LOPDP- ECUADOR

RESUMEN LEY ORGÁNICA DE PROTECCION DE DATOS PERSONALES

ONETHYCA
GOVERNANCE
RISK
COMPLIANCE

www.onethyca.com

Junio 2021

RESUMEN

El 26 de mayo de 2021 se publicó la Ley Orgánica de Protección de Datos de Ecuador en el Registro Oficial, una vez que el texto fue aprobado por la Asamblea Nacional y sancionado por el señor Presidente de la República. Las disposiciones relacionadas con el régimen sancionatorio y las medidas correctivas dispuestas por la Autoridad entrarán en vigencia dos años contados a partir de esta fecha. Las empresas en el transcurso de este período deberán adecuar sus procesos a lo exigido por esta nueva normativa.

ESTRUCTURA

Considerandos: 28
Capítulos: 12
Artículos: 77

Disposiciones generales: 9
Disposiciones transitorias:4
Disposiciones reformatorias: 4
Disposiciones derogatorias: 4
Disposición final: 1

CAPÍTULOS	ARTÍCULOS
Capítulo I Ámbito de Aplicación Integral	Art. 1- 9
Capítulo II Principios	Art. 10
Capítulo III Derechos	Art. 11- 24
Capítulo IV Categorías Especiales de Datos	Art. 25- 32
Capítulo V Transferencia o Comunicación y Acceso a Datos Personales por Terceros	Art. 33- 36
Capítulo VI Seguridad de Datos Personales	Art. 37- 46
Capítulo VII Del Responsable, Encargado y Delegado De Protección De Datos Personales	Art. 47- 51
Capítulo VIII De la Responsabilidad Proactiva	Art. 52- 54
Capítulo IX Transferencia o Comunicación Internacional de Datos Personales	Art. 55- 61
Capítulo X De Los Requerimientos Directos y de La Gestión del Procedimiento Administrativo	Art. 62-64
Capítulo XI Medidas Correctivas, Infracciones Y Régimen Sancionatorio	Art. 65-74
Capítulo XII Autoridad De Protección De Datos Personales	Art. 75-77

ALCANCE Y APLICABILIDAD

Extraterritorial cuando las actividades de tratamiento esten relacionadas con:

1) La oferta de bienes o servicios a dichos titulares, independientemente de si a estos se les requiere su pago o no

2) El control de su comportamiento, en la medida en que este tenga lugar en el Ecuador.

3) Adquieran la obligación en virtud de un contrato o de las regulaciones vigentes del derecho internacional público.

PRINCIPIOS

1. Juridicidad
2. Lealtad
3. Transparencia
4. Finalidad (explícitas, legítimas y comunicadas al titular)
5. Pertinencia y minimización
6. Proporcionalidad
7. Confidencialidad
8. Calidad y exactitud
9. Conservación (durante un tiempo no mayor al necesario)
10. Seguridad
11. Responsabilidad proactiva y demostrada
12. Aplicación favorable al titular (interpretación de la norma)
13. Independencia del control (autonomía e independencia del ente regulador)

CRITERIOS EN NORMA ESPECIALIZADA

Aplicación de los principios de **legalidad, proporcionalidad y necesidad** cuando su aplicación interfiera con otros derechos o ámbito (libertad de expresión, sectores regulados por normativa específica, gestión de riesgos, desastres naturales, seguridad nacional y defensa del Estado)

NUEVOS DERECHOS

1. Derecho a la información
2. Derecho de acceso
3. Derecho de rectificación y actualización
4. Derecho de eliminación
5. Derecho de oposición
6. Derecho a la portabilidad
7. Derecho a la suspensión del tratamiento
8. Derecho a la suspensión del tratamiento (limitación de su uso)
9. Derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas
10. **Derecho de consulta en el Registro Nacional de Protección de Datos Personales**
11. **Derecho a la educación digital**

- **Plazo de 15 días** para que el responsable atienda los derechos del titular
- Presentado el requerimiento ante el responsable este contará con un término de 10 días para contestar afirmativa o negativamente, notificar y ejecutar lo que corresponda. (Art. 62)

BASES LEGALES DE PROCESAMIENTO

Consentimiento (libre, específico, informado, inequívoco)
Obligación legal
Orden judicial
Interés público
Obligaciones contractuales
Intereses vitales, del interesado o de otra persona natural
Bases de datos de acceso público
Interés legítimo del responsable de tratamiento o de tercero

DEL CONSENTIMIENTO

- Libre
- Específico
- Informado
- Inequívoco
- Podrá revocarse en cualquier momento
- Menores de 15 años edad necesitán de su representante legal

PARTES INVOLUCRADAS

- Titular
- Responsable del tratamiento
- Encargado del tratamiento
- Destinatario
- Autoridad de Protección de Datos Personales
- Delegado de protección de datos personales (DPO)

DEL DELEGADO DE PROTECCIÓN DE DATOS-DPD

El DPO es la persona encargada informar a la entidad responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos. También deberá velar o supervisar el cumplimiento normativo así como de cooperar con la Autoridad y actuar como punto de contacto entre ésta y la entidad responsable del tratamiento de datos.

Cuándo se requiere de un DPO?

1. Instituciones que conforman el sector público
2. Control permanente y sistematizado por su volumen, naturaleza, alcance o finalidades del tratamiento
3. Tratamiento a gran escala de categorías especiales de datos

*En caso de incumplimiento de sus funciones, el delegado de protección de datos personales responderá **administrativa, civil y penalmente**, de conformidad con la ley.

DE LA AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES

Se crea la **Superintendencia de Protección de Datos**, entidad con plena independencia y poderes de investigación, sancionatorios, de autorización y consultivos.

CREACIÓN DE REGISTROS NACIONALES DE DATOS

- Registro Nacional de protección de datos personales
- Registro Único de responsables y encargados incumplidos

Obligaciones del Responsable del Tratamiento

- Aplicar e implementar requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas.
- Aplicar e implementar procesos de verificación, evaluación, valoración periódica de la eficiencia, eficacia y efectividad de los requisitos y herramientas implementadas.
- Implementar políticas de protección de datos en cada caso en particular
- Utilizar metodologías de análisis y gestión de riesgos.
- Realizar evaluaciones de adecuación al nivel de seguridad previas al tratamiento de datos personales.
- Tomar medidas para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas.
- Notificar a la Autoridad de Protección de Datos Personales y al titular de los datos acerca de violaciones a las seguridades
- Implementar la protección de datos personales desde el diseño y por defecto
- Suscribir contratos de confidencialidad y manejo adecuado de datos personales con el encargado
- Asegurar que el encargado del tratamiento de datos personales ofrezca mecanismos suficientes
- Registrar y mantener actualizado el Registro Nacional de Protección de Datos Personales
- Designar al Delegado de Protección de Datos Personales
- Permitir y contribuir a la realización de auditorías o inspecciones, por parte de un auditor acreditado por la Autoridad de Protección de Datos Personales
- Los demás establecidos en la presente Ley

Obligaciones del Encargado del Tratamiento

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

MEDIDAS DE SEGURIDAD DE DATOS PERSONALES

Las organizaciones deben implementar las medidas de seguridad necesarias para asegurar un nivel adecuado de protección de datos personales considerando los siguientes aspectos y medidas:

- anonimización, seudonomización o cifrado.
- confidencialidad, integridad y disponibilidad permanentes de los sistemas.
- resiliencia técnica, física, administrativa, y jurídica.
- estándares internacionales para una adecuada gestión de riesgos e implementación y manejo de sistemas de seguridad.
- códigos de conducta
- implementar un proceso de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo.

EVALUACIONES DE IMPACTO (PIA) Y ANÁLISIS DE RIESGOS

Cuándo son obligatorias las Evaluaciones de Impacto?

Las organizaciones deben realizar evaluaciones de impacto (PIA) previas al tratamiento de datos personales cuando conlleve un alto riesgo para los derechos y libertades del titular y cuando la Autoridad lo requiera. En los siguientes casos de tratamiento, la evaluación es obligatoria:

1. Evaluación sistemática y exhaustiva (tratamiento automatizado)
2. Tratamiento a gran escala de las categorías especiales de datos
3. Observación sistemática a gran escala de una zona de acceso público

Qué se debe considerar en los Análisis de riesgo, amenazas y vulnerabilidades?

1. Las particularidades del tratamiento
2. Las partes involucradas
3. Las categorías y el volumen

DE LAS VULNERACIONES DE SEGURIDAD

Notificación de vulneración de seguridad:

- El responsable debe notificar a la Autoridad de Protección de Datos Personales y la Agencia de Regulación y Control de las Telecomunicaciones a más tardar **en el término de cinco** (**5**) **días después de que haya tenido constancia de ella.**
- El encargado debe notificar al Responsable **tan pronto sea posible, y a más tardar dentro del término de dos** (**2**) **días contados a partir de la fecha en la que tenga conocimiento de ella**.

Notificación de vulneración de seguridad al titular

- Deberá notificar sin dilación la vulneración de seguridad de datos personales al titular cuando conlleve un riesgo a sus derechos fundamentales y libertades individuales, **dentro del término de** (**3**) **tres días contados a partir de la fecha en la que tuvo conocimiento del riesgo.**

TRANSFERENCIAS INTERNACIONALES DE DATOS

- Nivel adecuado de protección
- Garantías adecuadas (instrumento jurídico vinculante que contemple los estándares)
- Normas corporativas vinculantes (BCR)
- Autorización para transferencia internacional (deberá ser registradas previamente en el Registro Nacional de Protección de Datos Personales)

* Casos excepcionales de transferencias (Artículo 60)

MECANISMOS DE TUTELA

Códigos de conducta, certificaciones, sellos y marcas de protección, cláusulas tipo (SCC)

*Los resultados de las auditorías podrán ser considerados como elementos probatorios dentro de los procesos sancionatorios (Artículo 54)

SANCIONES Y MULTAS

	Leves	Graves
Multas para servidores públicos	1 a 10 salarios básicos unificados sin perjuicio de la responsabilidad extracontractual	10 a 20 salarios básicos unificados sin perjuicio de la responsabilidad extracontractual
Multas para responsables o encargados	Multa de entre el 0.1% y el 0.7% calculada sobre su volumen de negocio correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.	Multa de entre el 0.7% y el 1% calculada sobre su volumen de negocios, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.

Sanciones: responsables, encargados del tratamiento de datos personales y organismos de certificación

Responsable

Leves

- No tramitar peticiones o quejas del titular
- No implementar protección de datos desde el diseño y por defecto
- No mantener las políticas de protección de datos
- Elegir un encargado del tratamiento de datos personales que no ofrezca garantías suficientes
- Incumplir las medidas correctivas dispuestas por la Autoridad

Graves

- No implementar medidas administrativas, técnicas y físicas, organizativas y jurídicas
- Utilizar información o datos para fines distintos
- Ceder o comunicar datos personales sin cumplir con los requisitos
- No utilizar metodologías de análisis y gestión de riesgos
- No realizar evaluaciones de impacto
- No implementar medidas técnicas organizativas
- No notificar a la Autoridad y al titular de las vulneraciones de seguridad
- No suscribir contratos con el encargado
- No mantener actualizado o consignar el Registro Nacional de Protección de datos personales
- No designar DPO
- No permitir y no contribuir a la realización de auditorías o inspecciones
- Incumplir las medidas correctivas cumplir de forma tardía, parcial o defectuosa

SANCIONES Y MULTAS

Encargado

Leves

- No colaborar con el responsable para atender el ejercicio de derechos del titular
- No facilitar el acceso al responsable a toda la información referente al cumplimiento
- No permitir o no contribuir a la realización de auditorías o inspecciones
- Incumplir las medidas correctivas dispuestas por la Autoridad

Graves

- Realizar tratamientos de datos personales sin observar los principios y derechos
- No tratar datos personales de conformidad con lo previsto, en el contrato
- No suscribir contratos
- No implementar mecanismos destinados a mantener la confidencialidad, integridad, disponibilidad y resiliencia
- No implementar medidas preventivas y correctivas en la seguridad
- No suprimir o transferir los datos personales al responsable una vez finalizado el contrato
- Comunicación de datos personales sin cumplir con los requisitos
- Incumplir las medidas correctivas cumplir de forma tardía, parcial o defectuosa
- No notificar al responsable sobre cualquier vulneración de la
- seguridad

DISPOSICIONES TRANSITORIAS

- Las medidas correctivas y el régimen sancionatorio entrarán en vigencia en 2 años contados a partir del 26 de mayo de 2021.
- Instituciones estatales, empresas grandes y pequeñas dentro del plazo de 2 años contados a partir del 26 de mayo de 2021 deberán adecuar sus procesos a lo exigido por esta norma.

LL.M Johanna Suárez
Experta en Protección de Datos
johanna.suarez@onethyca.com