FI0.01 - Checklist para determinar si tu organización requiere un DPO.

Palabras: 3746.
Tiempo estimado de lectura: 25 minutos.
Páginas: 11.

Tabla de Contenidos.

FI0.01 - Checklist para determinar si tu organización requiere un DPO.

¿Sabías que a partir de diciembre de 2025 tu organización puede recibir sanciones de hasta USD 46.000 en el peor de los casos si no cumple con la LOPDP?

A partir de diciembre de 2025, las empresas privadas en Ecuador que no cumplan con la LOPDP podrán recibir sanciones equivalentes de hasta el **4% de sus ingresos anuales**, según el Modelo de Cálculo de Sanciones Administrativas

(MPRIV-1: Resolución SPDP-SPD-2024-0022-R para entidades privadas). ¿Sabes si la tuya necesita un Data Protection Officer (DPD en español)?

¿Tu organización necesita un Data Protection Officer?

Este Checklist práctico de Consulting DPO te ayuda a determinar lo que necesitas para cumplir la LOPDP en Ecuador.

1. Introducción.

De acuerdo con la **Resolución SPDP-SPD-2025-0028-R**, emitida el 31 de julio de 2025, las organizaciones privadas sujetas a esta obligación deberán registrar al **Data Protection Officer o DPO** (en español es DPD, equivalente a Delegado de Protección de Datos) en la plataforma de la Superintendencia de Protección de Datos Personales (SPDP) entre el **1 de noviembre y el 31 de diciembre de 2025**.

¿Por qué importa? Porque la **Ley Orgánica de Protección de Datos Personales (LOPDP)** aplica a **todas las organizaciones en Ecuador**, grandes o pequeñas, públicas o privadas. No se trata de si quieres o no cumplir: la pregunta es **qué nivel de cumplimiento necesitas**.

Tus clientes, empleados y usuarios **confían en ti** cada vez que te entregan sus datos. La ley protege esa confianza, y este Checklist es tu primer paso para cumplir con responsabilidad, proteger tu reputación y evitar sanciones.

2. ¿Qué es la LOPDP y por qué te afecta?

Desde 2021, Ecuador cuenta con la **LOPDP**, inspirada en el **Reglamento General de Protección de Datos (GDPR) de la Unión Europea**, considerado el estándar más alto a nivel mundial. Su origen responde a abusos históricos en los que la información personal fue utilizada en contra de las personas: desde censos en Mesopotamia para controlar poblaciones, hasta el uso de registros étnicos y religiosos en la Segunda Guerra Mundial.

La LOPDP parte de una premisa sencilla pero poderosa:

- **Todas las personas naturales tienen derechos LOPDP**: decidir quién usa sus datos, para qué se usan, y exigir que se eliminen cuando ya no sean necesarios.
- **Todas las organizaciones o personas que traten datos** (empresas, instituciones educativas, hospitales, bancos, apps, consultorios, ministerios, etc.) **tienen la obligación de respetar esos derechos** y adoptar medidas de seguridad y cumplimiento.

En otras palabras: **todas las personas tienen derechos bajo la LOPDP y todas las organizaciones deben cumplirlos.**

3. Ejemplos de Multas (según Modelo MPRIV-1 – entidades privadas).

Para comprender mejor las consecuencias del incumplimiento de la **Ley Orgánica de Protección de Datos Personales (LOPDP)**, a continuación se presentan tres escenarios prácticos con base en la metodología oficial de cálculo de sanciones para entidades privadas (**Modelo MPRIV-1**, Resolución SPDP-SPD-2024-0022-R).

3.1. Si una empresa necesita un DPO y no lo tiene.

- Constituye una **infracción grave**, por incumplimiento de los **artículos 47 a 50 de la LOPDP** (obligación de designar un Data Protection Officer).
- **Multa estimada:** entre **0,5 % y 1 % de los ingresos anuales** de la empresa, según la gravedad y la reincidencia.
    - **Ejemplo práctico:** si la empresa factura **USD 1.000.000 al año**, la multa sería:
        - Al **0,5 %: USD 5.000**
        - Al **1 %: USD 10.000**
- Además, la **SPDP** puede imponer **medidas correctivas inmediatas**, incluyendo la **designación formal del DPO** en un plazo máximo de **30 días**.

3.2. Si una empresa no necesita un DPO, pero no implementa medidas mínimas de cumplimiento (políticas, RAT, consentimiento, protocolos de incidentes)

- Constituye una **infracción leve**, conforme al **artículo 67 de la LOPDP**.
- **Multa estimada:** hasta el **0,1 % de los ingresos anuales**.
    - **Ejemplo práctico:** si la empresa factura **USD 1.000.000 al año**, la multa sería:
        - Al **0,1 %: USD 1.000**
- **Ejemplo:** una clínica pequeña o empresa de servicios que trate datos personales, pero no cuente con política de privacidad ni registro de actividades de tratamiento (RAT).

3.3. Si una empresa necesita un DPO y ocurre una filtración de datos sensibles.

- Se configuran **dos incumplimientos acumulativos**:

    1. No contar con un DPO (**grave**).
    2. Filtración de datos sensibles (**muy grave**, **artículo 73 de la LOPDP**).

- **Multa estimada:** entre **2 % y 4 % de los ingresos anuales**, dependiendo del nivel de afectación, la naturaleza de los datos y la intencionalidad.
    - **Ejemplo práctico:** si la empresa factura **USD 1.000.000 al año**, la multa sería:
        - Al **2 %: USD 20.000**
        - Al **4 %: USD 40.000**
- Si los datos comprometidos pertenecen a **niños, niñas o adolescentes (NNA)** o contienen información **sensible** (salud, biometría, creencias, orientación sexual), la sanción puede alcanzar el **máximo del rango**.

Notas aclaratorias.

- Los porcentajes indicados corresponden al **Modelo de Cálculo de Sanciones Administrativas (MPRIV-1)** emitido por la **Superintendencia de Protección de Datos Personales (SPDP)**.
- El cálculo se realiza sobre el **volumen anual de ventas o ingresos brutos declarados en el último ejercicio fiscal**.
- La **SPDP** evalúa además factores como **intencionalidad, daño, reiteración e impacto reputacional**, para determinar el porcentaje final dentro del rango.

Base normativa.

- **Constitución del Ecuador:** Art. 66 numeral 19 y Art. 92.
- **Ley Orgánica de Protección de Datos Personales:** Arts. 47–50, 65–74.
- **Reglamento General a la LOPDP:** Arts. 29–34.
- **Resolución SPDP-SPD-2024-0022-R:** *Modelo de Cálculo de Sanciones Administrativas (MPRIV-1 – entidades privadas).*

Sugerencia opcional de formato (para visualización dentro del Checklist):

Puedes colocar una tabla resumen después de esta sección, como recordatorio rápido:

Tipo de infracción	Rango de multa	Ejemplo (empresa con USD 1M de ingresos)
Leve	Hasta 0,1 %	USD 1.000
Grave	0,5 % – 1 %	USD 5.000 – 10.000
Muy grave	2 % – 4 %	USD 20.000 – 40.000

Tabla de consecuencias y multas (empresas privadas).

Resultado del Checklist	Nivel de incumplimiento si no actúa	Tipo de infracción (LOPDP)	Rango estimado de multa (% sobre ingresos anuales)	Ejemplo práctico (empresa con ingresos anuales de USD 1.000.000)
No requiere DPO, pero sin Compliance LOPDP mínimo	No contar con políticas, consentimiento, RAT o protocolos de incidentes.	**Leve**	Hasta **0,1 %**	**≈ USD 1.000**
Zona de análisis reforzado sin justificación formal	No sustentar documentalmente por qué no se designa un DPO.	**Grave**	**0,5 % – 1 %**	**≈ USD 5.000 – 10.000**
DPO obligatorio y no designado	Sin DPO, sin políticas avanzadas, sin registro de cumplimiento.	**Grave**	**0,5 % – 1 %**	**≈ USD 5.000 – 10.000**
Compliance LOPDP completo, pero con filtración de datos sensibles	Brecha de seguridad o pérdida de datos personales sensibles.	**Muy grave**	**2 % – 4 %**	**≈ USD 20.000 – 40.000**

Las sanciones no solo son económicas: también incluyen la obligación de corregir de inmediato, auditorías forzadas y, en casos graves, suspensión temporal de tratamientos.

Conclusión práctica: Aunque tu organización se ubique en "no necesita DPO", siempre debes cumplir con **medidas mínimas de la LOPDP**. No actuar significa exponerte a sanciones económicas y reputacionales.

Notas aclaratorias.

- Los rangos corresponden al **Modelo de Cálculo de Sanciones Administrativas (MPRIV-1)** para entidades privadas, conforme a la **Resolución SPDP-SPD-2024-0022-R**.
- El cálculo se aplica sobre los **ingresos brutos anuales del último ejercicio fiscal declarado**.
- La **SPDP** puede ajustar el porcentaje dentro del rango según la **intencionalidad, daño, reincidencia o impacto reputacional** del caso.

Base normativa.

- **Constitución del Ecuador:** Art. 66 numeral 19 y Art. 92.
- **LOPDP:** Arts. 47 – 50 y 65 – 74.
- **Reglamento General a la LOPDP:** Arts. 29 – 34.
- **Resolución SPDP-SPD-2024-0022-R:** *Modelo de Cálculo de Sanciones Administrativas (MPRIV-1 – entidades privadas).*

4. Cómo funciona este Checklist.

Este Checklist ha sido diseñado como una herramienta práctica de autoevaluación para organizaciones en Ecuador.
Funciona en **dos niveles**:

- **Versión Express** → 7 preguntas simples que cualquier persona puede responder con *sí* o *no* y conocer de inmediato si su organización necesita un DPO, no lo requiere o se encuentra en una zona de análisis reforzado.

- **Versión Pro** → profundiza en **5 secciones clave**:
  1. Naturaleza de la organización.
  2. Tipo de datos tratados.
  3. Escala de tratamiento.
  4. Tipo de actividad.
  5. Control y supervisión.

La **Versión Pro** permite elaborar el **Informe FI0.02**, documento formal con trazabilidad legal que determina la obligatoriedad de designar un DPO.

Sea cual sea tu resultado, recuerda: la LOPDP exige acción. Este Checklist es tu punto de partida; el siguiente paso es contar con una estrategia clara y documentada que **Consulting DPO** puede diseñar contigo.

Descargo de Responsabilidad Legal.

Este Checklist es una herramienta de autoevaluación preliminar basada en la Ley Orgánica de Protección de Datos Personales (LOPDP) del Ecuador. Su uso tiene únicamente fines informativos y de orientación.

- El resultado del Checklist **no constituye un dictamen legal definitivo**, ni garantiza la inexistencia de la obligación de designar un Data Protection Officer (DPO).

- La determinación formal debe realizarse mediante el **Informe FI0.02 - Evaluación de obligatoriedad de DPO**, con fundamento en la Constitución, la LOPDP y las resoluciones de la SPDP.
- **Consulting DPO puede ayudarte** en cualquiera de los escenarios:
    - **Si no necesitas un DPO** → te ayudamos a sustentar esa decisión y a implementar el **Compliance LOPDP mínimo** (políticas, cláusulas, protocolos de incidentes, registros RAT, etc.).
    - **Si estás en zona de casos que requieren análisis reforzado** → te asesoramos para documentar la justificación legal y aplicar un Compliance LOPDP intermedio.
    - **Si necesitas un DPO** → te acompañamos con la implementación completa y, además, puedes contar con nuestro servicio de **DPO mensual (DPO as a Service)** para cumplir con la ley de forma continua.

Ni el autor ni Consulting PDO serán responsables frente a terceros o autoridades por las decisiones que se adopten únicamente en base a este Checklist.

Este Checklist es un primer paso. La responsabilidad de cumplir con la LOPDP recae en cada organización, y Consulting DPO está aquí para que no lo hagas solo.

5. El Checklist (Express + Pro).

Este Checklist está diseñado para que cualquier organización pueda evaluar rápidamente si necesita designar un **Data Protection Officer (DPO)** y, al mismo tiempo, entender el nivel mínimo de cumplimiento LOPDP que debe implementar.

Versión Express - 7 preguntas rápidas.

1. ¿Manejas datos personales de clientes, pacientes, estudiantes o empleados (nombre, cédula, teléfono, correo)?
2. ¿Recolectas o usas datos de salud, huellas digitales, fotos, creencias religiosas, orientación sexual o datos de niños y adolescentes?
3. ¿Atiendes o procesas datos de más de 1.000 personas distintas al año?
4. ¿Usas cámaras de seguridad, aplicaciones móviles, geolocalización o herramientas de seguimiento digital de clientes?
5. ¿Guardas o compartes información en plataformas fuera del Ecuador (ej. Google, Meta, Microsoft, CRMs extranjeros)?
6. ¿Perteneces al sector público o a sectores regulados por la SPDP como bancos, salud, educación o telecomunicaciones)?
7. ¿Has tenido auditorías o controles de alguna entidad reguladora en el último año?

Resultado - Semáforo Express

- **De 0 a 1 "sí marcados"** → No necesitas DPO, pero sí un **plan mínimo de cumplimiento LOPDP**.
- **De 2 a 3 "sí marcados"** → Estás en zona de casos que requieren análisis reforzado, probablemente necesitas un DPO (depende de la escala), y necesitas un Compliance LOPDP más que el mínimo.
- **Más de 4 "sí marcados"** → Necesitas un DPO obligatorio + Compliance LOPDP completo.

Versión Pro - 5 secciones de análisis.

La versión Pro se utiliza como base para elaborar el **Informe FI0.02**, documento formal con trazabilidad legal que determina la obligatoriedad de designar un DPO.

A. Naturaleza de la organización.

1. ¿Tu organización es parte del sector público?
2. ¿Tu organización pertenece a un sector regulado por la SPDP como la banca, salud, telecomunicaciones, educación, o cooperativas?

B. Tipo de datos tratados.

3. ¿Tratas datos sensibles (salud, biometría, creencias, orientación sexual, datos financieros delicados)?
4. ¿Tratas datos de niños, niñas y adolescentes (NNA)?
5. ¿El tratamiento de datos sensibles o de NNA es una actividad principal de la organización?

C. Escala de tratamiento.

6. ¿Tratas más de 10.000 titulares al año (~833 al mes)?
7. ¿Superas los 50.000 titulares al año (~4.200 al mes)?
8. ¿Realizas tratamientos que generan bases de datos de carácter masivo (ej. marketing digital, clientes recurrentes, apps con usuarios)?

D. Tipo de actividad.

9. ¿Realizas observación sistemática y masiva (CCTV, geolocalización, apps de tracking, perfilado)?
10. ¿Ofreces servicios digitales masivos en línea?
11. ¿Realizas transferencias internacionales de datos recurrentes o de datos sensibles?

E. Control y supervisión.

12. ¿Has tenido auditorías o controles de la SPDP o de reguladores sectoriales en el último año?
13. ¿Te exigen auditorías recurrentes (≥1 vez al año)?

Escala Pro - Interpretación de cumplimiento.

- Cumple 1 condición del sector público o regulado → **DPO obligatorio**.
- Cumple 1 condición de datos sensibles/NNA a gran escala → **DPO obligatorio**.
- Cumple 2 o más condiciones de escala + riesgo → **DPO obligatorio**.
- No cumple, pero maneja más de 1.000 titulares al año → **DPO recomendable (voluntario)**.
- No cumple y <1.000 titulares → **No requiere DPO, pero sí Compliance LOPDP mínimo**.

6. Interpretación de resultados.

El objetivo de este Checklist además de determinar si tu organización debe designar un DPO, también ayuda a dejar claro que **todas las organizaciones en Ecuador deben cumplir la LOPDP en algún nivel**.

- **(0-1 "sí marcados")** → Tu organización **no necesita un DPO**, pero sí debe implementar un **Compliance LOPDP mínimo**:
  - Políticas de privacidad.
  - Procedimientos de consentimiento.
  - Registro de Actividades de Tratamiento (RAT).
- **(2-3 "sí marcados")** → Estás en una **zona de casos** que requieren análisis reforzado. Lo recomendable es contar con un **DPO voluntario** o, como mínimo, documentar la justificación legal de por qué no lo designas y aplicar un **Compliance LOPDP intermedio**.
- **(4+ "sí marcados")** → Tu organización **sí necesita un DPO** y debe cumplir con un **Compliance LOPDP completo**, incluyendo designación formal de DPO, notificación a la SPDP, políticas avanzadas, cláusulas contractuales y auditorías periódicas.

Mapa de consecuencias.

El resultado de este Checklist no solo indica si tu organización necesita designar un Data Protection Officer (DPO). También muestra el **nivel mínimo de cumplimiento de la LOPDP** que debes implementar y los **riesgos legales** en caso de no hacerlo.

La **Ley Orgánica de Protección de Datos Personales (arts. 65–74)** establece medidas correctivas, infracciones y sanciones. La **SPDP** cuenta además con un **Modelo de cálculo de sanciones administrativas**, y la **Constitución del Ecuador (art. 66.19 y art. 92)** reconoce la protección de datos personales como un derecho fundamental.

Esto significa que, incluso si tu resultado en el Checklist te aparece que no necesitas un DPO, igual estás obligado a cumplir con medidas mínimas. De lo contrario, puedes recibir sanciones.

Resultado Checklist	**Nivel de cumplimiento requerido**	**Riesgo si no actúas**	**Posibles sanciones (referencia normativa)**
(0–1 "sí marcados")	Compliance LOPDP mínimo (política de privacidad, Registro de Actividades de Tratamiento RAT, consentimiento), y no necesitas un DPO	Multas leves, observaciones de la SPDP	Arts. 67–71 LOPDP; Modelo de sanciones SPDP
(2–3 "sí marcados")	Compliance LOPDP intermedio y el DPO puede ser voluntario	Riesgo de infracciones graves	Arts. 68–72 LOPDP
(4+ "sí marcados")	Compliance LOPDP completo y sí necesitas un DPO	Multas altas, auditorías obligatorias	Arts. 73–74 LOPDP; Res. SPDP-SPD-2025-0028-R

En conclusión: el resultado del Checklist es el punto inicial que genera un mapa de acción. Sea cual sea el resultado, la LOPDP exige que implementes medidas, y **Consulting DPO** puede ayudarte a cumplir de manera clara, práctica y medible.

7. Invitación a actuar con Consulting DPO.

El plazo para implementar y registrar al Data Protection Officer (cuando corresponda) vence en **diciembre de 2025**. Después de esa fecha, la **Superintendencia de Protección de Datos Personales (SPDP)** podrá iniciar auditorías y aplicar sanciones a las organizaciones que no cumplan con la **LOPDP**.

No esperes a una auditoría o sanción. Con nuestro método **FI0-FI6 (Simple Steps Systems)**, transformamos la LOPDP en **pasos claros, prácticos y medibles** para tu organización.

Aunque tu resultado sea que no necesitas un DPO, igual necesitas políticas, cláusulas y un plan mínimo. Nosotros lo hacemos claro, simple y defendible ante la SPDP.

¿Por qué elegir Consulting DPO?

- **Simplificamos la ley**: traducimos la LOPDP en procesos que tu equipo puede aplicar fácilmente.
- **Te damos claridad**: sabrás si necesitas o no un DPO, y tendrás la justificación documentada.
- **Te acompañamos de principio a fin**: desde lo mínimo (políticas básicas, registros RAT, cláusulas contractuales) hasta lo más avanzado (evaluaciones de impacto, auditorías, DPO as a Service).

Aunque no necesites un DPO, sí necesitas cumplir con la LOPDP. En Consulting DPO te mostramos cómo hacerlo, de la forma más clara y simple en Ecuador.

Nuestro método FI0–FI6 (Simple Steps System) traduce la LOPDP en seis fases prácticas, con entregables claros y verificables. Desde la autoevaluación inicial hasta la auditoría continua, simplificamos el cumplimiento para que tu organización esté siempre protegida.

Nuestra misión es convertir un marco legal complejo en un sistema claro, simple y defendible. Para que la LOPDP deje de ser un problema para tu organización.

Cumplir con la LOPDP no es opcional. La diferencia está en cómo lo haces: con miedo a sanciones, o con claridad y acompañamiento experto.

Agenda hoy una sesión de diagnóstico con Consulting DPO y asegura que tu organización cumpla con la LOPDP antes de diciembre de 2025.

Descargo de Responsabilidad Legal Expandido sobre el uso de este Checklist.

La presente herramienta, denominada **Checklist para determinar si se requiere Data Protection Officer (DPO)**, forma parte del sistema metodológico de **Consulting DPO** para la implementación de la **Ley Orgánica de Protección de Datos Personales (LOPDP)** en el Ecuador.

Este documento no sustituye el asesoramiento jurídico especializado. Para efectos regulatorios, solo los informes FI0.02 y posteriores pueden servir como justificación formal ante la SPDP.

El objetivo de esta herramienta es **proporcionar una orientación preliminar** a organizaciones, profesionales o personas naturales respecto de la posible obligatoriedad de designar un Data Protection Officer (DPO).

1. Carácter orientativo de este Checklist.

- Este Checklist constituye únicamente un **primer paso de autoevaluación básica**, mediante un conjunto de preguntas simplificadas.
- Los resultados que se obtienen a través de esta herramienta **no constituyen un dictamen legal definitivo**, ni garantizan la inexistencia de la obligación de designar un DPO.
- La obligatoriedad debe determinarse mediante un **análisis técnico-jurídico posterior**, sustentado en la Constitución, la LOPDP y las resoluciones emitidas por la SPDP.

2. Siguiente paso obligatorio: FI0.02.

- Para contar con un resultado **formal y defendible ante la SPDP**, la organización o persona debe aplicar la herramienta **FI0.02 - Informe de evaluación sobre la obligatoriedad de designación de DPO**.
- El FI0.02 utiliza los resultados iniciales de este Checklist, los expande con **criterios normativos y de riesgo**, y documenta la justificación legal de por qué una organización sí o no requiere un DPO, en base a la **Constitución del Ecuador, la LOPDP y las resoluciones de la SPDP**.

3. Determinación de obligatoriedad del DPO.

El FI0.02 establece:

- **Organizaciones que requieren un DPO**: sector público, sectores regulados por la SPDP (banca, salud, educación, telecomunicaciones), tratamiento a gran escala de datos sensibles o de NNA, servicios digitales masivos, observación sistemática, transferencias internacionales recurrentes, auditorías anuales obligatorias.
- **Organizaciones que no requieren un DPO**: microempresas o profesionales con bajo volumen de datos, que no realizan tratamiento sensible a gran escala ni actividades de alto riesgo.
- **Zona de casos que requieren análisis reforzado:** organizaciones con tratamiento intermedio (ej. clínicas medianas, pymes digitales en expansión), donde el DPO puede ser recomendable aunque no obligatorio.

4. Necesidad universal de compliance LOPDP.

Independientemente de si la organización requiere o no un DPO, **toda entidad o persona que maneje datos personales debe implementar un plan de cumplimiento LOPDP acorde a su escala y riesgo**.

Compliance LOPDP mínimo (microempresas o profesionales con datos básicos):

1. Política de privacidad simplificada.
2. Consentimiento informado básico (ej. formularios, contratos).
3. Registro de Actividades de Tratamiento (RAT) en formato reducido.
4. Procedimiento para responder solicitudes de derechos ARCO+.
5. Medidas de seguridad mínimas: contraseñas seguras, copias de respaldo, control de accesos.

Compliance LOPDP intermedio (pymes o entidades con 1.000-10.000 titulares/año):

1. Políticas de privacidad completas.

2. Protocolos de incidentes y brechas de seguridad.
3. Procedimientos documentados de transferencias de datos.
4. Evaluaciones de riesgo y, cuando corresponda, Evaluaciones de Impacto (EIPD).
5. Cláusulas contractuales con terceros (según Res. SPDP 0006-R).

Compliance LOPDP avanzado (grandes organizaciones o con DPO obligatorio):

1. Todo lo anterior.
2. Designación formal de un DPO y notificación a la SPDP.
3. Auditorías periódicas (según Res. SPDP 0005-R).
4. Capacitación continua de personal.
5. Programas de sostenibilidad y recertificación (FI6).

5. Limitación de responsabilidad

- El uso exclusivo de este Checklist **no es suficiente para determinar con certeza** si una organización requiere un DPO.
- **Consulting DPO** y sus consultores **no asumen responsabilidad legal** por las decisiones adoptadas únicamente en base al resultado de este Checklist.
- La responsabilidad final de cumplir con la LOPDP recae en la **organización responsable del tratamiento de datos**.
- Para efectos legales y regulatorios, **solo el FI0.02 y los informes posteriores de Compliance LOPDP pueden servir como justificación formal frente a la SPDP.**

Nota: El sistema de cumplimiento Consulting DPO se encuentra alineado con los marcos ISO/IEC 27001, 27701, 31000, 29134 y 19011.