribución de los servicios de interoperabilidad permiten prevenir el fraude, suplantación de identidad y verificación de identidad, además en la segmentación efectuada por la Dirección de Servicios Electrónicos tiene la finalidad de interoperar los datos estrictamente necesarios para prevenir el mal uso de los datos personales de los ciudadanos por las entidades que tienen un instrumento legal vigente y deben disponer de un esquema integral basado en gobierno electrónico, controles técnicos, controles organizativos, cumplimiento normativo y monitoreo continuo, alineado con estándares establecidos en el Esquema Gubernamental de Seguridad de la Información (EGSI).

**9. RECOMENDACIONES**

- Una vez que se ha ejecutado la propuesta técnica de segmentación de campos de manera oportuna para asegurar que las entidades accedan a la información indispensable para los fines pertinentes, se recomienda aprobar el Catálogo Sectorizado de información, el mismo que establece los campos autorizados por cada sector y las restricciones correspondientes.
- Conforme al Artículo 27 del Reglamento, la Dirección de Servicios Electrónicos debe mantener un análisis constante de las estadísticas de uso para identificar si los campos asignados siguen siendo necesarios o si requieren ajustes futuros.
- Aprobar e implementar el esquema de segmentación de información por sector, su incorporación en el Registro de Actividades de Tratamiento y su aplicación vinculante en todos los instrumentos jurídicos de interoperabilidad, como medida esencial para garantizar el cumplimiento de la Ley Orgánica de Protección de Datos Personales y prevenir tratamientos excesivos o incompatibles con las finalidades legalmente establecidas.
- La Coordinación General de Servicios deberá gestionar la elaboración de la Evaluación de Impacto en Protección de Datos (EIPD) en el caso de existir modificaciones sustanciales en los tratamientos.