CONSIDERANDO

Que el numeral 19 del artículo 66 de la Constitución de la República reconoce y garantiza 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.

Que el artículo 141 de la Constitución de la República dispone que el Presidente de la República ejerce la Función Ejecutiva, es el Jefe del Estado y de Gobierno y responsable de la administración pública;

Que el numeral 13 del artículo 147 de la Constitución de la República prescribe que es atribución del Presidente de la República, expedir los reglamentos necesarios para la aplicación de las leyes, sin contravenirlas ni alterarlas, así como los que convengan a la buena marcha de la administración.

Que la Asamblea Nacional expidió la Ley Orgánica de Protección de Datos Personales, publicada en el Registro Oficial Suplemento No. 459 de 26 de mayo de 2021;

Que es necesario emitir el Reglamento a la Ley Orgánica de Protección de Datos Personales para establecer con claridad los preceptos y procedimientos para la ejecución de la Ley, sin exceder las disposiciones legales establecidas en la misma; y,

En ejercicio de las facultades y atribuciones que le confiere el numeral 13 del artículo 147 de la Constitución de la República y artículo 129 del Código Orgánico Administrativo, expide la siguiente;

REGLAMENTO A LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES

TÍTULO I
DISPOSICIONES GENERALES

Art. 1.- Objeto.- El presente Reglamento General tiene por objeto la aplicación de la Ley Orgánica de Protección de Datos Personales.

Art. 2.- Ámbito.- Las disposiciones de este Reglamento, se aplican a todas las personas naturales y jurídicas, del sector público y privado, así como organizaciones, entidades y organismos en general, que realicen tratamiento de datos personales, contenidos en soportes o ficheros automatizados o no, dentro o fuera del territorio nacional, que exceda el ámbito doméstico o familiar, en los términos previstos en los artículos 2 y 3 de la Ley Orgánica de Protección de Datos Personales.

Art. 3.- Definiciones.- Sin perjuicio de lo dispuesto en la Ley, para efectos de la aplicación del presente Reglamento, se establecen las siguientes definiciones:

1. Actividades familiares o domésticas: aquellas en las cuales la utilización de los datos personales se dé en un entorno de amistad, parentesco o grupo personal cercano y que no tengan como propósito su divulgación o utilización comercial.

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

3. Fuente accesible al público: Bases de datos que pueden ser consultadas por cualquier persona, cuyo acceso es público y generalizado y no está restringido a un círculo determinado de usuarios.

4. Tratamiento a gran escala: es aquel que afecta a una gran cantidad de datos, referentes a un elevado número de sujetos, procedentes de una amplia diversidad geográfica, y que pueden entrañar un riesgo para los titulares.

Art. 4.- De la recogida del consentimiento.- El responsable de datos personales deberá obtener el consentimiento del titular de conformidad a lo establecido en el artículo 8 de la Ley Orgánica de Protección de Datos Personales.

En todos los casos en los que de conformidad con la Ley se requiera el consentimiento explícito del titular para el tratamiento de sus datos, el responsable deberá informarle previa y detalladamente los tipos de tratamiento, finalidades, el tiempo de conservación, las medidas de protección a adoptarse, las consecuencias de su entrega, entre otros aspectos determinados en la Ley; lo cual deberá ser consentido inequívocamente por el titular.

El consentimiento del titular deberá reflejar de manera indubitada la aceptación de éste en relación con el tratamiento de sus datos personales a través de una declaración o clara acción afirmativa. El consentimiento otorgado por el titular deberá ser demostrado por el responsable que lo obtiene, cuando así sea requerido por la autoridad competente.

Cuando los datos personales recogidos pertenecen a un incapaz, bastará con el consentimiento del representante legal debidamente acreditado ante el responsable, en los términos señalados en el presente artículo

Art 5.- De la revocatoria del consentimiento.- El titular tendrá derecho a retirar su consentimiento en cualquier momento. La revocatoria del consentimiento no afectará a la licitud del tratamiento de datos llevados a cabo hasta el momento de la revocatoria. El responsable del tratamiento deberá contar con un procedimiento sencillo para que el titular pueda revocar su consentimiento.

El responsable del tratamiento deberá suspender el tratamiento de los datos del titular que haya revocado su consentimiento, inmediatamente de recibida la notificación por parte del titular.

Art. 6.- Tratamiento legítimo: Para efectos del correcto tratamiento de datos personales, se considerará lo siguiente:

En el caso de que sea necesario satisfacer un interés legítimo del responsable del tratamiento o de un tercero interesado, se aplicará la regla de ponderación, siempre que no prevalezca el interés o derechos fundamentales del titular.

La ponderación se realizará a través de una evaluación meticulosa que atienda los siguientes factores:

a) evaluación del interés legítimo del responsable del tratamiento o del tercero que deberá ser necesario y proporcionado,
b) impacto sobre los titulares que mida las consecuencias reales o potenciales derivadas del tratamiento,

c) equilibrio provisional, que contemple las medidas adoptadas por el responsable del tratamiento para cumplir sus obligaciones en términos de proporcionalidad y transparencia; y,
d) garantías adicionales aplicadas por el responsable del tratamiento para impedir cualquier impacto indebido sobre los titulares.

Para el tratamiento de datos personales que consten en bases de datos de acceso público, se considerará que los datos deben ser obtenidos de fuentes accesibles al público, según la definición de la Ley y el presente reglamento, respetando el principio de limitación de la finalidad, atendiendo a las razones concretas que han determinado la publicación de la información, especialmente cuando dicha publicación se realiza en cumplimiento de una obligación legal o por razones de interés público. Consecuentemente, el tratamiento de los datos personales obtenidos de fuentes accesibles al público requiere que la finalidad pretendida con el nuevo tratamiento sea compatible con la finalidad que justificó la publicación de los datos, por lo que, el hecho de que los datos figuren en fuentes públicas no determina, sin más, la posibilidad de realizar un tratamiento indiscriminado por parte de los responsables.

CAPITULO II
DE LOS PRINCIPIOS

Art. 7.- Confidencialidad.- Los responsables y encargados de tratamientos de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetos al deber de confidencialidad.

El deber de confidencialidad se mantendrá aun cuando haya finalizado la relación entre el obligado con el responsable o encargado de tratamiento y/o el titular.

Art. 8.- Responsabilidad proactiva y demostrada.- Entre los mecanismos que el responsable podrá adoptar para cumplir con el principio de responsabilidad proactiva y demostrada se encuentran los siguientes, sin perjuicio de otros que pueda definir el Superintendente de Protección de Datos Personales:

1. Destinar recursos para la instrumentación de programas y políticas de protección de datos personales;

2. Implementar sistemas de administración de riesgos asociados al tratamiento de datos personales;

3. Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable;

4. Implementar y mantener actualizados programas de capacitación en materia de protección de datos personales.

5. Revisar periódicamente las políticas y programas de seguridad de datos;

6. Contar con un sistema de supervisión que permita comprobar el cumplimiento de las políticas de protección de datos personales; y,

7. Establecer mecanismos para la recepción y atención de dudas y quejas por parte de los titulares.

CAPITULO III
DE LA CONSERVACION DE DATOS PERSONALES

Art. 9.- Plazos de conservación de los datos personales.- Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean estrictamente necesarios para el cumplimiento de las finalidades que justificaron el tratamiento, y deberán atender las disposiciones aplicables a la materia de que se trate.

Una vez cumplida la o las finalidades del tratamiento, y cuando no exista disposición legal o reglamentaria o no incurra la necesidad de mantener los datos en virtud del interés legítimo del responsable o por cumplimiento de una obligación legal que establezca lo contrario, el responsable deberá proceder a la cancelación de los datos en su posesión, para su posterior supresión.

El responsable establecerá procedimientos para la conservación, eliminación y supresión de los datos personales.

Art. 10.- Prueba del cumplimiento de los plazos de conservación. - Al responsable le corresponde demostrar que los datos personales se conservan o, en su caso, suprimen, cumpliendo los plazos previstos en el presente Reglamento, o bien, en atención a una solicitud de derecho de supresión, cuando esta se estime procedente.

Art. 11.- Fichero de registro.- El fichero del registro de la base de datos deberá contener obligatoriamente el plazo de conservación de los datos, que deberá observar necesariamente la naturaleza del dato, su tratamiento y finalidad.

Art. 12.- Finalizado el plazo de conservación de los datos, el responsable del tratamiento de datos deberá proceder a la eliminación de los mismos.

La Superintendencia de Protección de Datos Personales podrá requerir información cuando considere necesario, para el efecto, el responsable deberá almacenar la siguiente información:

1. Forma de obtención de los datos que se suprimieron.
2. Fecha de inicio del tratamiento del dato.
3. Finalidad para el tratamiento del dato.
4. Culminación del plazo.
5. Detalle de los datos eliminados.
6. Técnicas utilizadas para la eliminación de los datos y la fecha en la que este se llevó a cabo.
7. Razones para la eliminación.
8. Declaración de no conservar en ningún tipo de medio tecnológico o no, los datos a ser eliminados.
9. Firmas del responsable.

CAPITULO IV
DE LOS DERECHOS

Art.13.- Derecho de acceso.- El titular tendrá derecho a obtener del responsable del tratamiento, la confirmación de si se están tratando o no datos personales que le conciernan y, en tal caso, se le reconoce el derecho a acceder a los mismos y a la siguiente información:

1. Los fines del tratamiento.

2. Si sus datos personales se están tratando actualmente.

3. Las categorías de datos personales de que se trate.

4. Los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales.

5. De ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo.

6. La existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento.

7. Cuando los datos personales no se hayan obtenido del directamente interesado, la información respecto la forma en la que fueron recolectados y su origen.

9. Cuando se transfieran datos personales a un tercer país o a una organización internacional fuera del territorio ecuatoriano, el interesado tendrá derecho a ser informado de las garantías adecuadas relativas a la transferencia y al tratamiento.

Art. 14.- Plazo.- El responsable atenderá la solicitud del interesado en el término de quince (15) días contados desde la recepción de la solicitud, confirmando o no la existencia de una base de datos en que consten sus datos personales, proporcionando información sobre las condiciones del tratamiento y entregando una copia de los mismos, si así lo hubiese requerido; o a su vez, indicando las razones de su negativa, cuando fuere del caso.

Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará en dicho formato, salvo que el titular solicite que se facilite de otro modo, siempre que no signifique costos desproporcionados para el responsable.

Art. 15.- Abuso del derecho.- Se entenderá que existe abuso en el ejercicio de este derecho cuando se lo ejerza de forma repetitiva y desproporcionada, esto es, cuando se solicite acceder a los datos más de una vez en un plazo de seis (6) meses.

Art. 16.- Derecho de rectificación y actualización.- De conformidad con lo dispuesto en la Ley, el titular podrá solicitar en todo momento al responsable que rectifique o actualice sus datos personales que resulten ser inexactos o incompletos.

La solicitud deberá indicar con precisión el dato personal que se pretende rectificar o actualizar, así como la corrección que deba efectuarse, de ser necesario, y deberá ir acompañada de la documentación que ampare la procedencia de lo solicitado.

Art.-17.- Plazo.- El responsable procederá a la rectificación o actualización de los datos personales que consten en su(s) base(s) de datos, en el término de quince (15) días, contados desde la recepción de la misma y dará contestación en el mismo término a la solicitud del titular, confirmando que se ha procedido a la rectificación o actualización, o las razones de su negativa, cuando fuere del caso de conformidad con las excepciones previstas en el artículo 18 de la Ley.

El responsable informará sobre la rectificación o actualización a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que fuere imposible o exija un esfuerzo desproporcionado. El responsable identificará a los destinatarios, en caso de que el titular así lo requiera.

Art. 18.- Derecho de oposición.- El titular de datos personales podrá, en todo momento, oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo.

El titular deberá justificar que aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un perjuicio.

Este derecho tiene por objeto el cese del tratamiento respecto del cual se ejerció el derecho y no la cancelación o eliminación de los datos respecto de los cuales se ejerció, por lo que para acreditar que se cumplió con la solicitud de oposición será suficiente con demostrar que el tratamiento específico, respecto del que procedió la oposición, ya no se lleva a cabo.

Art. 19.- Plazo.- El responsable cesará en el tratamiento de los datos personales del titular en el término de quince (15) días contados desde la recepción de la oposición, y dará contestación en el mismo término a la solicitud del titular, confirmando que ha dejado de tratar los datos personales del titular; o las razones de su negativa, de conformidad con las excepciones previstas en los artículos 16 y 18 de la Ley.

Art. 20.- Derecho de eliminación: El titular podrá solicitar, en cualquier momento, la supresión de sus datos personales en los casos previstos en el artículo 15 de la Ley, en la medida en que no exista una de las excepciones previstas en el artículo 18 de la ley, indicando en su solicitud la causal que motiva su requerimiento.

La eliminación dará lugar a que los datos ya no estén disponibles, de manera que no podrán ser objeto de tratamiento.

La eliminación procederá respecto a la totalidad de los datos personales del Titular contenidos en una base de datos a cargo del responsable del tratamiento, o solo a una parte de ellos, según conste en la solicitud.

El responsable procederá a la supresión de los datos personales del titular en el término de quince días (15) contados desde la recepción de la solicitud de eliminación, y dará contestación en el mismo término a la solicitud del titular, confirmando la supresión de los datos personales de sus bases de datos, o las razones de su negativa, de conformidad con las excepciones previstas en el artículo 18 de la Ley.

El responsable del tratamiento informará sobre la eliminación a cada uno de los destinatarios, salvo que fuere imposible o exija un esfuerzo desproporcionado. El responsable identificará a los destinatarios, en caso de que el titular así lo requiera.

Art. 21.- Derecho a la portabilidad.- El titular tendrá derecho a recibir del responsable en un formato estructurado, de uso común y lectura mecánica, los datos personales que le conciernan y que hubiere facilitado al responsable cuando se cumplan los siguientes requisitos:

1. El tratamiento se efectúe por medios automatizados, y;

2. El tratamiento tenga como base o fundamento en el consentimiento del titular legítimamente otorgado en los términos previstos en la Ley o que el tratamiento de datos personales se sustente a petición del titular o para el cumplimiento de obligaciones contractuales.

El titular tendrá derecho a que los datos personales objeto del derecho a la portabilidad se transmitan directamente, de responsable a responsable, siempre y cuando esa transmisión sea técnicamente posible.

El ejercicio del derecho a la portabilidad siempre será gratuito para el titular.

Art. 22.- De la solicitud.- En la solicitud el titular deberá indicar si desea conservar o eliminar los datos transmitidos o transferidos. El responsable confirmará la eliminación de los datos personales del titular de su base de datos en caso de haber sido solicitada por el titular.

El responsable procederá a la transferencia de los datos personales en el término de treinta (30) días contados desde la recepción de la solicitud, o las razones de su negativa, de conformidad con las excepciones previstas en el artículo 17 y 18 de la Ley.

Art. 23.- Derecho de suspensión.- El titular podrá, en cualquier momento, solicitar al responsable la suspensión del tratamiento de sus datos personales, siempre y cuando se cumpla alguna de las condiciones previstas en el artículo 19 de la Ley.

Para tal efecto, el titular deberá hacer constar en la solicitud el motivo por el cual solicita la suspensión del tratamiento de conformidad con el artículo 19 de la Ley.

El Responsable del procederá a la suspensión del tratamiento de los datos personales en el término de quince (15) días contados desde la recepción de la solicitud, y dará contestación en el mismo término a la solicitud del titular, confirmando que el tratamiento de los datos personales ha sido suspendido o en su defecto, las razones de su negativa, de conformidad con las excepciones previstas en la Ley.

El responsable informará sobre la suspensión del tratamiento a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que fuere imposible o exija un esfuerzo desproporcionado. El responsable identificará a los destinatarios, en caso de que el titular así lo requiera.

A fin de hacer efectivo este derecho, el responsable, podrá utilizar los siguientes mecanismos:

1. Mover temporalmente los datos seleccionados a otro sistema de tratamiento.
2. Evitar el acceso de usuarios a los datos personales seleccionados.
3. Suprimir temporalmente los datos publicados de un sitio web.
4. Otros que garanticen que los datos personales objeto de la suspensión, no se modifiquen, supriman o borren.

Mientras dure la suspensión el responsable, únicamente podrá conservarlos y tratarlos para los supuestos previstos en el artículo 19 de la Ley.

Art. 24.- Derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas.- Cuando el responsable trate datos personales, como parte de un proceso de toma de decisiones, sin que intervenga una persona natural, deberá informar de esta circunstancia a su titular.

El titular podrá, en cualquier momento, solicitar al responsable, información sobre los aspectos contenidos en el artículo 20 de la Ley.

El responsable atenderá los requerimientos realizados por el titular en el término de quince (15) días contados desde la recepción de la solicitud, en la que responderá a las peticiones del titular; o expondrá las razones de su negativa, de conformidad con las excepciones previstas en el artículo 20 de la Ley.

De ser el caso, con base en la contestación obtenida, el titular podrá ejercer el derecho de rectificación, cuando considere que alguna información sea inexacta o incompleta.

Art. 25.- Derecho de consulta.- El titular, responsable del tratamiento, encargados del tratamiento, destinatarios, delegados de protección de datos personales y ciudadanos en general, podrán presentar a la Superintendencia de Protección de Datos Personales, en cualquier momento, inquietudes o dudas respecto al contenido, alcance o aplicación de la Ley Orgánica de Protección de Datos Personales, así como sobre el ejercicio de derechos previstos en la misma.

La Superintendencia de Protección de Datos Personales, deberá atender y absolver las inquietudes o consultas planteadas en el término de quince (15) días contados desde la recepción de la misma.

La Superintendencia de Protección de Datos Personales pondrá a disposición de los ciudadanos las herramientas y medios físicos y digitales, sencillos y expeditos, para formular las consultas, dudas o inquietudes sobre la aplicación de la Ley Orgánica de Protección de Datos Personales, su Reglamento y demás normativa secundaria.

Art. 26.- Derecho a la educación digital.- El Estado, a través de las autoridades competentes, elaborarán un plan transversal de educación y desarrollo de habilidades digitales, destinado a alfabetizar y capacitar sobre el manejo de las tecnologías de la información y comunicación y ciberseguridad, con énfasis en los grupos de atención prioritaria.

Asimismo, el Estado, a través de las autoridades competentes, trabajarán en la elaboración de políticas públicas, planes, programas, talleres, capacitaciones, con el objeto de promover una cultura de protección de datos personales en el país.

El sistema educativo nacional, incluyendo el sistema de educación superior, incorporará dentro de su pensum de estudios y oferta académica, la temática de las tecnologías de la información y comunicación, en especial, en el derecho a la protección de datos personales y ciberseguridad.

Art. 27.- Ejercicio de derecho de protección de datos personales para niños, niñas y adolescentes.- El Estado diseñará e implementará políticas públicas y programas destinados al uso adecuado, responsable y seguro de los datos personales de niños, niñas y adolescentes, de conformidad con la normativa técnica que para el efecto emita la Superintendencia de Protección de Datos Personales.

En lo no previsto expresamente en la Ley Orgánica de Protección de Datos y su Reglamento para el ejercicio de los derechos de niños, niñas y adolescentes, se aplicarán las demás normas del ordenamiento jurídico interno, que no contradigan los principios que se reconocen en la Ley Orgánica de Protección de Datos Personales y sean más favorables para la vigencia de este grupo.

Art. 28.- Sin perjuicio de lo dispuesto en este Reglamento, corresponderá a la Superintendencia de Protección de Datos Personales emitir la normativa secundaria que garantice el ejercicio de los derechos reconocidos en la Ley.

Art. 29.- Personas facultadas para el ejercicio de los derechos.- Los derechos consagrados en la Ley se ejercerán por el titular del dato personal, previa acreditación de su identidad, o por el representante del titular, previa constatación de la identidad del representado y representante y de la vigencia de la representación.

Tratándose de personas fallecidas, los titulares de derechos sucesorios podrán ejercer los derechos reconocidos en la Ley, previa acreditación de su identidad y la relación con la del fallecido. En caso de ser varias las personas con derecho a la sucesión, deberán designar un apoderado, que constará por documento privado debidamente noratizado.

En caso de fallecimiento de niñas, niños, adolescentes o personas que la ley reconozca como incapaces, el ejercicio de los derechos reconocidos en la Ley se llevará a cabo por su último representante legal, y si estos fueran varios, por cualquier de ellos.

Para el ejercicio de los derechos consagrados en la Ley con respecto a los datos personales de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad, se estará a las reglas de representación dispuestas en el Código Civil.

Art. 30.- Medios para el ejercicio de los derechos.- El responsable habilitará preferentemente herramientas o canales informáticos simplificados de fácil acceso para el titular, con la finalidad de receptar y atender oportunamente, hasta su conclusión, las solicitudes o peticiones formuladas, que permitan y garanticen una interacción segura, fiable y rápida entre el responsable y el titular, sin perjuicio de que las mismas puedan también ser presentadas por medios físicos.

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

Art. 31.- Contenido de la solicitud.- La solicitud para el ejercicio de los derechos consagrados en la Ley contendrá:

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

A la solicitud se acompañará los documentos que justifiquen la pertinencia de lo solicitado, cuando proceda, y los que acrediten la identidad o, en su caso, la representación legal o convencional del titular.

Art. 32.- Requerimiento de información adicional.- En caso de que la solicitud presentada no cumpla todos los requisitos, o la información que en ella se consigne merezca ser aclarada a juicio del responsable, este podrá requerir al titular, por una sola vez y dentro del término de cinco (5) días de recibida la solicitud, que la aclare o complete.

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

Si el titular aclara o completa la solicitud dentro del término concedido, el responsable acordará su admisión y le dará la debida atención, caso contrario, la archivará sin formular trámite, notificando este particular al titular. El archivo del requerimiento inicial no impedirá la presentación de una nueva solicitud.

Art. 33.- Registro de solicitudes.- El responsable deberá registrar todas las solicitudes de ejercicio de derechos.

Art. 34.- Reclamo ante la Superintendencia de Protección de Datos Personales.- El titular de datos personales que se encuentre disconforme con la respuesta que el responsable ha concedido a su solicitud, o que no haya recibido respuesta en el plazo establecido, podrá acudir a la Superintendencia de Protección de Datos Personales a presentar un reclamo, el cual se sustanciará conforme al procedimiento previsto en el Código Orgánico Administrativo y en la normativa complementaria que, para el efecto, emita el Superintendente.

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

TITULO II
DE LAS CATEGORIAS ESPECIALES

Art. 35.- Las categorías de datos especiales se clasifican en dos tipos:

a) Datos sensibles; y,
b) Datos que, por sus connotaciones particulares, requieren una regulación especial, adicional a la establecida con carácter general en la Ley Orgánica de Protección de Datos Personales.

CAPITULO I
DISPOSICIONES GENERALES SOBRE DATOS SENSIBLES

Art. 36.- Datos sensibles.- Constituyen datos sensibles todos aquellos previstos en la definición del artículo 4 de la Ley Orgánica de Protección de Datos Personales, de los cuales se distinguen dos tipos:

a) Datos personales cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico; y,
b) Datos genéticos y datos biométricos dirigidos a identificar de manera unívoca a una persona física y los datos relativos a la salud.

Art. 37.- Prohibición de tratamiento de datos sensibles: El tratamiento de datos sensibles está prohibido de conformidad con lo previsto en el artículo 26 de la Ley Orgánica de Protección de Datos Personales, salvo que concurra alguna de las causas señaladas en la referida disposición normativa, entre las que se destacan:

1) Que el titular de los datos personales sensibles haya dado su consentimiento explícito para tal tratamiento, entendido éste como una categoría cualificada del consentimiento general previsto en la ley, que se manifiesta mediante una declaración expresa, clara y determinante, que elimine cualquier posible duda y potencie la falta de evidencia en el futuro. En tal sentido, el sólo consentimiento general del titular previsto en la ley, no será suficiente.

2) Que el tratamiento sea 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. Para el efecto, el responsable deberá establecer las garantías apropiadas, a efectos de proteger los datos personales y otros derechos fundamentales e intereses del titular y el tratamiento se limitará a dar cumplimiento con los preceptos normativos dictados en materia laboral y de seguridad social, así como los previstos en el contrato colectivo de trabajo. Ello incluirá aquellos tratamientos que sean necesarios para fines de medicina preventiva, para la evaluación de la capacidad laboral del trabajador, el diagnóstico médico, la prestación de asistencia sanitaria o social, la gestión de sistemas y servicios de asistencia sanitaria o social.

Si el tratamiento de los datos personales especialmente protegidos de los trabajadores se basa en el consentimiento, la dependencia del trabajador en la relación laboral y las circunstancias en las que se dio el consentimiento se tendrán en cuenta para evaluar si éste se lo dio libremente. En estos casos, se considerará que el consentimiento se ha otorgado en forma libre, particularmente, si está asociado a una ventaja jurídica o económica para el trabajador, o si el empleador y el trabajador persiguen los mismos intereses.

3) Que el tratamiento sea 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. Para tal efecto, se considerará las reglas sobre incapacidades previstas en los artículos 517 y siguientes del Código Civil.

Se entiende por "interés vital" situaciones en las que se exponga la vida o integridad del titular o del tercero, así como amenazas que supongan un riesgo de lesiones u otro daño para la salud del titular o del tercero.

4) Que el tratamiento se refiera a datos personales que el titular ha hecho manifiestamente públicos. Por tanto, el titular, de un modo manifiesto, notorio e indudable, debe de haber publicado sus datos personales a una colectividad de la que no tiene control, que excede su círculo privado. Para tal efecto, no se considerará que un dato personal sensible se ha hecho público por parte del titular, si éste ha sido divulgado en redes sociales o a través de otras formas de las que no se pueda concluir, en forma evidente, que el titular lo ha hecho público.

SECCIÓN I
DATOS SENSIBLES RELATIVOS A LA SALUD

Art. 38.- Se dará una interpretación amplia a la definición de datos de salud establecida en la ley, de tal forma que comprenda la información relativa a todos los aspectos, tanto físicos como psíquicos, de la persona. Se incluyen todos los datos relativos al estado de salud del titular que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona natural recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia; todo número, símbolo o dato asignado a una persona natural que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del titular, independientemente de su fuente.

CAPÍTULO II
DISPOSICIONES APLICABLES A TRATAMIENTOS CONCRETOS

SECCIÓN I
DE LOS DATOS DE LAS PERSONAS FALLECIDAS

Art. 39.- De los datos de personas fallecidas.- A efectos de que los causahabientes, representantes y/o terceros debidamente autorizados puedan ejercer los derechos de acceso, rectificación, actualización y eliminación de los datos del fallecido ante el responsable del tratamiento, previsto en el artículo 27 de la Ley, deberán cumplir con lo siguiente:

1) Acreditar, junto con la solicitud del derecho que se ejerce, el derecho como causahabiente, último representante legal y/o tercero autorizado por la persona fallecida, a través de los instrumentos legales reconocidos por el ordenamiento jurídico ecuatoriano.
2) Acreditado el derecho del causahabiente, representante legal y/o tercero autorizado, el responsable del tratamiento deberá dar respuesta dentro de los tiempos y procedimientos establecidos para el ejercicio del respectivo derecho por parte de los titulares de datos personales.
3) El causahabiente, representante legal y/o tercero autorizado de la persona fallecida podrá ejercer el referido derecho las veces que considere oportuno, dentro de las limitaciones que plantea la normativa vigente para el ejercicio de derechos por parte de los titulares de datos personales.

SECCIÓN II
DE LOS DATOS CREDITICIOS

Art. 40.- De los datos crediticios.- A efectos de lo dispuesto en el artículo 28 de la Ley Orgánica de Protección de Datos Personales, será lícito el tratamiento de datos personales que tengan como fin informar sobre el incumplimiento de obligaciones comerciales o crediticias siempre que:

a) Los datos se refieran a deudas ciertas, vencidas y exigibles, que no se encuentren pendientes de resolución por reclamaciones administrativas o judiciales o procedimientos alternativo de resolución de conflictos solicitados por el deudor y vinculante entre las partes;

b) El acreedor haya informado al titular de datos personales (deudor) en el contrato o en el momento de requerir el pago acerca de la posibilidad de inclusión en sistemas de buró de crédito, con indicación de aquéllos en los que participe;

c) Los datos referidos a un deudor determinado solamente puedan ser consultados por quien mantuviese una relación contractual con el deudor que tenga una incidencia comercial y económica;

d) Los datos únicamente se mantengan en el sistema mientras persista el incumplimiento; y,

e) Haya existido previamente requerimiento de pago por parte del acreedor al deudor y se tenga constancia de aquello.

Las entidades que mantengan el sistema y las acreedoras, respecto del tratamiento de los datos referidos a sus deudores, tendrán la condición de corresponsables del tratamiento de los datos.

SECCIÓN III
DE LOS DATOS DE MENORES DE EDAD

Art.41.- De los datos de menores de edad.- De conformidad con lo previsto en el artículo 21 de la Ley Orgánica de Protección de Datos Personales, para el tratamiento de datos personales de menores de 15 años de edad, se requerirá el consentimiento del representante legal.

Los adolescentes mayores de 15 años, podrán brindar, en calidad de titulares, su consentimiento explícito para el tratamiento de sus datos personales.

Cuando el consentimiento se obtenga directamente del adolescente según lo señalado en el párrafo precedente, el responsable deberá realizar sus mayores esfuerzos para que la información a proporcionar al adolescente, previo a que otorgue su consentimiento, sea clara, en un lenguaje sencillo propio de su edad, utilizando métodos que le permitan entender lo que ocurrirá con sus datos personales, las finalidades que se persiguen, los derechos que tiene y cómo ejercerlos y cualquier otra información necesaria para obtener su consentimiento explícito. Asimismo, los responsables del tratamiento deberán utilizar la tecnología disponible, para cerciorarse que el adolescente tiene la edad que declara.

Sin perjuicio de lo anterior, también podrá otorgar el consentimiento del adolescente mayor de 15 años, quien ejerce la patria potestad, sin perjuicio de que el adolescente, en cualquier momento, pueda revocar este consentimiento. El titular de la patria potestad del adolescente no podrá revocar el consentimiento otorgado explícitamente por el adolescente en su calidad de titular.

Art. 42.- Del interés superior del niño.- El consentimiento obtenido para el tratamiento de datos personales de un menor de edad, no podrá, bajo ninguna circunstancia, menoscabar el interés superior del menor, conforme a las disposiciones del Código de la Niñez y Adolescencia y demás normativa vigente. De identificarse aquello, el consentimiento obtenido será considerado inválido.

TÍTULO III
TRANSFERENCIA O COMUNICACIÓN DE DATOS A TERCEROS

Art. 43.- Transferencia de datos personales a un tercero.-La transferencia o comunicación de datos personales a un tercero no requerirá el consentimiento del titular si previo a realizar la misma, se han disociado los datos, de manera que no se pueda identificar a qué persona se refieren.

Art. 44.- Supuestos para la transferencia de datos a terceros.- La transferencia o comunicación de datos personales a terceros se podrá realizar siempre que concurran los siguientes supuestos:

1) Para el cumplimiento de fines directamente relacionados con las funciones legítimas del responsable y del tercero destinatario, en cuyo caso, el destinatario se obliga a cumplir con la normativa de protección de datos; y,
2) Cuando se cuente con el consentimiento previo del titular, el cual puede ser revocado en cualquier momento.

No se requerirá el consentimiento del titular en los supuestos previstos en el artículo 36 de la Ley.

Ar. 45.- El titular de los datos personales ejercerá los derechos de rectificación, actualización, oposición y eliminación, directamente al responsable de tratamiento, quien, a su vez, deberá notificar de aquello al tercero destinatario de la comunicación de datos personales para que proceda con la rectificación, actualización, oposición o eliminación, según sea el caso.

TITULO IV
DE LA VULNERACIÓN A LA SEGURIDAD DE DATOS PERSONALES

Art. 46.- De la notificación de vulneración de seguridad.- De conformidad con lo dispuesto en el artículo 43 de la Ley, el responsable del tratamiento deberá notificar a la Superintendencia de Protección de Datos y a la Agencia de Regulación y Control de Telecomunicaciones cualquier vulneración a la seguridad de los datos personales, siempre que sea probable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas naturales. Por tanto, no deberá notificarse cualquier incidente a la seguridad de los datos.

Se entiende que la vulneración o violación a la seguridad constituye un riesgo para los derechos y las libertades de las personas naturales cuando concurre cualquiera de las siguientes causales:

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

La notificación realizada a la Agencia de Regulación y Control de Telecomunicaciones tendrá específicamente fines de registro y estadísticos. En tal sentido, las facultades de control y sancionatorias corresponderá exclusivamente a la Superintendencia de Protección de Datos Personales.

La notificación de las vulneraciones de seguridad de datos personales tendrá como objetivo principal que la Superintendencia de Protección de Datos Personales lleve un registro estadístico sobre vulneraciones e identificar posibles medidas de seguridad para cada una de ellas, así como identificar sectores o instituciones más vulnerables y promover nuevas regulaciones que busquen mejorar las seguridades exigibles a los responsables de tratamiento y otorgar seguridad jurídica en el tratamiento de datos personales.

Art. 47.- Contenido de la notificación.- La notificación de vulneración de seguridad Deberá contener lo siguiente:

1) La naturaleza y tipo de vulneración;
2) El detalle inicial de los sistemas afectados;
3) La causa presunta de la vulneración;
4) El volumen y tipos de datos expuestos o comprometidos;
5) Las medidas adoptadas y previstas para responder a la vulneración y mitigar las consecuencias presuntas;
6) La evaluación del riesgo que la vulneración implica para los derechos y libertades de los titulares.

Art.- 48.- Notificación de vulneración de seguridad por parte del encargado.- El encargado deberá notificar al responsable del tratamiento de datos personales la vulneración de la seguridad de datos personales.

La notificación de vulneración de seguridad deberá contener la misma información detallada en el artículo precedente, a excepción de la evaluación del riesgo.

El encargado responderá solidariamente por el incumplimiento de la notificación de vulneración de seguridad por parte del responsable.

Art.- 49.- Notificación de vulneración de seguridad al titular.- La notificación de vulneración de datos al titular deberá cumplir con lo establecido en el artículo 47 del presente Reglamento.

La notificación deberá realizarse en lenguaje claro y sencillo, observando los derechos de los titulares.

La Superintendencia de Protección de Datos Personales velará por que las excepciones a la obligación de notificación señaladas en el artículo 46 de la Ley sean utilizadas de manera restringida y de manera justificada.

Art. 50.- Evaluación de impacto del tratamiento de datos personales.- La evaluación de impacto es un análisis preventivo de naturaleza técnica mediante el cual el responsable valora los impactos reales respecto de un tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con el cumplimiento de los principios y el respeto de los derechos y de las obligaciones establecidas en la Ley Orgánica de Protección de Datos Personales, su Reglamento y demás normativa aplicable.

Art. 51.- Objeto de la evaluación de impacto.- La evaluación de impacto tiene por objeto:

1. Identificar y describir los riesgos potenciales y probables de determinados tratamientos de datos personales;

2. Describir las acciones concretas para la gestión de los riesgos identificados;

3. Actuar de forma preventiva en el cumplimiento de las obligaciones establecidas en la Ley, su Reglamento y demás normativa aplicable; y,

4. Propiciar una cultura preventiva de la protección de datos personales aplicando metodologías de prevención de fuga de información y la implementación de soluciones tecnológicas en seguridad de la información.

Art. 52.- Evaluación de impacto obligatoria.- Las evaluaciones de impacto del tratamiento de datos serán obligatorias en los tres supuestos establecidos en el artículo 42 de la Ley y deberán realizarse de forma previa al inicio del tratamiento de datos personales.

Los responsables podrán utilizar los criterios establecidos en el presente Reglamento para determinar en qué casos se está en presencia de una evaluación sistemática y exhaustiva de aspectos personales, de un tratamiento a gran escala de categorías especiales de datos, de datos relativos a condenas e infracciones penales; o, de una observación sistemática a gran escala de una zona de acceso público.

En caso de duda, el responsable podrá dirigir una consulta a la de Protección de Datos Personales con la finalidad de que determine si se presenta alguno de los supuestos previstos en el artículo 42 de la Ley. La Superintendencia de Protección de Datos Personales deberá contestar en el término máximo de cinco (5) días contados desde la recepción de la consulta.

Art. 53.- Requisitos de la evaluación de impacto.- En los casos en que sea obligatoria, la evaluación de impacto será presentada ante la Superintendencia de Protección de Datos Personales y contendrá, al menos, lo siguiente:

1. La descripción sistemática de las operaciones de tratamiento y las finalidades de ese tratamiento;

2. La justificación de la necesidad de llevar a cabo esas operaciones de tratamiento, así como su proporcionalidad con respecto de la finalidad;

3. La evaluación de riesgos a los derechos y libertades de los titulares; y,

   Las medidas previstas para hacer frente a los riesgos, las garantías, medidas de seguridad de la información y gobernanza interna de datos, mecanismos destinados a salvaguardar y demostrar el respeto al derecho de los titulares a la protección de sus datos personales;

La información otorgada en virtud de los numerales precedentes debe limitarse a la que sea necesaria para respaldar la evaluación y no incluir detalles potencialmente confidenciales relacionados con las implementaciones de seguridad o la información confidencial.

TITULO V
RESPONSABLE DEL TRATAMIENTO, ENCARGADO DE TRATAMIENTO Y DELEGADO DE PROTECCIÓN DE DATOS.

CAPÍTULO I
DEL RESPONSABLE DE TRATAMIENTO

Art. 54.- 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 tratamiento 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.

Art 55.- Estado de la técnica.- Se entiende por estado de la técnica a los progresos actuales de la tecnología disponible en el mercado, que deberá ser considerado al determinar las medidas técnicas y organizativas adecuadas. El responsable del tratamiento deberá evaluar continuamente el estado de la técnica.

Art. 56.- Costos de aplicación.- Los costos de aplicación no deben considerarse solamente en términos monetarios, sino los recursos que en general deba invertir el responsable de tratamiento, incluidos el tiempo y el humano. El responsable de tratamiento deberá evaluar los riesgos para los derechos y libertades de los interesados que conlleva el tratamiento y estimar los costos de la aplicación de las medidas adecuadas en el tratamiento para mitigar dichos riesgos. La incapacidad de asumir los costos no es excusa para el incumplimiento de la Ley y el presente Reglamento.

Art. 57.- De la prueba de las medidas de protección.- Los responsables del tratamiento deberán demostrar que han aplicado medidas para la protección de datos personales. Para ello, el responsable del tratamiento podrá determinar los indicadores clave de rendimiento adecuados para demostrar el cumplimiento. Estos indicadores pueden incluir métricas para demostrar la eficacia de las medidas en cuestión. Las métricas pueden ser cuantitativas, como el nivel de riesgo, la reducción de las reclamaciones, la reducción del tiempo de respuesta cuando los interesados ejercen sus derechos; o cualitativas, como las evaluaciones del rendimiento, el uso de escalas de o evaluaciones de expertos.

Art. 58.- Responsables conjuntos.- Si dos o más responsables del tratamiento determinan conjuntamente los fines y los medios del tratamiento de los datos personales, se considerarán responsables conjuntos. Los co responsables del tratamiento definirán sus respectivas tareas y responsabilidades en materia de protección de datos de forma transparente a través un contrato, en la medida en que éstas no estén ya definidas en disposiciones legales, buscando precautelar los intereses y derechos de los titulares.

Dicho acuerdo no impedirá que el interesado ejerza sus derechos contra cualquiera de los co responsables del tratamiento y que estos sean responsables solidarios ante la autoridad de control y los titulares.

Además, cada co responsable deberá cumplir las obligaciones que determina la Ley, en función de las responsabilidades asumidas en el acuerdo, cuya evidencia deberá estar a disposición de la autoridad de control, cuando así lo solicite. En este sentido, cada co responsable es sujeto del régimen sancionador, en forma diferenciada sobre la base de las responsabilidades adquiridas.

Los acuerdos de protección de datos entre co responsables deben ser compartidos con los titulares interesados cuando así sea requerido por éstos, sobre la base del principio de transparencia.

Art. 59.- Registro de actividades de tratamiento.- El responsable del tratamiento que cuente con cien (100) trabajadores o más, llevará un registro de todas las actividades de tratamiento de datos personales que sean de su competencia.

Este registro contendrá la siguiente información:

a) El nombre y los datos de contacto del responsable del tratamiento y, en su caso, del responsable que actúa conjuntamente con el responsable del tratamiento, así como el nombre y los datos de contacto del delegado de protección de datos,
b) Los fines del tratamiento,
c) Las categorías de destinatarios a los que se han comunicado o se comunicarán los datos personales,
d)Una descripción de las categorías de interesados y de las categorías de datos personales,
e) En su caso, el uso de perfiles,
f) En su caso, las categorías de transferencias de datos personales a organismos de un tercer país o a una organización internacional,
g) Información sobre la base legal del tratamiento,
h) Los plazos previstos para la supresión o la revisión de la necesidad de conservar las diferentes categorías de datos personales
i) Una descripción general de las medidas técnicas y organizativas.

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

Art. 60.- La obligación de registro de actividades también la tendrán los responsables de tratamiento que, teniendo menos de 100 trabajadores, cumplan alguna de las siguientes condiciones:

1. El tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los titulares,
2. No se trate de un tratamiento ocasional;
3. Incluya categorías especiales de datos personales.

CAPÍTULO II
DEL ENCARGADO DE TRATAMIENTO

Art. 61.- Encargado.- El encargado del tratamiento deberá ofrecer garantías suficientes para aplicar medidas técnicas y organizativas apropiadas para que el tratamiento cumpla con las disposiciones de la Ley y garantice la protección de los derechos de los titulares.

Art. 62.- De la relación entre responsable y encargado.- La relación entre el responsable del tratamiento y un encargado debe regirse por un contrato escrito, en el cual se detallen las instrucciones encomendadas respecto del tratamiento de datos personales, además deberá incluir, al menos: el objeto, la duración, la naturaleza, la finalidad del tratamiento de los datos, el tipo de datos personales y las categorías de titulares y las obligaciones y responsabilidades del encargado.

El encargado de tratamiento deberá respetar las instrucciones que, para el efecto, determine el responsable en cuanto al tratamiento de los datos personales, para lo cual, deberá establecer las medidas técnicas y organizativas adecuadas, previo a brindar el servicio, que deberán ser equiparables a aquellas que está obligado el responsable en función de los datos y los tipos de tratamiento aplicables, de tal forma que se garantice la protección de datos de los titulares.

Art. 63.-Obligación del responsable.- El responsable del tratamiento de datos personales será el directo obligado de garantizar el correcto ejercicio de los derechos reconocidos en la Ley a los titulares, sin embargo, el encargado deberá asistir al responsable y realizar todas las acciones necesarias y bajo su responsabilidad para que el responsable pueda cumplir con esta obligación; ello, sin perjuicio de que en las instrucciones se determine que el encargado deba dar algún tipo de respuesta directa al titular en caso de que ejerza algún derecho.

Art. 64.- El encargado del tratamiento que, por cualquier causa, determine los fines y los medios del tratamiento, se considerará, para efectos de la Ley, responsable del tratamiento en lo que respecta a dicho tratamiento. En tal sentido, para que el encargado sea considerado tal, debe actuar a nombre y por cuenta del responsable y conforme a las instrucciones documentadas. Si el encargado considera que una instrucción es ilegal, informará al responsable del tratamiento sin demora injustificada, para que se corrija la instrucción, de ser pertinente.

Art. 65.- Registro de actividades del tratamiento.- El Encargado del tratamiento tiene la obligación de mantener un registro de actividades del tratamiento, conforme a lo determinado para el responsable.

Art. 66.- Contratación.- El encargado del tratamiento podrá contratar a un tercero para la prestación de un servicio al responsable del tratamiento de datos personales siempre que:

a) Cuente con la autorización escrita del responsable del tratamiento; o,
b) Que se lo haga constar expresamente en el contrato celebrado entre el responsable y el encargado de tratamiento o conste en las instrucciones emitidas por el responsable.

La contratación se hará siempre en nombre y por cuenta del responsable del tratamiento.

Art. 67.- El encargado deberá devolver o suprimir todos los datos personales, según las instrucciones impartidas por el responsable del tratamiento, una vez finalizada la relación que justifica el tratamiento de datos personales, destruyendo todas copias existentes, salvo que exista la obligación de conservar los datos en virtud de una disposición legal.

Art. 68.- El encargado de tratamiento deberá permitir al responsable o a la persona determinada por éste, en cualquier momento que así lo solicite el responsable, la revisión de los registros y procesos que tengan relación con los tratamientos de datos personales encomendados, a fin de verificar el correcto cumplimiento del contrato y las obligaciones de la Ley y el presente Reglamento, así como la adopción de medidas técnicas, organizativas y de seguridad adecuadas.

En tal sentido, el encargado deberá proporcionar al responsable o a su auditor toda la información necesaria, en particular los registros de datos personales, para demostrar el cumplimiento de sus obligaciones y dar todas las facilidades del caso.

CAPÍTULO III
DELEGADO DE PROTECCIÓN DE DATOS

Art. 69.- Delegado de protección de datos.- 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 encargado en materia de protección de datos personales.

Podrá realizar otras actividades relacionadas con la protección de datos personales, que les 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 encargado, quienes estarán compelidos a facilitar la asistencia, recursos y elementos que les sea oportunamente requeridos para garantizar que el cumplimiento de los deberes y responsabilidades a cargo del delegado, y a cumplir las recomendaciones relativas al cumplimiento de la normativa sobre protección de datos personales.

Sin perjuicio de lo que disponga la Ley y este Reglamento, corresponderá a la Superintendencia 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.

Art. 70.- El delegado de protección de datos podrá ser contratado por el responsable bajo relación de dependencia o a través de un contrato de prestación de servicios, sin perjuicio de lo cual, en cualquiera de los casos, deberá respetar y garantizar que se presten los servicios de manera independiente.

Art.- 71.- Un grupo de empresas puede designar a un único delegado de protección de datos personales, en la medida en que pueda ejecutar sus actividades.

Art. 72.- El responsable y encargado no podrán remover al delegado de protección de datos personales, así como aplicar sanciones por el hecho de desempeñar y cumplir sus funciones. En caso que el delegado removido o sancionado considerare que su desvinculación o sanción se ha dado por cumplir con sus funciones, podrá poner este hecho en conocimiento de la Superintendencia de Protección de Datos Personales, que valorará las circunstancias en las que la desvinculación o sanción se produjo y podrá aplicar las sanciones correspondientes.

Art. 73.- Deberán designar delegado de protección de datos personales las personas naturales o jurídicas, públicas o privadas, a las que la Ley les imponga dicha obligación.

Sin perjuicio de lo anterior, los responsables o encargados de tratamiento que no se encuentren dentro de las categorías de obligados a designar un delegado de protección de datos, podrán hacerlo de manera voluntaria como un mecanismo de buena práctica y como parte de las medidas de responsabilidad proactiva a adoptar.

En atención a sus necesidades institucionales, además del delegado principal, los responsables y encargados podrán designar un suplente, que actuará en caso de ausencia o impedimento temporal o definitivo del primero.

Art. 74.- Actividades de control permanente y sistematizado de datos.- Para determinar si las actividades de un responsable o encargado en materia de protección de datos requieren de un control permanente, se deberá considerar, entre otros factores que defina la Superintendencia de Protección de Datos Personales, los siguientes:

1. Si el tratamiento de datos es continuado o si se produce en intervalos concretos durante un periodo de tiempo.

2. Si el tratamiento de datos es recurrente o repetido en momentos prefijados.

3. Si el tratamiento tiene lugar de manera constante o periódica. Por su parte, para determinar si el control es sistematizado, se deberá verificar los siguientes supuestos, sin perjuicio de aquellos que determine el Superintendente:

1. Si el tratamiento de datos se produce de acuerdo con un sistema.

2. Si el tratamiento de datos está de alguna manera preestablecido, organizado o es metódico.

3. Si el tratamiento de datos tiene lugar como parte de un plan general de recogida de datos.

4. Si el tratamiento de datos es llevado a cabo como parte de una estrategia.

En caso de suscitarse dudas entre los responsables y encargados respecto a los supuestos que dan lugar a la designación del delegado de protección de datos personales, podrán dirigir sus respectivas consultas a la Superintendencia de Protección de Datos Personales, cuya decisión será de cumplimiento obligatorio para los consultantes.

Art. 75.- Tratamiento a gran escala de categorías especiales de datos.- Para determinar si un tratamiento de datos personales se produce a gran escala, se deberá considerar, entre otros factores que defina el Superintendente de Protección de Datos Personales, los siguientes:

1. El número de titulares de datos personales afectados;
2. El volumen de datos o la variedad de datos que son objeto de tratamiento;
3. La duración o permanencia de la actividad del tratamiento;

4. El alcance geográfico de la actividad del tratamiento; y,

Art. 76- Requisitos para ser delegado.- Para ser delegado de protección de datos personales, la persona natural deberá cumplir los siguientes requisitos, sin perjuicio de otros más que disponga el Superintendente de Protección de Datos Personales mediante normativa secundaria:

1. Estar en pleno goce de sus derechos civiles y políticos.

2. Ser mayor de edad.

3. Acreditar título de tercer nivel,

4. Acreditar conocimientos especializados en protección de datos personales, lo cual podrá ser demostrado a través de mecanismos de certificación.

Art. 77.- Impedimento para ser delegado.- No podrán ser delegados de protección de datos personales las siguientes personas naturales, sin perjuicio de otras que defina la Superintendencia de Protección de Datos Personales:

1. Las personas naturales que formen parte de los órganos de administración y control del responsable y encargado.

2. Los socios o accionistas del responsable y encargado.

3. Los cónyuges de los administradores, directores o comisarios de la compañía, en caso de haberlos, del responsable y encargado, o sus parientes hasta el cuarto grado de consanguinidad o segundo de afinidad.

4. Los que tengan conflicto de intereses con el responsable y encargado.

Tratándose de instituciones del sector público, la Superintendencia Protección de Datos Personales definirá las incompatibilidades para ejercer el cargo de delegado de protección de datos personales para cada caso en particular.

Art. 78.- El delegado de protección de datos personales podrá formar parte de la estructura orgánica del responsable o encargado, o bien, podrá ser contratado como asesor externo, en cuyo caso su contratación se regulará por el derecho civil y tratándose de instituciones públicas, por las normas que regulan la contratación pública, y, además, para ambos casos, por la Ley Orgánica de Protección de Datos Personales, este Reglamento y la normativa que emita la Superintendencia de Protección de Datos Personales..

La relación jurídica de vinculación entre el delegado y el responsable o encargado, cualquiera que esta fuese, deberá garantizar la objetividad e independencia del delegado para el adecuado desempeño de sus funciones.

El documento de designación recogerá los términos y condiciones que libremente decidan las partes, respetando los preceptos de la Ley, este Reglamento y aquellos que emita por normativa que emita la Superintendencia de Protección de Datos Personales.

Art. 79.- Prestación de servicios a diversos responsables o encargados.- El delegado de protección de datos personales podrá prestar sus servicios a uno o varios responsables o encargados siempre que al hacerlo no incurra en un conflicto de intereses, o bien, resulte en menoscabo del adecuado desempeño de sus funciones.

Art. 80.- Acuerdos de Confidencialidad.- Si el responsable o encargado lo estimaren necesario, podrán exigir que el delegado de protección de datos personales suscriba un acuerdo de confidencialidad respecto de la información que llegase a conocer o respecto de la cual puedan llegar a tener acceso por el desempeño de su cargo. Las partes acordarán libremente los términos y condiciones del acuerdo, pero en ningún caso tales documentos podrán limitar el acceso del delegado a la información que estime necesaria para el desempeño de su función.

Aún en caso de no requerirse la suscripción de acuerdo de confidencialidad, el delegado de protección de datos personales es responsable de guardar el debido sigilo respecto de la información que tuviere conocimiento, y no podrá usarla o reproducirla en forma alguna, bajo las responsabilidades civiles y penales a las que hubiere lugar.

Este deber de guardar confidencialidad subsistirá incluso una vez que haya concluido la relación jurídica con el responsable o encargado.

TÍTULO VI
DE LA RESPONSABILIDAD PROACTIVA

CAPÍTULO I
EXIGENCIA DE RESPONSABILIDAD PROACTIVA Y DEMOSTRABLE

Art.- 81.- El responsable del tratamiento está obligado a aplicar medidas técnicas y organizativas apropiadas, a fin de garantizar y poder demostrar que el tratamiento de datos que realiza es conforme con la normativa, atendiendo:

1) A la naturaleza
2) Al ámbito
3) A la finalidad del tratamiento
4) A los riesgos, sobre la base de una evaluación objetiva que determine si las operaciones de tratamiento de datos suponen riesgo o si el riesgo es alto.

Este principio implica también revisar y actualizar las medidas cuando sea necesario.

Art. 82.- Medidas de protección de datos desde el diseño: El responsable del tratamiento tiene la obligación de establecer medidas técnicas y organizativas adecuadas para aplicar los principios señalados en la normativa de forma eficaz y proteger así los derechos de los titulares, de manera previa al tratamiento de datos personales.

Para la fijación de estas medidas debe tenerse en cuenta:

a) La naturaleza, ámbito y finalidad del tratamiento
b) Los riesgos de diversa probabilidad y gravedad

c) El estado de la técnica
d) El coste de aplicación

Art. 83.- Medidas de protección de datos por defecto: El responsable del tratamiento adoptará las medidas técnicas y organizativas apropiadas para garantizar que, mediante ajustes, por defecto sólo puedan tratarse, en principio, aquellos datos personales cuyo tratamiento sea necesario para la respectiva finalidad específica del tratamiento. Esto se refiere a la cantidad de datos recogidos, el alcance de su tratamiento, su período de almacenamiento y su accesibilidad. Además, mediante los respectivos ajustes, las medidas deben garantizar que, por defecto, los datos no puedan ser accesibles a un número indefinido de personas de forma automatizada.

Esta obligación se debe extender:

a) A la cantidad de los datos recopilados
b) A la extensión del tratamiento
c) Al periodo de almacenamiento
d) A la accesibilidad

Para acreditar el cumplimiento de esta medida, podrá utilizarse un mecanismo de certificación, tal y como autoriza la Ley Orgánica de Protección de Datos Personales.

CAPITULO II
DE LOS MECANISMOS DE AUTORREGULACIÓN

Art. 84.- Mecanismos de autorregulación.- Los mecanismos de autorregulación pueden ser adoptados para el cumplimiento de los principios, ejercicio de derechos, medidas de seguridad, transferencias, procedimientos y, en general, para cumplir cualquiera de los deberes previstos en la Ley Orgánica de Protección de Datos Personales, este Reglamento demás normativa aplicable y el estado de la técnica en materia de protección de datos, seguridad de la información y ciberseguridad

Los mecanismos de autorregulación constituyen instrumentos que permiten adecuar de mejor forma esquemas de cumplimiento para sectores específicos o en situaciones muy particulares y dar cumplimiento a la Ley Orgánica de Protección de Datos y demás normativa aplicable.

Art. 85.- Mecanismos de autorregulación.- Serán mecanismos de autorregulación los siguientes:

1. Esquemas certificados en materia de protección de datos personales por el Servicio Ecuatoriano de Acreditación.

2. Reglas específicas, creadas para adaptar la normativa de protección datos personales a un determinado sector o situación. En este tipo de reglas estarán comprendidos los códigos de conducta, las normas corporativas vinculantes y las cláusulas tipo.

3. Esquemas validados por la Superintendencia de Protección de Datos Personales conforme a las reglas que para tal efecto emita.

Art. 86.- Registro de mecanismos de autorregulación.- Se crea el registro de mecanismos de autorregulación con la finalidad de dar a conocer la siguiente información:

1. Las reglas destinadas a adaptar la normativa de datos personales para determinado sector o situación con la finalidad de facilitar y hacer efectivo su cumplimiento;

2. Las entidades de acreditación autorizadas por el Servicio Ecuatoriano de Acreditación en materia de protección de datos personales;

3. Las entidades de evaluación acreditadas para otorgar certificaciones en materia de protección de datos personales por el Servicio Ecuatoriano de Acreditación, en el marco de la Ley, este Reglamento y las reglas que se emitan para el efecto; y,

4. Los responsables y encargados que se hayan adherido a algún mecanismo o estándar de calidad de seguridad de la información ya sea este de facto, una versión actualizada al estado de la técnica o alguna certificación internacional utilizada en su organización o grupo empresarial.

Art. 87.- Administración y regulación del registro de mecanismos de autorregulación.- El registro de mecanismo de autorregulación estará a cargo de la Superintendencia de Protección de Datos Personales la cual emitirá las reglas para su creación y funcionamiento.

SECCIÓN I
DE LA CERTIFICACIÓN

Art. 88.- Objeto de la certificación.- La certificación tiene por objeto determinar el grado de cumplimiento de un mecanismo de autorregulación con relación a las obligaciones de la Ley Orgánica de Protección de Datos Personales, este Reglamento y demás normativa aplicable.

Corresponderá privativamente a Superintendencia de Protección de Datos Personales emitir y actualizar periódicamente los parámetros básicos o estándares mínimos de evaluación necesarios a los que deberán someterse los responsables y encargados para obtener la certificación a la que se refiere este capítulo.

Art. 89.- Temporalidad de la certificación.- La certificación se expedirá por un periodo máximo de tres años, vencido el cual podrá ser renovada en las mismas condiciones, siempre y cuando se cumplan los requisitos establecidos para el efecto.

Art. 90.- Entidades de certificación.- La certificación en materia de protección de datos estará a cargo de las entidades de certificación acreditadas por el Servicio Ecuatoriano de Acreditación, de conformidad con la normativa que para el efecto emitan en conjunto la Superintendencia de Protección de Datos Personales y la Autoridad Nacional de Acreditación.

Para la acreditación de la entidad de certificación se revisará el cumplimiento, entre otros, los siguientes requisitos:

a) Haber demostrado su independencia y pericia en relación con el objeto de la certificación;
b) Haber establecido procedimientos adecuados para la expedición, la revisión periódica y la retirada de sellos y certificaciones de cumplimiento en materia de protección de datos;
c) Haber demostrado que sus funciones y cometidos no dan lugar a conflictos de intereses.

Para la aprobación de las Entidades Certificadoras se deberá de tener en cuenta, además, el cumplimiento por parte de estas entidades de normas internacionales como la ISO/IEC 17065 relativa a los requisitos para organismos que certifican productos, procesos y servicios.

Art. 91.- Cuando el responsable o encargado de tratamiento dejen de cumplir con los requisitos que dieron paso al otorgamiento de la certificación, ésta podrá ser revocada por el mismo organismo de certificación que la otorgó o por la autoridad de control competente.

SECCIÓN II
DE LOS CÓDIGOS DE CONDUCTA

Art. 92.- Cualquier persona natural o jurídica podrá presentar códigos de conducta que tengan como fin el cumplimiento de la normativa vigente en materia de protección de datos personales.

Los códigos de conducta deberán contener al menos los siguientes requisitos:

1. Exposición de motivos clara y concisa, que describa detalladamente el objetivo del código, su ámbito de aplicación y cómo facilitará la aplicación efectiva de la Ley y este Reglamento.

2. Ámbito de aplicación definido que determine de forma clara y precisa las operaciones de tratamiento (o las características del tratamiento) de datos personales que abarca, así como las categorías de responsables o encargados del tratamiento a las que se aplica. Esto incluirá las cuestiones del tratamiento que pretenda abordar el código y aportará soluciones prácticas.

3. Mecanismos de supervisión para controlar el pleno cumplimiento de sus disposiciones.

Art. 93.- Admisibilidad.- El proponente del código presentará formalmente su proyecto de código, ya sea en formato electrónico o físico a la Superintendencia de Protección de Datos Personales.

Presentado el proyecto de código, la Superintendencia de Protección de Datos Personales, en el término máximo de cinco (5) días, examinará si cumple los criterios de admisibilidad, antes de proceder a una evaluación completa de su contenido.

Si los cumple, calificará, tramitará y dispondrá la evaluación del contenido del proyecto de código. Si el proyecto no cumple con los requisitos formales previstos en el artículo 92, la Superintendencia de Protección de Datos Personales dispondrá que el proponente la complete o aclare en el término de cinco (5) días, determinando explícitamente el o los defectos. Si no lo hace, ordenará el archivo y la devolución del proyecto, sin necesidad de dejar copias. No se ordenará el archivo si el proponente aclaró o completó en el término legal previsto en este artículo.

Art. 94.- Evaluación del fondo.- Admitido el proyecto de código, la Superintendencia de Protección de Datos Personales, deberá en el plazo de un (1) mes ejecutar una evaluación integral del mismo, en la cual incluye verificar que el código contribuya a la correcta aplicación de la Ley, el presente Reglamento y la normativa aplicable en materia de protección de datos, teniendo en cuenta las características específicas de los diversos sectores del tratamiento, así como las obligaciones y los requisitos concretos de los responsables o encargados del tratamiento a los que se aplique.

Además de los criterios que determine la Superintendencia de Protección de Datos Personales para la aprobación de los Códigos de Conducta, se verificara que el proyecto cumpla los siguientes criterios:

1.- Satisface una necesidad específica de ese sector o actividad de tratamiento.- el código debe abordar cuestiones relacionadas con la protección de datos que surjan para un sector o actividad de tratamiento en concreto.

2.- Especificar la aplicación de la Ley y el Reglamento.- Es necesario que los códigos especifiquen la aplicación práctica de la Ley, el presente Reglamento y la normativa que emita la Superintendencia de Protección de Datos Personales y que reflejen de forma precisa la naturaleza de la actividad o el sector del tratamiento. Deben poder aportar mejoras claras y específicas del sector en cuanto al cumplimiento de la legislación en materia de protección de

datos. Deben establecer normas realistas y asequibles para todos sus miembros y deben contar con la calidad y coherencia interna necesarias para aportar suficiente valor añadido

El código no debe limitarse a repetir los preceptos de la Ley, y el presente Reglamento, sino que debe codificar cómo ha de aplicarse dicha normativa de forma específica, práctica y precisa. Las normas y reglas acordadas deberán ser inequívocas, concretas, asequibles y aplicables.

3.- Aporta garantías suficientes.- el código de conducta debe contar con las garantías suficientes y eficaces para mitigar el riesgo que entraña el tratamiento de datos y para respetar los derechos y las libertades de los particulares, para ello, se deberá adjuntar los medios de prueba suficientes que demuestren que el código cumplirá estos requisitos

4.- Dispone de mecanismos eficaces para supervisar el cumplimiento del código.- el código debe contener mecanismos adecuados para garantizar que se supervisan correctamente las normas y que existen medidas de ejecución eficaces y significativas para garantizar su pleno cumplimiento.

Deberá identificar y proponer específicamente las estructuras y procedimientos que velen por una supervisión eficaz y una sanción de las infracciones. Asimismo, el proyecto de código debe designar un órgano adecuado que disponga de mecanismos que le permitan velar por la supervisión eficaz del cumplimiento del código.

Los citados mecanismos pueden incluir una auditoría periódica y requisitos de presentación de informes, la gestión clara y transparente de las reclamaciones y los procedimientos de solución de litigios, sanciones específicas y medidas correctivas en caso de infracción del código, así como mecanismos para denunciar las infracciones de sus disposiciones.

SECCIÓN III
DE LAS AUDITORIAS

Art. 95.- De las Auditorías voluntarias.- Son un mecanismo preventivo de carácter voluntario que tiene por finalidad corroborar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados por el responsable o encargado para el cumplimiento de las disposiciones previstas en la Ley, el Reglamento y demás normativa aplicable.

Las auditorías voluntarias deberán ser llevadas a cabo por personas naturales o jurídicas, públicas o privadas, especializadas en actividades de supervisión o auditoria de datos personales, previamente calificadas por la Superintendencia de Protección de Datos Personales de conformidad a las normas, requisitos y procedimientos que ésta determine para el efecto.

El informe de auditoría dictaminará acerca de la adecuación de las medidas y controles implementados por los responsables y encargados, identificará las áreas de oportunidad y mejora y formulará las recomendaciones a que hubiere lugar.

Art. 96.- La adhesión a un código de conducta, certificaciones, sellos y marcas de protección, clausulas tipo, será considerada como una circunstancia atenuante de la responsabilidad administrativa.

TITULO VII
DE LAS TRASNFERENCIA O COMUNICACIÓN INTERNACIONAL DE DATOS

Art. 97.- Régimen de transferencias internacionales.- Se podrán realizar transferencias internacionales o transfronterizas de datos a terceros países, organizaciones o territorios económicos internacionales, en los siguientes supuestos:

1. Cuando el país, organización o territorio económico internacional cumpla con un nivel adecuado de protección de datos personales, conforme a la normativa ecuatoriana;

2. Si no se observa lo anterior, cuando se ofrezca garantías adecuadas al titular, según lo determinado en la Ley y el presente Reglamento.

3. Si no se observa lo anterior, cuando se presente alguno de los casos excepcionales del artículo 60 de la Ley, para lo cual no se requerirá autorización por parte de la Superintendencia de Protección de Datos Personales

4. Si no se observa ninguno de los supuestos anteriores, cuando la Superintendencia de Protección de Datos Personales autorice la transferencia internacional de datos, según lo previsto en la Ley y el presente Reglamento.

La declaración de adecuación de un país, territorio u organización internacional tendrá efectos generales, por lo que las transferencias internacionales hacia ese país, territorio u organización internacional se podrán realizar libremente.

Las garantías adecuadas, los casos excepcionales y las autorizaciones que emita la Superintendencia de Protección de Datos Personales, producirán efectos individuales únicamente respecto de los responsables que adopten alguna de las garantías adecuadas, invoquen un caso excepcional u obtengan la autorización para cada operación de transferencia de datos.

Art. 98.- Declaratoria de nivel adecuado.- Las transferencias de datos personales hacia los países, organizaciones o territorios económicos internacionales, que a criterio de la Superintendencia de Protección de Datos Personales cuenten con un nivel adecuado de protección de datos, no requerirán de autorización previa.

Art. 99.- Resolución.- La Superintendencia de Protección de Datos Personales, mediante resolución motivada, indicará los países, organizaciones o territorios económicos internacionales que se considera cuentan con adecuados niveles de protección para transferirles o comunicarles datos personales, para lo cual, la autoridad de control revisará que los estándares de protección sean equivalentes o superiores a aquellos que plantea la normativa ecuatoriana vigente.

La Superintendencia de Protección de Datos Personales publicará su resolución en el Registro Oficial y por medios digitales, y mantendrá un registro, disponible al público, con el listado de países, territorios y organizaciones internacionales que hayan sido reconocidos con adecuados niveles de protección.

En la resolución respectiva, la Superintendencia de Protección de Datos Personales establecerá el mecanismo de revisión periódica de los niveles adecuados de protección, que deberá llevarse a cabo, al menos, cada tres años.

En caso de que no exista un pronunciamiento al respecto por parte de la autoridad de control, el interesado podrá presentar una solicitud de consulta a ella, a fin de que la Superintendencia de Protección de Datos Personales se pronuncie al respecto y determine el nivel adecuado o no del país, organización o territorio económico internacional de destino.

La falta de pronunciamiento por parte de la Superintendencia de Protección de Datos Personales implicará que no se podrán realizar transferencias internacionales amparado en niveles adecuados de protección.

Art. 100.- Parámetros mínimos para análisis de nivel adecuado de protección.- Para determinar si un país, organización o territorio económico internacional posee un nivel adecuado de protección de datos se tendrán en cuenta los siguientes criterios, sin perjuicio de otros más que pueda definir la Superintendencia de Protección de Datos Personales:

1. La legislación nacional y normativa sectorial del país, que tenga incidencia en materia de protección de datos personales;

2. La legislación en materia de seguridad nacional, pública y, en general, aquella que tenga relación con la defensa y seguridad del Estado, así como la legislación penal. En estas materias se deberá poner especial énfasis en la revisión de las disposiciones que habiliten el acceso a datos personales por parte de las autoridades de ese país, territorio u organización internacional;

3. La normativa sobre transferencias ulteriores de datos personales a destinatarios en terceros países, organizaciones o territorios económicos internacionales;

4. La jurisprudencia vinculada a la protección de datos personales;

5. El reconocimiento de derechos y los mecanismos de ejercicio de los mismos a favor de los titulares de datos personales;

6. El establecimiento de deberes y obligaciones de responsables y encargados en el marco del tratamiento de datos personales;

7. La existencia de mecanismos legales efectivos que permitan el cumplimiento y la observancia de los derechos de protección de datos personales a favor de los titulares;

8. La existencia de una Superintendencia de Protección de Datos Personales que sea independiente y que tenga competencias de control y vigilancia del cumplimiento de la normativa en materia protección de datos personales, así como de sanción en caso del cometimiento de infracciones en esta materia. Además, deberá brindar asistencia y asesoría a los titulares y cooperación internacional con otras autoridades; y,

9. Los compromisos internacionales asumidos por el país, organización o territorio económico internacional en cuanto a la materia de protección de datos personales.

Art. 101.- Control continuo.- La Superintendencia de Protección de Datos Personales realizará una revisión periódica de los niveles adecuados de protección de países, territorios y organizaciones internacionales.

En el caso de que la autoridad identifique, en cualquier momento, que algún país, organización o territorio económico internacional ha dejado de cumplir los parámetros de niveles adecuados de protección, dictará una resolución en la que se deje sin efectos, modifique o suspenda, la resolución por la que se reconoció con un adecuado nivel de protección al país, organización o territorio económico internacional, sin que este acto tenga efectos retroactivos.

Art. 102.- Los instrumentos jurídicos a los que se refiere el artículo 57 de la Ley para justificar el cumplimiento de las garantías adecuadas para realizar transferencias internacionales de datos serán, entre otros, los siguientes:

a) Instrumentos jurídicamente vinculantes y exigibles entre las autoridades u organismos públicos;
b) Normas corporativas vinculantes aprobadas por la Superintendencia de Protección de Datos Personales;

c) Cláusulas tipo de protección de datos adoptadas por organismos internacionales de protección de datos avaladas por la autoridad de control;
d) Códigos de conducta, que incluyan compromisos vinculantes del responsable o el encargado del tratamiento en el tercer país, organización o territorio económico internacional de aplicar garantías adecuadas, que incluya las relativas a los derechos de los interesados;
e) Mecanismos de certificación, que incluyen sellos y marcas de protección, que incorporen compromisos vinculantes del responsable o el encargado del tratamiento en el tercer país, organización o territorio económico internacional de aplicar garantías adecuadas, así como aquellos relativos a los derechos de los interesados; y
f) Cláusulas contractuales que no correspondan a las cláusulas tipo y que estén debidamente autorizadas por la Superintendencia de Protección de Datos Personales.

Art. 103.-Normas corporativas vinculantes.- Son normas corporativas vinculantes las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en la República del Ecuador para realizar transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta.

Art. 104.- Todo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta tendrá la posibilidad de invocar normas corporativas vinculantes autorizadas para sus transferencias internacionales de datos a terceros países, siempre que tales normas corporativas incorporen todos los principios de tratamiento de datos personales y derechos aplicables; y garantías de seguridad adecuadas para las transferencias de datos de personales.

Art. 105.- Las normas corporativas vinculantes, para que constituyan garantías adecuadas de protección, deberán ser autorizadas por la Superintendencia de Protección de Datos Personales.

Para ello, la Superintendencia de Protección de Datos Personales deberá observar que las normas corporativas vinculantes cumplan los siguientes requisitos:

a) Sean jurídicamente vinculantes;
b) Confieran expresamente a los titulares derechos exigibles en relación con el tratamiento de sus datos personales; y,
c) Cumplan con los requisitos establecidos en el artículo 58 de la ley.

Art. 106.- Autorización previa para la transferencia o comunicación internacional.- La Superintendencia de Protección de Datos Personales autorizará con carácter previo la transferencia o comunicación internacional de datos personales en todos aquellos casos no contemplados en los artículos precedentes, para lo cual dictará la normativa pertinente en atención a la naturaleza de los datos personales que desean transferirse o comunicarse al exterior y al lugar o destinario de los mismos.

Para que la Superintendencia de Protección de Datos Personales autorice con carácter previo una operación de transferencia internacional de datos personales, resultará indispensable que el responsable cumpla, al menos, con los siguientes supuestos:

1. Que el destinatario se obligue, voluntaria y formalmente, a cumplir con la Ley, el Reglamento y demás normativa aplicable, así como a aceptar la autoridad y competencia de la Superintendencia de Protección de Datos Personales y de los tribunales ecuatorianos, para cualquier efecto a que haya lugar con motivo del tratamiento de los datos objeto de la transferencia; o,

2. Que el destinatario se obligue, voluntaria y formalmente, a cumplir con la Ley, el Reglamento y demás normativa aplicable, y que en el país o territorio donde se encuentre establecido el

destinatario se garantice el ejercicio de los derechos, incluido el derecho a presentar una reclamación ante una Superintendencia de Protección de Datos Personales y el derecho a la tutela judicial efectiva, por parte de los titulares.

En términos de lo establecido en los artículos 59, 61, último párrafo y 76, numerales 8) y 10) de la Ley, la Superintendencia de Protección de Datos Personales pondrá a disposición del público información sobre los países, territorios u organizaciones que garantizan los derechos de los titulares y que cuentan con acciones legales efectivas ante una Superintendencia de Protección de Datos Personales y los tribunales para hacer valer sus derechos.

Art. 107.- Inscripción de información sobre transferencias internacionales en el Registro Nacional de Protección de Datos.- En el Registro Nacional de Protección de Datos se inscribirá la siguiente información:

1. El país, territorio u organización internacional donde se ubica el destinatario de los datos;
2. Las categorías de datos objeto de la transferencia;
3. Las finalidades de la transferencia;
4. El nombre, denominación, razón social o nombre comercial con el que se identifique al destinatario.
5. El mecanismo o esquema autorizado, conforme a la Ley y el Reglamento, para realizar la transferencia;
6. El supuesto de excepción que se haya utilizado de los previstos en el artículo 60 de la Ley, en su caso

La Superintendencia de Protección de Datos Personales privilegiará la utilización de medios digitales para la inscripción de la información descrita, y emitirá las reglas conforme a las cuales se hará el registro de la información, los medios disponibles para el registro, los plazos, así como los mecanismos para la actualización de dicha información, en su caso.

TITULO VIII
DE LA SUPERINTENDENCIA DE PROTECCIÓN DE DATOS PERSONALES

Art. 108.- Superintendencia de Protección de Datos Personales.- Es la Autoridad Nacional de Protección de Datos Personales. Para el cumplimiento de sus fines, goza de autonomía administrativa, técnica, operativa y financiera. Estará a cargo del Superintendente de Protección de Datos Personales.

Tendrá su sede en la ciudad de Quito.

Para el ejercicio de la administración desconcentrada, la Superintendencia de Protección de Datos Personales podrá establecer las oficinas que fueren necesarias a nivel nacional, a cargo de Intendencias con atribuciones expresamente delegadas por el Superintendente de Protección de Datos Personales.

El Superintendente de Protección de Datos Personales aprobará el Estatuto Orgánico Funcional, que contendrá la estructura orgánica de la Superintendencia de Protección de Datos Personales, la misma que estará integrada por las unidades administrativas que fueren necesarias para el cumplimiento de sus fines y atribuciones.

Art. 109.- Atribuciones.- La Superintendencia de Protección de Datos Personales, además de las señaladas en la Ley de la materia, tendrá las siguientes:

1. Hacer cumplir las regulaciones que dicte en el marco de la protección de datos personales;

2. Registrar las bases de datos y ficheros que contengan datos personales en el Registro Nacional de Protección de Datos Personales;

3. Dirigir y administrar el Registro Único de Responsables y Encargados Incumplidos;

4. Emitir regulaciones para la protección de datos personales;

5. Emitir los informes técnicos dentro de los mecanismos de control y supervisión que se dispongan;

6. Ejecutar análisis y proponer propuestas normativas que garanticen la mejora del marco regulatorio de aplicación de la Ley;

7. Emitir guías de referencias que ayuden a los responsables y encargados del tratamiento de datos en el proceso de adecuación y cumplimiento de la normativa de protección de datos personales;

8. Conocer y resolver las peticiones, quejas, reclamos y recursos que se propongan en el ámbito de su competencia y de conformidad con la Ley; y,

9. Las demás que se le asignen en este Reglamento.

Art. 110.- Planes anuales.- La Superintendencia de Protección de Datos Personales ejercerá sus atribuciones de control en base a planes anuales, que se elaborarán considerando la naturaleza de las organizaciones controladas, el volumen y la sensibilidad de los datos personales sujetos a tratamiento, la aplicación de los diferentes procedimientos de control y la disponibilidad presupuestaria.

Se podrán ejecutar procedimientos de control no considerados dentro de los planes anuales, si la situación lo amerite, basados en criterios de criticidad, oportunidad y posibles lesiones al derecho a la protección de datos personales de uno o más titulares de datos personales.

Art. 111.- Mecanismos de control.- La Superintendencia de Protección de Datos Personales determinara los procedimientos de control.

Los procedimientos de control se regirán por las reglas previstas en el Código Orgánico Administrativo.

Art. 112.- Funciones y Atribuciones del Superintendente de Protección de Datos Personales.- Son funciones del Superintendente de Protección de Datos Personales, a más de las señaladas en la Ley y este Reglamento, las siguientes:

1. Representar legal y judicialmente a la Superintendencia de Protección de Datos Personales, en todos los actos, contratos y relaciones jurídicas sujetas a su competencia.

2. Elaborar y publicar, anualmente, información estadística, de las organizaciones sujetas a su control y de los tratamientos de datos personales.

3. Formular, aprobar y ejecutar el presupuesto de la Superintendencia de Protección de Datos Personales.

4. Preparar estudios y propuestas sobre reformas legales y reglamentarias que se requieran para el correcto ejercicio del derecho a la protección de datos personales, y ponerlos en consideración de los órganos encargados de aprobarlas.

5. Aprobar y expedir normas internas, reglamentos y manuales que sean necesarios para el buen funcionamiento de la Superintendencia a su cargo.

Art. 113.- Registro Nacional de Protección de Datos Personales.- El Registro Nacional de Protección de Datos Personales constituye un registro público a cargo de la Superintendencia de Protección de Datos Personales, que registra las bases de datos, ficheros o tratamientos de datos personales realizados por responsables de tratamiento de datos personales en los términos previstos en la Ley.

Serán objeto de inscripción en el Registro Nacional de Protección de Datos Personales, las bases de datos o ficheros que contengan datos personales, que sean utilizados para el tratamiento de estos, en cualquier tipo de soporte, automatizados o no, así como a toda modalidad de uso posterior que sea realizado por personas naturales o jurídicas, de naturaleza pública o privada, en el territorio ecuatoriano o fuera de él, en los términos previstos en los artículos 2 y 3 de la Ley Orgánica de Protección de Datos Personales, y sus actualizaciones.

Art1. 114.- Responsabilidad del registro.- El responsable del tratamiento de datos personales debe inscribir en el Registro Nacional de Protección de Datos Personales cada una de las bases de datos o ficheros que contengan datos personales sujetos a tratamiento.

El registro se realizará de manera independiente por cada base de datos o fichero.

La Superintendencia de Protección de Datos Personales regulará los procesos de inscripción y actualización en el Registro Nacional de Protección de Datos Personales a su cargo que deberán cumplir los responsables de tratamiento de datos personales.

Art. 115.- Inscripción oportuna.- El registro de bases de datos o ficheros en el Registro Nacional de Protección de Datos Personales deberá realizarse dentro del término de diez (10) días contados a partir del día siguiente al inicio del tratamiento.

Art. 116.- Registro Único de Responsables y Encargados del Tratamiento Incumplidos.- El Registro Único de Responsables y Encargados Incumplidos constituye un registro público a cargo de la Superintendencia de Protección de Datos, en el que se harán constar los Responsables y Encargados del Tratamiento que hubieren incurrido en alguna de las infracciones establecidas en la Ley Orgánica de Protección de Datos Personales y cuenten con una resolución o sentencia en firme, de conformidad con lo dispuesto en el ordenamiento jurídico vigente.

Dicho registro contendrá los siguientes datos:

a) Nombre de la persona natural o jurídica infractora.
b) Indicación de la infracción cometida.
c) Indicación de la sanción impuesta.
d) Reiteración o reincidencias en el cometimiento de infracciones.

Art. 117.- El presente registro será utilizado exclusivamente para fines estadísticos, preventivos y de capacitación

La Superintendencia de Protección de Datos Personales guardará la confidencialidad y privacidad de los datos contenidos en el Registro y aplicará las medidas de seguridad a fin de proteger la información personal contenida en el mismo.

La Superintendencia de Protección de Datos Personales mantendrá permanentemente actualizado el Registro, de tal forma que responda con veracidad y exactitud a los datos contenidos en el mismo.

Art. 118.-El plazo máximo de conservación de los datos contenidos en el Registro de Responsables y Encargados del Tratamiento Incumplidos es de cinco (5) años contados desde la fecha de la emisión de la resolución o sentencia en firme.

Art. 119.- Si del procedimiento de control realizado se determinare el incumplimiento de la Ley Orgánica de Protección de Datos Personales, su Reglamento o la normativa aplicable en materia de protección de datos, se iniciará el correspondiente procedimiento administrativo sancionatorio, conforme a las disposiciones establecidas en el Código Orgánico Administrativo.

Art. 120.- De determinarse responsabilidades, la Superintendencia de Protección de Datos Personales, emitirá la correspondiente resolución sancionatoria, la cual deberá encontrarse debidamente fundada y motivada, debiendo considerar al menos lo siguiente:

1. El impacto de la infracción, tomando en cuenta la naturaleza, gravedad y duración de la infracción, considerando la legalidad del tratamiento de los datos, el número de personas concernidas afectadas y el nivel de daños y perjuicios que hayan sufrido.

2. Los siguientes atenuantes y agravantes:

    2.1. La naturaleza del dato.
    2.2. La notoria improcedencia de la negativa del responsable, para realizar los actos solicitados por el titular, en términos de la Ley.
    2.3. El carácter intencional o no, de la acción u omisión constitutiva de la infracción.
    2.4. La capacidad económica del responsable.
    2.5. La reincidencia

Art. 121.- Las sanciones a las que hubiere lugar se impondrán sin perjuicio de la responsabilidad civil o penal que resulten del cometimiento de la infracción.

DISPOSICIÓN GENERAL

ÚNICA.- En el plazo de un (1) año contado a partir de la fecha de publicación de este Reglamento en el Registro Oficial, la Superintendencia de Protección de Datos Personales coordinará y llevará a cabo capacitaciones técnicas y cursos de formación dirigidos al público en general, orientados a promover el ejercicio del derecho a la protección de datos personales y a la profesionalización de los delegados de protección de datos personales.

DISPOSICIÓN FINAL

El presente Reglamento entrará en vigencia en el plazo de dos meses a partir de su publicación en el Registro Oficial.

Dado en el Distrito Metropolitano de Quito, el XX de diciembre de 2022.