

Resolución Nro. 007-NG-DINARP-2025

Magister. Paolo Sebastián Grijalva González
DIRECTOR NACIONAL DE REGISTROS PÚBLICOS (E)

CONSIDERANDO:

Que, el artículo 18 de la Constitución de la República del Ecuador, determina: *“Todas las personas en forma individual o colectiva tienen derecho a: 1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior. 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. En caso de violación a los derechos humanos, ninguna entidad pública negará la información.”;*

Que, el numeral 19 del artículo 66 de la Norma Suprema establece: *“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 226 de la Constitución de la República del Ecuador dispone: *“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 Carta Magna dispone: *“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 1 de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, determina: *“La presente ley crea y regula el sistema de Registros Públicos y su acceso, en entidades públicas o privadas que administren dichas bases o registros. El objeto de la ley es: garantizar la seguridad jurídica, organizar, regular, sistematizar e interconectar la información, así como: la eficacia y eficiencia de su manejo, su publicidad, transparencia, acceso e implementación de nuevas tecnologías.”;*

Que, el artículo 2 de la norma ibidem, prescribe: *“La presente Ley rige para las instituciones del sector público y privado que actualmente o en el futuro administren bases o registros de datos públicos, sobre las personas naturales o jurídicas, sus bienes o patrimonio y para las usuarias o usuarios de los registros públicos.”*;

Que, el inciso primero del artículo 4 de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, dispone: *“Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. (...)”*;

Que, el artículo 6 de la norma referida, 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. 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.”*;

Que, el artículo 22 de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, indica: *“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 con lo establecido, en esta Ley y en su Reglamento.”*;

Que, el artículo 28 de la norma ibidem, estipula: *“Créase el Sistema Nacional de Registros Públicos con la finalidad de proteger los derechos constituidos, los que se constituyan, modifiquen, extingan y publiciten 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 de datos 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 Orgánica del Sistema Nacional de Registro de Datos Públicos, prescribe: *“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 mantuvieren 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 artículo 31 de la norma ibidem, determina: *“La Dirección Nacional de Registros Públicos tendrá las siguientes atribuciones y facultades: 1. Presidir el Sistema Nacional de Registros Públicos, cumpliendo y haciendo cumplir sus finalidades y objetivos; 2. Dictar las resoluciones y normas necesarias para la organización y funcionamiento del sistema; (...) 5. Consolidar, estandarizar y administrar la base única de datos de todos los Registros Públicos, para lo cual todos los integrantes del Sistema están obligados a proporcionar información digitalizada de sus archivos, actualizada y de forma simultánea conforme ésta se produzca; (...) 14. Controlar y supervisar que las entidades pertenecientes al Sistema Nacional de Registros Públicos incorporen mecanismos de protección de datos personales, así como dar cumplimiento a las disposiciones establecidas en la Ley Orgánica de Protección de Datos Personales, su reglamento de aplicación y demás normativa que la Autoridad de Protección de Datos Personales dicte para el efecto (...).”*;

Que, el numeral 2 del artículo 21 de la Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos, señala: *“Sin perjuicio de lo establecido en la Ley del Sistema Nacional de Registros Públicos, todas las entidades reguladas por esta Ley deberán utilizar obligatoriamente la información que reposa en: [...] 2. El Sistema Nacional de Registros 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 Registros Públicos en el plazo y con las formalidades requeridas por la Ley del Sistema Nacional de Registros Públicos y la entidad que presida el Sistema Nacional de Registros Públicos.”*;

Que, el artículo 7 de la norma ibidem, estipula: *“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.”;

Que, el artículo 25 de la Ley Orgánica de Protección de Datos Personales, señala: “*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, prescribe: “*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 4 numeral 6 de la Ley Orgánica de Transparencia y Acceso a la Información Pública, define a la información pública como: “*Todo tipo de dato en documentos de cualquier formato, final o preparatoria, haya sido o no generada por el sujeto obligado, que se encuentre en poder de los sujetos obligados por esta Ley,*

contenidos, creados u obtenidos por ellos, que se encuentren bajo su responsabilidad y custodia o que se hayan producido con recursos del Estado.”;

Que, el artículo 2 del Reglamento a la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, establece que el Sistema Nacional de Registros Públicos está conformado por: *“(…) las instituciones públicas y privadas determinadas en la Ley Orgánica del Sistema Nacional de Registros Públicos, y las que en el futuro determine, mediante resolución, el Director Nacional de Registros Públicos, en ejercicio de sus competencias.”;*

Que, el artículo 9 de la misma norma, establece: *“Sin perjuicio de las competencias que ejercen los entes de control, definidos en la Constitución de la República, la Dirección Nacional de Registros de Públicos es el órgano de regulación, control, auditoría y vigilancia de todos los integrantes del Sistema Nacional de Registros Públicos en torno a la interoperabilidad de datos.*

La regulación, control, auditoría y vigilancia comprenden todas las acciones necesarias para garantizar la disponibilidad del servicio. Las decisiones administrativas internas de cada ente registral corresponden exclusivamente a sus autoridades, pero la Dirección Nacional de Registros Públicos arbitrará las medidas que sean del caso cuando perjudiquen la disponibilidad de los servicios”;

Que, el artículo 13 de la norma ibidem, determina: *“La Dirección Nacional de Registros Públicos, de conformidad con la ley, expedirá las normas técnicas que contengan los estándares, mecanismos y herramientas para precautelar la seguridad, custodia y conservación de la información accesible y confidencial. La integridad y protección de los registros de datos públicos es responsabilidad de las instituciones del sector público y privado, a través de sus representantes legales y las personas naturales que directamente los administren.”;*

Que, el artículo 14 del Reglamento a la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, señala: *“La Dirección Nacional de Registros Públicos realizará las acciones necesarias para que todas las bases de datos de los registros públicos que integran el Sistema Nacional de Registros Públicos, interoperen entre sí, con las respectivas seguridades tecnológicas, con la que brindará los servicios tanto a la ciudadanía como a las instituciones. La Dirección Nacional de Registros Públicos podrá conceder acceso al servicio de interoperabilidad a instituciones privadas, siempre que cumplan con las disposiciones de la Ley Orgánica de Protección de Datos Personales, su reglamento de aplicación, los requisitos que mediante resolución determine la Dirección Nacional de Registros Públicos; y, cancelen los valores por el acceso a dicha información.”*

Que, el artículo 8 de la Resolución Nro. 003-NG-DINARP-2025, indica: *“Las entidades que soliciten el acceso a los servicios del Sistema Nacional de Registros Públicos, deberán obligatoriamente previo a la oficialización del requerimiento de acceso, contar con una revisión previa por parte de las unidades administrativas de la Dirección Nacional de Registros Públicos que intervengan en los procesos.”*

Que, la disposición transitoria tercera de la Resolución Nro. 003-NG-DINARP-2025, determina: *“En el término de treinta (30) días contados a partir de la publicación de la presente resolución en el Registro Oficial, la Dirección de Normativa elaborará la normativa que establezca el procedimiento de revisiones previas determinadas en la presente resolución.”*

Que, mediante Acuerdo Ministerial Nro. MINTEL-MINTEL-2025-0008 de 07 de mayo del 2025, el doctor César Antonio Martín Moreno, Ministro de Telecomunicaciones y de la Sociedad de la Información, acuerda: *“(…) Designar al magister Paolo Sebastián Grijalva Gonzalez, Subdirector Nacional, como Director Nacional de Registros Públicos Encargado, a partir del 8 de diciembre de 2025, funcionario quién ejercerá las competencias y atribuciones previstas en la Ley Orgánica del Sistema Nacional de Registros Públicos y demás normativa aplicable. (...)”;*

Por las consideraciones expuestas, en ejercicio de las facultades que le otorga la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, el Director Nacional de Registros Públicos Encargado,

RESUELVE:

REGULAR EL PROCEDIMIENTO DE REVISIONES PREVIAS A LOS REQUERIMIENTOS DE CONSUMO EN EL SISTEMA NACIONAL DE REGISTROS PÚBLICOS

CAPÍTULO I GENERALIDADES

Artículo 1.- Objeto. - La presente norma tiene por objeto establecer el procedimiento para llevar a cabo las revisiones previas a requerimientos de consumo solicitados por las entidades incorporadas al Sistema Nacional de Registros Públicos.

Artículo 2.- Ámbito de aplicación. - La presente norma es de cumplimiento obligatorio para la Dirección Nacional de Registros Públicos y para todas las entidades públicas y privadas incorporadas al Sistema Nacional de Registros Públicos que requieran acceso a los servicios proporcionados por esta Institución.

Artículo 3.- Glosario de Términos. - Para efectos de aplicación de la presente norma, se establecen las siguientes definiciones:

Campo(s) de dato(s): Categoría o nomenclatura de la unidad que contiene datos o información, sea esta de carácter accesible o confidencial, que forma parte de un conjunto de datos o base de datos provistos por las fuentes de información que integran el Sistema Nacional de Registros Públicos.

Catálogo: Listado de campos de datos integrados en el Sistema Nacional de Registros Públicos, por parte de las entidades que forman parte del referido sistema.

Dato accesible: Información que no tiene el carácter de confidencial conforme al ordenamiento jurídico.

Dato confidencial: Son datos que contienen características especialmente sensibles y que requieren de protección adicional debido a su naturaleza o importancia que podrían encontrarse dentro de categorías especiales de datos personales o podrían consistir en datos que, combinados con otros, podrían conllevar a la identificación de un individuo.

Enrolamiento: Procedimiento formal mediante el cual una entidad se registra en el Sistema Nacional de Registros Públicos, conforme a los requisitos establecidos en la normativa legal vigente. Este proceso habilita a la entidad a solicitar el acceso a los servicios del Sistema y a utilizar los servicios que ofrece la Dirección Nacional de Registros Públicos, en función de sus necesidades específicas, garantizando la formalización y validación en dicho sistema.

Entidad: Toda institución pública o privada que forma parte del Sistema Nacional de Registros Públicos de acuerdo con lo establecido en la ley.

Fuente: Es el conjunto ordenado de información, dispuesto en una tabla o base de datos integrado al Sistema Nacional de Registros Públicos proporcionado por el ente registral.

Infodigital: es una herramienta tecnológica de verificación que permite a las instituciones públicas realizar la respectiva validación de la información pública que se encuentra integrada al Sistema Nacional de Registros Públicos, de manera justificada y controlada, como parte de la política de simplificación de trámites, reducción de requisitos y cero papeles.

Interoperabilidad: Es el intercambio y uso de información entre dos o más sistemas, aplicaciones o componentes tecnológicos.

Justificación de uso: Es la finalidad del uso de cada campo explicada de forma determinada y explícita, asegurando que se encuentra alineada con las funciones y competencias institucionales, lo cual justifica el tratamiento legítimo de datos personales. Además, debe incluir los sistemas, aplicativos, servicios o procesos en los cuales se utilizará la información, evitando justificaciones genéricas como "cumplimiento de la misión y visión institucional" o "verificación de datos ciudadanos". Asimismo, deberá detallar las unidades administrativas que tendrán acceso a la información.

Justificación jurídica: Es la justificación sobre la legitimidad del tratamiento de datos personales, cumpliendo con lo dispuesto en la Ley Orgánica de Protección de Datos Personales (LOPDP), su reglamento y otras normativas aplicables que regulen las funciones, atribuciones y responsabilidades de la entidad. Deberá estar conforme a las condiciones de legitimidad y los principios establecidos en la Ley Orgánica de Protección de Datos Personales (LOPDP), para lo cual deberá citar los artículos que corresponda de la normativa que regula sus funciones y competencias, partiendo desde el marco constitucional, Leyes, Reglamentos, Ordenanzas, Decretos y cualquier otra norma pertinente.

En el campo de la justificación jurídica también debe describir la motivación y demostrar la necesidad del acceso a los campos seleccionados, indicando que el tratamiento de los datos personales se va a realizar conforme a las condiciones de legitimidad y los principios establecidos en la Ley Orgánica de Protección de Datos Personales (LOPDP).

Legitimación de acceso: Constituye la justificación de uso y/o justificación jurídica que evidencia el cumplimiento de las condiciones para que el tratamiento de datos personales sea legítimo y lícito.

Artículo 4.- Enrolamiento. - Una vez que la entidad se haya enrolado al Sistema Nacional de Registros Públicos conforme a lo dispuesto en la normativa vigente, podrá solicitar el acceso a los servicios ofrecidos por la Dirección Nacional de Registros Públicos.

CAPÍTULO II

PROCEDIMIENTO DE REVISIONES PREVIAS PARA LOS SERVICIOS INTEROPERABILIDAD, INFODIGITAL Y FICHA DE REGISTRO ÚNICO DEL CIUDADANO (FRUC)

Artículo 5.- Solicitud de revisiones previas. - Las entidades que requieran acceder a los servicios de Interoperabilidad, Infodigital y/o Ficha de Registro Único del Ciudadano

deberán remitir una solicitud al correo electrónico institucional designado por la Dirección Nacional de Registros Públicos, a través de su Coordinador Institucional adjuntando toda la documentación habilitante determinadas para cada servicio específico en la normativa legal vigente.

Artículo 6.- Datos accesibles. - Si el Coordinador Institucional selecciona en el catálogo los campos clasificados como accesibles, se deberá justificar únicamente la finalidad de uso por cada entidad fuente, especificando de manera clara y concreta en relación con sus competencias institucionales.

Artículo 7.- Datos confidenciales. – Si el Coordinador Institucional selecciona campos clasificados como confidenciales, deberá realizar las justificaciones de uso y jurídica por cada campo de manera determinada y explícita.

Artículo 8.- Verificación de requisitos. - En el término de hasta dos (2) días, la Dirección de Gestión y Registro verificará que la solicitud cumpla con los requisitos establecidos en la normativa legal aplicable.

En caso de incumplimiento de alguno de los requisitos, la Dirección de Gestión y Registro notificará a la entidad las razones por las cuales incumple con los requisitos. La entidad tendrá el término de hasta dos (2) días para que complete o aclare la información requerida, de no hacerlo o persistir la inexactitud en el cumplimiento de lo solicitado se considerará como no presentada.

Si la entidad cumple con los requisitos y ha solicitado acceso a datos clasificados como confidenciales, la Dirección de Gestión y Registro remitirá por medio de la herramienta interna definida para el efecto, a la Dirección de Protección de la Información para que evalúe si las justificaciones de uso y jurídicas cumplen con la normativa vigente y validen la legitimidad del acceso a los datos requeridos.

Artículo 9.- Verificación de justificaciones. - La Dirección de Protección de la Información dispondrá de un término de hasta tres (3) días, contados desde la recepción de la documentación, para revisar el catálogo, ya sea para los servicios de Infodigital y/o la Ficha de Registro Único del Ciudadano (FRUC), contados desde la verificación del cumplimiento de los requisitos determinados para cada proceso.

Cuando se trate de solicitudes de revisión para el servicio de interoperabilidad, la Dirección de Protección de la Información tendrá el término de hasta cinco (5) días, contados desde la recepción de la documentación, no obstante, cuando por el volumen de campos involucrados así lo requiera, este proceso podrá ampliarse excepcionalmente hasta por diez (10) días término, conforme a la tabla expedida por la Dirección competente.

Artículo 10.- Observaciones. - Si se identifican observaciones en las justificaciones presentadas, la Dirección de Protección de la Información emitirá un pronunciamiento detallando los aspectos a corregir y las acciones necesarias para su subsanación.

Esta información será remitida a la Dirección de Gestión y Registro, para que en el término de hasta un (1) día notifique a la entidad y proceda con las correcciones requeridas.

Artículo 11.- Subsanación de las observaciones. - La entidad tendrá el término de hasta cinco (5) días contados desde la notificación de las observaciones, para presentar ante la Dirección de Gestión y Registro las justificaciones subsanadas, acompañando los soportes documentales de haber sido requeridos.

Si la entidad remite el catálogo subsanado, la Dirección de Gestión y Registro remitirá el mismo a la Dirección de Protección de la Información en el término de hasta un (1) día para que evalúe si las justificaciones de uso y jurídicas se encuentren conforme a la normativa vigente y validen la legitimidad del acceso a los datos requeridos.

Si la entidad no remite la subsanación de las observaciones en el término establecido, la Dirección de Gestión y Registro notificará a la institución en el término de hasta un (1) día con el cierre de su trámite, de persistir la necesidad la entidad podrá presentar un nuevo requerimiento de revisión.

Artículo 12.- Verificación de justificaciones subsanadas. - La Dirección de Protección de la Información, dentro de un término de hasta tres (3) días contados a partir de la recepción de la documentación, verificará si las justificaciones y la legitimación presentadas para acceder a los datos confidenciales, han sido subsanadas conforme a las observaciones emitidas previamente y, el cumplimiento con la normativa legal vigente.

Si se detectan errores persistentes en la documentación presentada, la Dirección de Gestión y Registro en el término de hasta un (1) día devolverá el trámite a la entidad solicitante para su corrección por última vez en un término de hasta cinco (5) días, con base en las observaciones realizadas.

En caso de que los errores no sean subsanados en el término establecido, la Dirección de Gestión y Registro notificará a la institución en el término de hasta un (1) día con el cierre de su trámite, de persistir la necesidad la entidad podrá presentar un nuevo requerimiento de revisión.

Artículo 13.- Respuesta. - Con base a la revisión realizada por la Dirección de Protección de la Información, la Dirección de Gestión y Registro emitirá una respuesta a la entidad en el término de hasta un (1) día sobre la aprobación de la revisión previa de la solicitud y la continuidad del proceso con base a la normativa emitida por la Dirección Nacional de Registros Públicos.

La aprobación de la revisión previa constituye un requisito para la oficialización de la solicitud.

CAPÍTULO III

PROCEDIMIENTO DE REVISIONES PREVIAS PARA ENTREGA DIRECTA Y EXCEPCIONAL DE DATOS O INFORMACIÓN

Artículo 14.- Solicitud revisiones previas. – Posterior al enrolamiento al Sistema Nacional de Registros Públicos, si la entidad cumple con los supuestos de excepción, podrá solicitar la autorización para el consumo directo de datos e información, para lo cual deberá enviar una solicitud al correo institucional establecido por la Dirección Nacional de Registros Públicos, a través de su Coordinador Institucional adjuntando los requisitos conforme a lo establecido en la normativa legal aplicable para su valoración.

Artículo 15.- Verificación de la solicitud. – Una vez remitida la solicitud, la Dirección de Gestión y Registro dentro del término de hasta dos (2) días verificará el cumplimiento de los requisitos de la solicitud, documentos que deberán ser remitidos en formato borrador editable.

Si cumple con los requisitos, la Dirección de Gestión y Registro remitirá a la Coordinación de Infraestructura y Seguridad Informática para su respectiva revisión.

En caso de incumplimiento, la Dirección de Gestión y Registro notificará a la entidad los motivos por los cuales incumple con los requisitos. La entidad tendrá el término de hasta dos (2) días para que lo complete, aclare o adjunte la información requerida, de no hacerlo o persistir el incumplimiento se considerará como no presentada.

Artículo 16.- Evaluación de los requisitos técnicos. – En el término de hasta dos (2) días, la Coordinación de Infraestructura y Seguridad Informática revisará y analizará lo siguiente:

1. Justificación técnica y tecnológica, que dificulte consumir datos a través de la plataforma de interoperabilidad de la Dirección Nacional de Registros Públicos; que deberá contener al menos el método de consumo de la información y la frecuencia de actualización;
2. Mecanismo de anonimización;
3. Estructura de la base de consulta;
4. El informe de cumplimiento de los protocolos de seguridad, respecto a la evaluación técnica, deberá contener:
 - a) Implementación o actualización del Esquema Gubernamental de Seguridad de la Información (EGSI) o Sistema de Gestión de Seguridad

de la Información implementado en la institución, a la misma se deberá adjuntar la declaración y documentación de respaldo de la implementación.

- b) Los preceptos tecnológicos que garanticen la disponibilidad, confidencialidad e integridad de la información digital, así como una carta de compromiso respecto al cumplimiento de las medidas de seguridad tecnológica, que deberá incluir lo siguiente:
 - i. Aseguramiento del canal de transmisión mediante el empleo de redes privadas virtuales o en su efecto hacer uso del enlace de datos de la red nacional gubernamental;
 - ii. Autenticación, mediante el empleo de usuarios y contraseñas para acceder a la información;
 - iii. Compresión de datos como método para transformarlos y reducir su tamaño;
 - iv. Cifrado de datos como método para transformarlos y mantenerlos en secreto; y;
 - v. Anonimización

- 5. Informe de análisis de riesgo y evaluación de impacto, que identifique los riesgos sobre el proceso de transferencia de información que ejecutarán, para ello, podrán utilizar la metodología establecida en el Esquema Gubernamental de Seguridad de la Información (EGSI) para el análisis de riesgos, u otra metodología equivalente y pertinente para este tipo de análisis.

Una vez revisado el cumplimiento técnico, tecnológico y seguridades por parte de la Coordinación de Infraestructura y Seguridad de la Información, emitirá su pronunciamiento favorable o, en su defecto las observaciones detallando los aspectos que deberán ser subsanadas, dentro de la herramienta determinada por la Dirección Nacional de Registros Públicos.

La Coordinación de Infraestructura y Seguridad Informática remitirá la solicitud a la Dirección de Gestión y Registro, la misma que en el término de hasta un (1) día remitirá a la Dirección de Protección de la Información para su revisión.

Artículo. 17. Evaluación de los requisitos jurídicos - La Dirección de Protección de la Información, en un término de hasta cinco (5) días revisará y analizará que el requerimiento cumpla con la normativa emitida por la Dirección Nacional de Registros Públicos y con lo dispuesto por la Ley Orgánica de Protección de Datos Personales y su reglamento.

Debiendo contener lo siguiente:

1. Identificación de la entidad fuente;
2. La finalidad del tratamiento del dato;
3. Datos a los que desea acceder con la descripción y la categoría del dato;
4. Legitimación de acceso, que contiene la motivación jurídica para el tratamiento de datos; conforme lo previsto en la Ley Orgánica de Protección de Datos Personales;
5. Temporalidad solicitada;
6. Tiempo de conservación de los datos; mecanismos de destrucción;
7. Acta de trabajo entre entidad consumidora y entidad fuente que debe contener los supuestos de excepcionalidad, los acuerdos para llevar a cabo el consumo de información y el tiempo acordado;
8. El acuerdo de uso y confidencialidad por parte de aquellos servidores públicos involucrados en la entrega y tratamiento de información;
9. Informe de cumplimiento de los protocolos de seguridad, respecto a la evaluación jurídica sobre el parámetro de protección de datos personales.

En caso de incumplimiento, determinará las observaciones, detallando los aspectos que deberán ser subsanados, y remitir las mismas a través de la herramienta establecida por la Dirección Nacional de Registros Públicos.

Artículo. 18. Observaciones. - En el término de hasta un (1) día, la Dirección de Gestión y Registro recopilará las observaciones emitidas por la Coordinación de Infraestructura y Seguridad Informática y la Dirección de Protección de la Información, para ser remitidos a la entidad ya sea para que subsane las observaciones que existiere o, en su defecto formalice el requerimiento para la autorización de consumo.

Artículo. 19.- Subsanación de las observaciones. - La entidad tendrá el término de hasta cinco (5) días para remitir a la Dirección de Gestión y Registro la solicitud con las observaciones subsanadas.

Si la entidad remite la subsanación de las observaciones, la Dirección de Gestión y Registro en el término de hasta un (1) día, remitirá la solicitud a la Coordinación de Infraestructura y Seguridad Informática y/o a la Dirección de Protección de la Información, según corresponda, para que se verifique si las observaciones han sido subsanadas.

Si la entidad no remite la subsanación de las observaciones en el término establecido, la Dirección de Gestión y Registro notificará a la institución en el término de hasta un (1) día con el cierre de su trámite, de persistir la necesidad la entidad podrá presentar un nuevo requerimiento para revisión.

Artículo 20.- Verificación de subsanación a las justificaciones tecnológicas. - La Coordinación de Infraestructura y Seguridad Informática en el término hasta dos (2) días

emitirá su pronunciamiento a través de la herramienta tecnológica determinada, respecto al cumplimiento sobre aspectos técnicos, tecnológicos y de seguridad.

Si se detectan errores persistentes en la documentación presentada, la Coordinación de Infraestructura y Seguridad Informática emitirá su pronunciamiento en la herramienta tecnológica determinada por la Dirección Nacional de Registros Públicos.

Artículo 21.- Verificación de subsanación de justificaciones jurídicas. - La Dirección de Protección de la Información en el término de hasta tres (3) días evaluará si la solicitud cumple con lo dispuesto en la normativa emitida por la Dirección Nacional de Registros Públicos y la Ley Orgánica de Protección de Datos Personales, su reglamento y demás normas conexas.

Si se detectan errores persistentes en la documentación presentada, la Dirección de Protección de la Información emitirá su pronunciamiento en la herramienta tecnológica determinada por la Dirección Nacional de Registros Públicos.

Artículo. 22.- Observaciones no subsanadas. - Si se detectan errores persistentes en la documentación presentada, la Dirección de Gestión y Registro recopilará las observaciones emitidas por la Coordinación de Infraestructura y Seguridad Informática y Dirección de Protección de la Información en el término de hasta un (1) día y, devolverá el trámite a la entidad solicitante para su corrección por última vez en un término de hasta cinco (5) días, con base en las observaciones realizadas.

En caso de que los errores no sean subsanados en el término establecido, la Dirección de Gestión y Registro notificará a la institución en el término de hasta un (1) día con el cierre de su trámite, de persistir la necesidad la entidad podrá presentar un nuevo requerimiento para revisión.

Artículo. 23.- Respuesta. - Con base a la revisión realizada por la Coordinación de Infraestructura y Seguridad Informática y la Dirección de Protección de la Información, la Dirección de Gestión y Registro emitirá una respuesta a la entidad en el término de hasta un (1) día sobre la aprobación de la revisión previa de la solicitud y la continuidad del proceso con base a la normativa emitida por la Dirección Nacional de Registros Públicos.

La aprobación de la revisión previa constituye un requisito para la oficialización de la solicitud.

DISPOSICIONES GENERALES

PRIMERA. - Disponer a la Coordinación de Infraestructura y Seguridad Informática, Coordinación de Gestión, Registro y Seguimiento; y, Coordinación de Normativa y

Protección de la Información, o quien haga sus veces la ejecución y cumplimiento de la presente resolución.

SEGUNDA. - Disponer a la Dirección de Comunicación Social la difusión y publicación de la presente resolución en la página web institucional.

TERCERA. - Disponer a la Coordinación de Infraestructura y Seguridad Informática, Coordinación de Gestión, Registro y Seguimiento; y, Coordinación de Normativa y Protección de la Información, el acompañamiento y coordinación de mesas de trabajo, en caso de que las entidades requieran para el efectivo uso de la presente resolución.

DISPOSICIONES TRANSITORIAS

PRIMERA. - En el término de cuarenta y cinco (45) días contados desde la entrada en vigencia de esta resolución, la Dirección de Protección de la Información junto a la Dirección de Comunicación Social, elaborará el Instructivo para llenar el catálogo de los servicios.

SEGUNDA. - En el término de quince (15) días contados desde la entrada en vigencia de esta resolución, la Dirección de Protección de la Información, elaborará la tabla para determinar el número de días para la revisión previa en interoperabilidad dependiendo del volumen de campos involucrados, con un margen de hasta máximo 10 días término, conforme al artículo 9 de la presente resolución.

TERCERA. - La Dirección de Gestión y Registro capacitará a los Coordinadores Institucionales sobre el contenido de la presente resolución, en el término treinta (30) días contados desde la publicación de la presente resolución en el Registro Oficial.

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

Quito, a los 05 días del mes de junio de 2025.

Mgs. Paolo Sebastián Grijalva González
DIRECTOR NACIONAL DE REGISTROS PÚBLICOS (E)

Revisado y aprobado por:	Abg. Patricia Estefanía Rosero Rivadeneira Coordinadora de Normativa y Protección de la Información
Elaborado por:	Mgs. Jennifer Mishel Carrillo Rosales Directora de Normativa