

G.2 Protección de datos y cumplimiento

Eje transversal · Gobernanza, Seguridad y Cumplimiento · Ficha de capacidad



Framework de Adopción de IA v1.4
Espacio de Innovación con IA · CESSI

PREGUNTA CLAVE

¿Sabemos qué datos propios y de clientes se exponen a qué modelo, con qué acuerdo — y las demos corren sobre datos seguros?

POR QUÉ IMPORTA

Responder 'cumplimos Ley 25.326' en un RFP sin haber revisado qué hacen los proveedores con lo que el equipo sube a diario es compliance declarativo. Para exportadores, los clientes preguntan esto antes que el precio.

LOS CUATRO NIVELES

N1

No se evalúa qué se expone; las demos usan datos reales sin autorización.

N2

Restricciones básicas comunicadas, primeras revisiones de términos, anonimización artesanal en demos sensibles.

N3

Controles técnicos y contractuales: clasificación, acuerdos con proveedores, cláusulas de IA con clientes, Ley 25.326 revisada con asesoría, datos seguros por defecto en demos y pilotos (sintéticos, anonimizados u otros controles según riesgo).

N4

Privacidad by design en todo el ciclo, auditable; abre sectores regulados y exportación; demostrar sin exponer es diferencial de venta.

CÓMO SUBIR UN NIVEL

Transición	Acción	Tiempo (est.)	Quién	Evidencia de hecho
N1 → N2	Clasificar lo obvio (confidencial, de cliente, público), comunicar 3 reglas de exposición, instalar la regla 'las demos no usan datos reales de clientes' y leer los términos de los 3 proveedores más usados.	3-4 semanas	Responsable de seguridad + dirección	Clasificación básica publicada; términos de los 3 proveedores revisados; regla de demos vigente.
N2 → N3	Formalizar con asesoría legal: matriz datos vs. herramientas permitidas, acuerdos de procesamiento con proveedores, revisión de contratos con clientes sobre uso de IA, y sistematización de datos sintéticos.	2 trimestres	Seguridad + legales + plataforma	Matriz vigente; acuerdos firmados; % de demos sobre datos sintéticos > 90%. Requiere revisión legal.
N3 → N4	Elevar a estándar exportable (marcos internacionales de privacidad y gestión de riesgo de IA) y auditar periódicamente.	2-3 trimestres	Seguridad + calidad	Auditoría periódica registrada; cero incidentes de exposición en pruebas.

QUÉ MEDIR

% de herramientas con términos revisados y acuerdo vigente
· Datos clasificados vs. total relevante · % de demos y pilotos sobre datos sintéticos o anonimizados

Tablero: Se lee con M5 y M8.

VARIANTES POR PERFIL

PyME (≈30). Tres reglas de exposición y la regla de demos ya son N2; la asesoría legal para N3 puede ser puntual.

Empresa grande (≈500). Fintech, salud y gobierno: condición de entrada; validar requisitos específicos (BCRA u organismo correspondiente) con asesoría.

ANTI-PATRÓN

El compliance declarativo: 'cumplimos' en el RFP sin que nadie haya revisado los proveedores.

EN QUÉ SE APOYA

Laney (lo que no está clasificado no se puede proteger ni valorar) · Agrawal et al. (datos de entrada y de entrenamiento son componentes distintos: preguntar por ambos). Ley 25.326 e ISO/IEC 42001 orientan y requieren validación legal.

Ver también: G.1 · 4.1 · 4.4