DELTA LEGAL

LISTA DE VERIFICACIÓN

Protección de Datos Personales (LOPDP) para PYMES

¿Su empresa cumple con la Ley Orgánica de Protección de Datos Personales? Verifíquelo en menos de 10 minutos.

2021	2%	9	30
Año de entrada en vigencia	Sanción máx. sobre facturación	Documentos clave requeridos	Puntos de verificación

■ LEY VIGENTE	La LOPDP es de cumplimiento obligatorio desde 2021 para toda persona natural o jurídica, pública o privada, que trate datos personales en Ecuador. No es una norma futura ni opcional: actualmente es exigible y fiscalizable por la Autoridad de Protección de Datos (Superintendencia).
■ NOTA DE USO	Esta guía tiene fines educativos e informativos. No reemplaza el asesoramiento jurídico profesional. Para un diagnóstico completo y la implementación de la LOPDP en su empresa, consulte con un especialista de Delta Legal.

deltalegal.net · info@deltalegal.net · 098-322-2720

INTRODUCCIÓN

¿A quién aplica la LOPDP?

La **Ley Orgánica de Protección de Datos Personales (LOPDP)** aplica a toda organización que trate datos personales de personas naturales en Ecuador, independientemente de su tamaño, sector o actividad. Si su empresa maneja cualquiera de los siguientes datos, está obligada a cumplir:

TIPO DE DATO	EJEMPLOS COMUNES EN UNA PYME	¿OBLIGA?
Datos de identificación	Nombres, cédulas, pasaportes, direcciones	✓ Sí
Datos de contacto	Teléfonos, correos electrónicos, redes sociales	✓ Sí
Datos laborales	Contratos, sueldos, cargos, evaluaciones de empleados	✓ Sí
Datos financieros	Números de cuenta, historial de pagos, facturación	✓ Sí
Datos de proveedores	Información personal de contactos de proveedores y aliados	✓ Sí
Datos sensibles	Salud, biometría, opiniones políticas, afiliación sindical	■ Mayor rigor

RIESGO DE NO CUMPLIR

Sanciones económicas de hasta el 2% de la facturación anual · Responsabilidad civil frente a clientes y empleados · Daño reputacional · Observaciones en auditorías, contratos y procesos de expansión · Riesgos legales ante incidentes de seguridad.

BENEFICIOS DE CUMPLIR

Reducción de riesgos legales y sancionatorios · Mayor confianza de clientes y aliados · Procesos internos más ordenados · Preparación para auditorías y expansión · Posicionamiento como empresa responsable y profesional.

BLOQUE A · DIAGNÓSTICO

¿Qué datos trata su empresa?

Antes de implementar cualquier medida, su empresa debe saber **qué datos trata, para qué, cómo los obtiene y dónde los almacena**. Este es el punto de partida del cumplimiento.

01	**Identifique todos los tipos de datos personales que trata** Haga un inventario: datos de clientes, empleados, proveedores, visitantes. Incluya datos en papel, en sistemas informáticos, en correos electrónicos y en la nube. ■ *Muchas empresas desconocen la cantidad de datos que realmente tratan.* ✓ *Designe a una persona responsable de coordinar este inventario.*	OBLIGATORIO
02	**Identifique la base legal de cada tratamiento** Por cada tipo de dato debe existir una razón jurídica válida: consentimiento del titular, ejecución de un contrato, cumplimiento de una obligación legal, interés legítimo, etc. ■ *Tratar datos sin base legal es una infracción directa a la LOPDP.* ■ *Documento: Registro de Actividades de Tratamiento*	OBLIGATORIO
03	**Elabore el mapa de flujos de información** Documente cómo entran los datos a su empresa, cómo circulan internamente, quién tiene acceso, a quién se comparten y cómo se eliminan. ✓ *El mapa permite identificar puntos de riesgo que no son visibles sin este análisis.* ■ *Documento: Mapa de flujos de información*	OBLIGATORIO
04	**Identifique si trata datos sensibles** Los datos de salud, biometría, filiación política, religión, orientación sexual o situación migratoria requieren medidas adicionales y mayor cuidado. ■ *Tratar datos sensibles sin protecciones adecuadas puede generar sanciones agravadas.*	CRÍTICO
05	**Verifique si está obligado a designar un Delegado de Protección de Datos (DPD)** El DPD es obligatorio para el sector público y para empresas que traten de forma habitual datos sensibles (salud, biometría), o que pertenezcan a sectores financiero, telecomunicaciones, salud o educación. Las demás pueden designar un responsable interno. ■ *Si tiene personal de salud ocupacional o trabajo social, probablemente está obligado a designar un DPD.* ✓ *El DPD debe registrarse ante la Superintendencia dentro de los plazos establecidos.* ■ *Documento: Designación de Responsable / DPD*	VERIFICAR

BLOQUE B · DOCUMENTACIÓN

Los 9 documentos clave que su empresa debe tener

La LOPDP exige contar con un conjunto de documentos que demuestren cumplimiento. Sin estos documentos, su empresa no puede acreditar cumplimiento ante la Superintendencia en caso de inspección o denuncia.

01	**Política de Protección de Datos Personales** Documento principal que establece el compromiso de su empresa con la protección de datos, los principios que aplica, los tipos de datos que trata y los derechos de los titulares. Debe estar aprobada por la gerencia y ser accesible a todos. ✓ *Publique un resumen en su sitio web o en un lugar visible para clientes.* ■ *Documento: Política de Protección de Datos Personales*	OBLIGATORIO
02	**Registro de Actividades de Tratamiento (RAT)** Inventario de todos los tratamientos de datos que realiza su empresa: qué datos, para qué fin, con qué base legal, quién los trata, cuánto tiempo se conservan y a quién se comparten. Uno por cada categoría de titular (clientes, empleados, proveedores). ■ *El RAT es el documento que primero solicita la Autoridad en una inspección.* ■ *Documento: Registro de Actividades de Tratamiento*	OBLIGATORIO
03	**Avisos de Privacidad** Informes que deben entregarse a cada titular de datos al momento de recolectarlos. Explica qué datos se recogen, para qué, por cuánto tiempo, a quién se comparten y cuáles son sus derechos. Debe haber uno para clientes, uno para empleados y uno para proveedores. ■ *No informar al titular es infracción directa. El aviso no puede ser solo una página interna.* ✓ *Incluya el aviso en formularios de contacto, contratos de trabajo y contratos con proveedores.* ■ *Documento: Avisos de Privacidad (clientes, empleados, proveedores)*	OBLIGATORIO
04	**Procedimiento para el ejercicio de derechos de los titulares** La LOPDP reconoce 8 derechos: acceso, rectificación, cancelación, oposición, portabilidad, limitación, no ser objeto de decisiones automatizadas y anonimización. Su empresa debe tener un procedimiento escrito para atender estas solicitudes. ■ *Si un titular solicita eliminar sus datos y su empresa no tiene procedimiento, la sanción es automática.* ✓ *El plazo legal de respuesta es de 15 días. Tenga un canal habilitado (email, formulario).* ■ *Documento: Procedimiento de ejercicio de derechos ARCO+*	OBLIGATORIO

05	**Análisis de riesgos y medidas de seguridad** Documento que identifica los principales riesgos para los datos personales que trata su empresa (acceso no autorizado, pérdida, robo, uso indebido) y las medidas técnicas y organizativas adoptadas para mitigarlos. ✓ *Para PYMES se acepta un análisis simplificado y proporcional al volumen y sensibilidad de datos.* ■ *Documento: Análisis simplificado de riesgos*	OBLIGATORIO
06	**Procedimiento de gestión de incidentes de seguridad** Protocolo escrito que describe qué hacer si hay una brecha de seguridad: quién se encarga, cómo se notifica a la Autoridad (en 72 horas si aplica) y cómo se comunica a los titulares afectados. ■ *La LOPDP obliga a notificar incidentes graves a la Superintendencia en 72 horas.* ✓ *Tenga identificado de antemano quién es el responsable de activar este protocolo.* ■ *Documento: Procedimiento de gestión de incidentes*	OBLIGATORIO
07	**Cláusulas de protección de datos en contratos laborales** Los contratos de trabajo deben incluir cláusulas de confidencialidad y tratamiento de datos personales. Los empleados que acceden a datos de clientes o de otros empleados deben estar expresamente autorizados y obligados a reserva. ✓ *Revise contratos existentes y añada adendas si no tienen estas cláusulas.* ■ *Documento: Cláusulas contractuales laborales*	OBLIGATORIO
08	**Cláusulas de protección de datos con proveedores y encargados** Si comparte datos personales con proveedores (contables, tecnología, marketing, logística), debe firmar contratos que obliguen al proveedor a tratar esos datos solo para los fines autorizados y con las mismas garantías. ■ *Compartir datos con un proveedor sin contrato de encargo de tratamiento es infracción.* ■ *Documento: Contratos de encargo de tratamiento*	OBLIGATORIO
09	**Evidencias de capacitación al personal** Su empresa debe capacitar a los empleados que acceden a datos personales y conservar evidencia de esa capacitación (registros de asistencia, materiales, evaluaciones). La Autoridad puede solicitar estas evidencias. ✓ *Una capacitación anual breve con registro de asistencia cumple este requisito para la mayoría de PYMES.* ■ *Documento: Registro de capacitación LOPDP*	OBLIGATORIO

BLOQUE C · SEGURIDAD TÉCNICA

Medidas técnicas mínimas requeridas

La LOPDP no exige solo documentos — también requiere medidas técnicas proporcionales al riesgo. Estas son las mínimas que toda PYME debe implementar:

01	**Control de acceso a los sistemas con datos personales** Solo las personas que necesitan los datos para su trabajo deben poder acceder. Use contraseñas robustas, usuarios individuales (no compartidos) y permisos por rol. ■ *Las contraseñas compartidas o por defecto son una brecha de seguridad inmediata.*	OBLIGATORIO
02	**Cifrado o protección de datos almacenados y transmitidos** Los datos personales almacenados en computadores, servidores o la nube deben estar cifrados o protegidos. Las comunicaciones con datos personales (email, formularios) deben usar HTTPS y protocolos seguros. ✓ *Use servicios de correo y almacenamiento en la nube con cifrado activado (Google Workspace, Microsoft 365).*	OBLIGATORIO
03	**Copias de seguridad periódicas** Realice copias de seguridad regulares de los sistemas que contienen datos personales. Pruebe periódicamente que las copias se pueden restaurar. ■ *Una pérdida de datos sin copia de seguridad puede ser considerada incidente de seguridad.* ✓ *Frecuencia recomendada: diaria para datos críticos, semanal para el resto.*	OBLIGATORIO
04	**Registro de accesos (log de auditoría)** Los sistemas que contienen datos personales deben registrar quién accedió, cuándo y qué operaciones realizó. Este registro debe conservarse. ✓ *La mayoría de sistemas modernos (ERP, CRM, correo corporativo) tienen esta función activable.*	RECOMENDADO
05	**Política de pantalla limpia y escritorio despejado** Los empleados no deben dejar datos personales visibles en pantalla o en papel cuando se alejan de su puesto. Bloquear el equipo al alejarse debe ser obligatorio. ✓ *Establezca el bloqueo automático de pantalla en máximo 5 minutos de inactividad.*	RECOMENDADO
06	**Proceso de destrucción segura de documentos físicos** Los documentos en papel con datos personales (contratos, historiales, formularios) deben destruirse de forma segura (trituradora) cuando ya no sean necesarios. ■ *Botar documentos con datos personales en la basura común es infracción.*	OBLIGATORIO

BLOQUE D · DERECHOS Y DPD

Derechos de los titulares y Delegado de Protección de Datos

Su empresa debe estar preparada para responder solicitudes de titulares y, en ciertos casos, designar un Delegado de Protección de Datos.

Los 8 derechos que su empresa debe garantizar

DERECHO	QUÉ IMPLICA	PLAZO DE RESPUESTA
Acceso	El titular puede pedir saber qué datos tiene la empresa sobre él	15 días
Rectificación	Corregir datos incorrectos o desactualizados	15 días
Cancelación / Eliminación	Solicitar que se eliminen sus datos cuando ya no sean necesarios	15 días
Oposición	Oponerse al tratamiento de sus datos para ciertos fines	15 días
Portabilidad	Recibir sus datos en formato estructurado y reutilizable	15 días
Limitación del tratamiento	Restringir el uso de sus datos mientras se resuelve una disputa	15 días
No ser objeto de decisiones automatizadas	No ser evaluado solo por algoritmos sin intervención humana	15 días
Anonimización	Solicitar que sus datos se anonimicen en lugar de eliminarse	15 días

¿Necesita su empresa un Delegado de Protección de Datos?

TIPO DE EMPRESA	¿DPD OBLIGATORIO?	ALTERNATIVA
Sector público	**Sí — siempre**	—
Financiero, seguros, telecom, salud, educación	**Sí — obligatorio**	—
Empresas con datos sensibles habituales (salud ocup., biometría)	**Sí — obligatorio**	—
PYME sin datos sensibles habituales	**No — opcional**	Responsable interno de datos

IMPORTANTE

El DPD no implementa la LOPDP ni toma decisiones operativas. No puede ser oficial de seguridad ni parte de la alta dirección. Su nombramiento debe registrarse ante la Superintendencia dentro de los plazos establecidos. Requisitos: título de tercer nivel, 5 años de experiencia y formación específica en protección de datos.

RESUMEN EJECUTIVO

¿En qué nivel de cumplimiento está su empresa?

Use esta escala para evaluar el estado actual de su empresa y priorizar acciones:

NIVEL	DESCRIPCIÓN	RIESGO LEGAL	ACCIÓN
0 — Sin cumplimiento	No hay documentos ni procesos de protección de datos	**MUY ALTO**	Iniciar diagnóstico urgente
1 — Inicial	Hay conciencia del tema pero sin documentación formal	**ALTO**	Priorizar RAT y Política
2 — En proceso	Algunos documentos elaborados, procesos parcialmente implementados	**MEDIO**	Completar documentación y capacitar
3 — Cumplimiento básico	Documentos completos, procesos implementados y personal capacitado	**BAJO**	Monitoreo y actualización anual
4 — Maduro	Cumplimiento continuo, mejora periódica, DPD o responsable activo	**MUY BAJO**	Mantener y mejorar

Checklist rápido de estado — marque lo que ya tiene:

☐	Política de Protección de Datos aprobada y publicada	*BLOQUE B · #1*
☐	Registro de Actividades de Tratamiento completo	*BLOQUE B · #2*
☐	Avisos de Privacidad entregados a clientes, empleados y proveedores	*BLOQUE B · #3*
☐	Procedimiento ARCO+ documentado y canal habilitado	*BLOQUE B · #4*
☐	Análisis de riesgos realizado	*BLOQUE B · #5*
☐	Protocolo de incidentes de seguridad definido	*BLOQUE B · #6*
☐	Contratos laborales con cláusulas de datos actualizados	*BLOQUE B · #7*
☐	Contratos con proveedores con cláusulas de encargo firmados	*BLOQUE B · #8*
☐	Personal capacitado con evidencia conservada	*BLOQUE B · #9*
☐	Controles técnicos: acceso, cifrado, copias de seguridad	*BLOQUE C*
☐	DPD o responsable interno designado (si aplica)	*BLOQUE D*

Esta guía fue elaborada por **Delta Legal S.A.S.** con fines informativos. La normativa puede actualizarse. Consulte siempre la versión vigente de la LOPDP, su Reglamento y las resoluciones de la Superintendencia de Protección de Datos.