MENTINNO
INTELIGENCIA & ANALÍTICA DE NEGOCIOS

Cumplimiento DATA & IA 2026

Checklist corporativo accionable para responsables de negocio, tecnología, legal, riesgo y talento en Ecuador.

LOPDP · LOTDA · SPDP IA · Estrategia Nacional de IA

- **Gobernanza**
- **Consentimiento**
- **Derechos ARCO+**
- **Seguridad**
- **IA Responsable**
- **Terceros**
- **Auditoría**

Versión ejecutiva | Mayo 2026

El cumplimiento dejó de ser un trámite legal

Debe operar como sistema de gestión: evidencias, responsables, controles y mejora continua.

Lo que cambia para las empresas

- ☐ La protección de datos exige responsabilidad proactiva y evidencia verificable.
- ☐ La IA agrega nuevos deberes: transparencia, supervisión humana, evaluación de riesgos y trazabilidad.
- ☐ Los incidentes de seguridad activan plazos críticos y documentación obligatoria.

Principio operativo

No basta con declarar cumplimiento. Hay que demostrarlo con registros, decisiones documentadas, dueños de control, medición periódica y capacidad de respuesta.

Mapa del ecosistema normativo DATA & IA

Una lectura integrada para responsables corporativos.

LOPDP

Base legal del tratamiento de datos, derechos de titulares, obligaciones, seguridad y sanciones.

Reglamento LOPDP

Procedimientos, Registro Nacional, DPO, brechas y operación de la autoridad.

LOTDA

Transformación digital, servicios digitales, eficiencia, interoperabilidad y confianza digital.

SPDP IA 2026

Reglas específicas para IA cuando trate datos personales: roles, información, riesgos, auditoría.

Estrategia Nacional IA

Marco país para innovación, talento, infraestructura, ética, sostenibilidad e inclusión.

Acción recomendada

Taller de estrategia y gobernanza de Datos e IA

Modelo operativo de cumplimiento en 8 fases

De la política al control recurrente.

Cada fase debe traducirse en controles mínimos: política, responsable, evidencia, frecuencia de revisión y KPI.

Criterio de éxito: pasar de “cumplimos porque existe un documento” a “cumplimos porque existe un sistema vivo, auditable y medido”.

Checklist ejecutivo para responsables de empresas

12 controles mínimos para activar cumplimiento con evidencia.

01	**Mapa de datos y sistemas IA**	Legal + Tecnología
02	**Base legal y consentimiento por finalidad**	Legal + Marketing
03	**Política de privacidad 2026 publicada**	Legal + CX
04	**Registro de Actividades de Tratamiento actualizado**	DPO + Procesos
05	**DPO designado y notificado cuando aplique**	Dirección + Legal
06	**Canal ARCO+ con SLA y trazabilidad**	CX + Legal
07	**DPIA para tratamientos de alto riesgo e IA**	Riesgo + DPO
08	**Controles de seguridad y logs permanentes**	CISO + TI
09	**Plan de brechas probado con simulacro**	CISO + Legal
10	**Contratos con encargados y transferencias revisadas**	Compras + Legal
11	**Inventario y clasificación de roles IA**	Innovación + TI
12	**Auditoría trimestral y mejora continua**	Comité DATA & IA

Fase 1 · Gobernanza y responsabilidad proactiva

Sin gobierno no hay cumplimiento sostenible.

- ☐ Designar sponsor ejecutivo y Comité DATA & IA. — **CEO**
- ☐ Actualizar inventario de bases de datos, tratamientos y sistemas de IA. — **DPO**
- ☐ Formalizar DPO / delegado cuando aplique y documentar funciones. — **Legal**
- ☐ Mantener RAT con finalidad, base legal, categorías, terceros, riesgos y medidas. — **DPO**
- ☐ Definir política corporativa de uso responsable de IA y datos. — **Comité**

Evidencias esperadas

Acta de comité · matriz RAT · nombramiento DPO · política DATA & IA · inventario de modelos y proveedores.

KPI sugerido

% tratamientos registrados y con responsable asignado.

Fases 2 y 3 · Consentimiento, transparencia y derechos ARCO+

El titular debe entender, decidir y reclamar sin fricción.

Captación y consentimiento

- ☐ Avisos claros por finalidad y canal.
- ☐ Consentimiento libre, específico, informado e inequívoco cuando sea la base legal.
- ☐ Aviso explícito de automatización o IA cuando aplique.
- ☐ Tratamiento reforzado para datos sensibles y menores.

Derechos ARCO+

- ☐ Canal gratuito físico o digital.
- ☐ SLA interno para acceso, rectificación, eliminación, oposición, portabilidad y no decisión automatizada.
- ☐ Bitácora de reclamos, respuesta y cierre.
- ☐ Criterios de escalamiento a Legal/DPO.

Diseño práctico: *conectar formularios, CRM, mesa de ayuda y DPO en una sola trazabilidad.*

Fase 4 · Seguridad y ciberseguridad

La seguridad es control legal, operativo y reputacional.

Datos

Minimización · cifrado · anonimización · seudonimización

Identidad

MFA · privilegios mínimos · segregación de funciones

Sistemas

Hardening · parches · monitoreo · backups

Operación

Logs · alertas · respuesta · lecciones aprendidas

Controles accionables

1) Matriz de accesos mensual · 2) Retención y destrucción de datos · 3) Pruebas de restauración · 4) Revisión de logs · 5) Hardening de ambientes IA.

Fase 5A · Clasificación de roles en IA

El rol define la obligación, la evidencia y el riesgo contractual.

Desarrollador

Crea o entrena el sistema.

Diseño ético, pruebas, mitigación de sesgos.

Desplegador

Usa IA para prestar un servicio.

Información al usuario, supervisión humana.

Distribuidor

Comercializa o provee el sistema.

Debida diligencia y cumplimiento local.

Implementador

Integra IA en procesos internos.

DPIA, control operativo y monitoreo.

Pregunta de control: ¿para cada sistema de IA sabemos si somos quien lo desarrolla, lo implementa, lo despliega o lo distribuye?

Fase 5B · DPIA, comités y gobernanza ética

Todo sistema de alto riesgo debe pasar por evaluación antes de operar.

1. Describir tratamiento y finalidad
2. Identificar datos, titulares y terceros
3. Evaluar necesidad, proporcionalidad y base legal
4. Medir riesgos para derechos y libertades
5. Definir mitigaciones, responsables y monitoreo

Mínimo accionable **Ningún modelo con datos personales sensibles, perfilamiento o decisiones automatizadas debería pasar a producción sin DPIA, aprobación de comité y plan de monitoreo.**

Fase 6 · Gestión de brechas e incidentes

El reloj comienza cuando se detecta la brecha.

3

días máximo

para notificar a la autoridad cuando corresponda, acompañado de documentación y plan de mitigación.

- ☐ Contener: aislar, preservar evidencia, cortar vectores de ataque. — **CISO**
- ☐ Evaluar: tipo de dato, volumen, titulares, riesgo y causa raíz. — **DPO**
- ☐ Notificar: autoridad, titulares y terceros críticos según proceda. — **Legal**
- ☐ Remediar: plan, responsables, fechas, comunicación y auditoría post-incidente. — **Comité**

Simulacro recomendado

Realizar al menos un tabletop semestral: ransomware, fuga por proveedor, error humano y exposición pública de base.

KPI: tiempo de detección, tiempo de contención y cierre de acciones correctivas.

Fases 7 y 8 · Terceros, transferencias y auditoría

El riesgo de datos viaja por la cadena de valor.

Antes de contratar

Due diligence de seguridad, privacidad, subencargados, ubicación de datos y uso de IA.

Durante el servicio

Cláusulas de tratamiento, instrucciones documentadas, confidencialidad, SLA, auditoría y brechas.

Después / continuo

Devolución o eliminación de datos, revisión anual, auditoría algorítmica y mejora continua.

Control crítico: ningún proveedor que trate datos personales o integre IA debería operar sin anexo de tratamiento de datos y matriz de riesgos.

Roadmap 30-60-90 días

Convertir cumplimiento en ejecución medible.

0-30 días

Diagnóstico

Inventario de datos e IA · gap assessment · sponsor · comité · quick wins críticos

31-60 días

Diseño

Políticas · RAT · DPIA prioritarios · contratos · plan de brechas · canal ARCO+

61-90 días

Operación

Simulacro · tablero KPIs · auditoría interna · capacitación · plan anual de mejora

Criterio de éxito: al día 90 debe existir tablero ejecutivo con % avance por control, evidencia adjunta, riesgo residual y próxima acción.

Matriz RACI mínima

Claridad de responsabilidad para evitar cumplimiento “de nadie”.

Control	CEO	Legal/DPO	TI/CISO	Negocio	Proveedor
Gobierno DATA & IA	**A**	**R**	**C**	**C**	**I**
RAT e inventario IA	**I**	**R**	**C**	**C**	**I**
Consentimiento y privacidad	**I**	**A/R**	**C**	**R**	**I**
Seguridad y brechas	**I**	**C**	**A/R**	**C**	**C**
DPIA y alto riesgo	**A**	**R**	**C**	**C**	**I**
Contratos terceros	**I**	**A/R**	**C**	**C**	**R**

A = Accountable · R = Responsible · C = Consulted · I = Informed

Glosario ejecutivo

Conceptos mínimos para alinear Legal, Tecnología y Negocio.

Dato personal	Información que identifica o hace identificable a una persona natural.
Dato sensible	Dato que puede afectar intimidad, derechos o generar discriminación.
Responsable	Quien decide fines y medios del tratamiento.
Encargado	Quien trata datos por cuenta del responsable.
DPO / Delegado	Rol de asesoría, supervisión y enlace en protección de datos.
RAT	Registro de Actividades de Tratamiento.
DPIA	Evaluación de Impacto de Protección de Datos.
ARCO+	Acceso, rectificación, eliminación, oposición, portabilidad y derechos frente a automatización.
IA	Sistema capaz de inferir, recomendar, clasificar o generar resultados a partir de datos.
Auditoría algorítmica	Revisión de trazabilidad, sesgos, desempeño, explicabilidad y controles.

Fuentes y advertencia de uso

Este material es una guía corporativa, no sustituye asesoría legal específica.

Ley Orgánica de Protección de Datos Personales - Registro Oficial Suplemento 459, 26-may-2021	Ministerio de Telecomunicaciones / Registro Oficial
Reglamento General a la LOPDP - Decreto Ejecutivo No. 904, Registro Oficial Tercer Suplemento 435, 13-nov-2023	Presidencia de la República / MINTEL
Ley Orgánica para la Transformación Digital y Audiovisual - Registro Oficial 245, 07-feb-2023	Gob.ec / SRI
Resolución SPDP-SPD-2026-0009-R - Norma para protección de datos en sistemas de IA, publicada en Registro Oficial No. 240, 10-mar-2026	SPDP / Registro Oficial; referencias legales secundarias
Estrategia Nacional de Inteligencia Artificial de Ecuador	MINTEL
Presentación base: Mentinno DATA & IA Compliance Checklist 2026	Archivo cargado por el usuario

Recomendación: validar con asesoría legal local antes de usar esta presentación como política corporativa o matriz de cumplimiento formal.