Clase 9 — Protección de datos personales y bases de datos.

Desarrollo para exposición oral, con preguntas al curso, ejemplos de arquitectura de software y taller integrador. La guía de resolución del taller es material docente: separar esa sección si se comparte la consigna con estudiantes.

Pregunta que organiza el encuentro: "¿Qué decisiones tenemos que cambiar para que TurnoApp respete a las personas cuyos datos utiliza?".

El recorrido oral se apoya en un mismo caso. Las transcripciones normativas desplegables son material de consulta: no se leen todas en voz alta. En clase se seleccionan las frases decisivas y se las aplica; el resto queda como respaldo para estudiar. Los apartados técnicos ampliados y la guía de resolución tampoco son contenido para exponer íntegramente.

Al terminar, cada estudiante debería poder:

- Reconocer datos personales, sensibles y datos aparentemente anónimos que permiten reidentificar.
- Vincular una finalidad concreta con los datos estrictamente necesarios.
- Distinguir consentimiento, excepciones legales, información y seguridad.
- Diseñar funcionalidades que permitan ejercer derechos.
- Identificar riesgos de proveedores, nube, logs y ambientes de prueba.
- Diferenciar obligaciones argentinas de estándares europeos.

I. Apertura — ¿Por qué esto le importa a quien programa?

"Hasta ahora trabajamos quiénes pueden contratar, cómo se forma el consentimiento y qué responsabilidades aparecen cuando desarrollamos software. Hoy vamos a mirar un componente presente en casi todos esos proyectos: los datos personales.

Imaginen que una clínica les pide una aplicación de turnos. El formulario solicita nombre, DNI, teléfono, fecha de nacimiento, diagnóstico, ubicación permanente y acceso a contactos.

Desde lo técnico podemos crear todas esas columnas. La pregunta jurídica es otra: ¿necesitamos todos esos datos?, ¿para qué?, ¿quién puede verlos?, ¿cuándo se borran?, ¿qué ocurre si alguien pide una copia o denuncia un error?

El problema puede empezar antes de un ataque informático: en el formulario, en el modelo de datos, en una configuración por defecto o en una copia de producción que alguien descarga para probar un bug.

Una base puede estar cifrada y, sin embargo, ser jurídicamente problemática porque recolecta información excesiva o la usa para una finalidad incompatible".

Preguntas al curso

TurnoApp — Escena 1: el pedido del cliente

La clínica es ficticia. Atiende en Argentina y contrata a un equipo para organizar reservas y recordatorios. No se presume todavía que opere en Europa. La aplicación no necesita ser una historia clínica completa.

El cliente propone: "Pidamos todo ahora; después veremos para qué sirve. Y pongamos un solo aceptar para cubrirnos".

Intervención docente: “Antes de abrir el editor, escriban dos columnas: finalidad y dato necesario. No decidan todavía con una casilla de consentimiento”.

Respuesta orientativa: organizar un turno puede justificar identificar a la persona y disponer de un canal de contacto. No demuestra por sí solo que sean necesarios religión, contactos del teléfono, diagnóstico detallado o ubicación permanente. Algunos identificadores pueden requerirse por el contexto sanitario, pero hay que justificarlo, no suponerlo.

Recoger dos respuestas sin corregir todo de inmediato. Volver a ellas al trabajar los arts. 4, 5 y 6.

- ¿Un dato publicado en internet puede utilizarse para cualquier cosa?
- ¿Aceptar términos y condiciones equivale a autorizar cualquier tratamiento?
- ¿Si reemplazo el nombre por un número, el dato deja de ser personal?
- ¿Borrar la cuenta implica borrar absolutamente todos los registros?

Fundamento constitucional

Los arts. 18 y 19 de la Constitución Nacional protegen, entre otros aspectos, las comunicaciones, la intimidad y la esfera de autonomía personal. El tercer párrafo del art. 43 contempla el hábeas data: conocimiento de datos y finalidad, y mecanismos de supresión, rectificación, confidencialidad o actualización en los supuestos constitucionales.

Constitución Nacional — Artículo 18 — Texto completo

> “Ningún habitante de la Nación puede ser penado sin juicio previo fundado en ley anterior al hecho del proceso, ni juzgado por comisiones especiales, o sacado de los jueces designados por la ley antes del hecho de la causa. Nadie puede ser obligado a declarar contra sí mismo; ni arrestado sino en virtud de orden escrita de

autoridad competente. Es inviolable la defensa en juicio de la persona y de los derechos. El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación. Quedan abolidos para siempre la pena de muerte por causas políticas, toda especie de tormento y los azotes. Las cárceles de la Nación serán sanas y limpias, para seguridad y no para castigo de los reos detenidos en ellas, y toda medida que a pretexto de precaución conduzca a mortificarlos más allá de lo que aquélla exija, hará responsable al juez que la autorice."

Aplicación a la clase: la protección de la correspondencia y los papeles privados permite abordar la tutela constitucional de comunicaciones y documentación digitales. Esta aplicación es una interpretación jurídica, no una mención literal a internet en el texto constitucional.

Constitución Nacional — Artículo 19 — Texto completo

"Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe."

Aplicación a la clase: sustenta la protección de la privacidad y la autonomía personal frente a intromisiones injustificadas, también en entornos digitales.

Constitución Nacional — Artículo 43, tercer párrafo — Transcripción del párrafo pertinente

"Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o

discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística."

Aplicación a la clase: es el fundamento constitucional específico del hábeas data. La cita reproduce solamente el tercer párrafo, no la totalidad del artículo 43, que también regula amparo y hábeas corpus.

Fuente oficial de los artículos constitucionales — Ley 24.430.

La Ley 25.326 desarrolla un régimen de protección. Su art. 1 comprende archivos públicos y privados destinados a dar informes y prevé aplicación pertinente a datos de personas jurídicas. No conviene enseñar que cualquier archivo doméstico recibe automáticamente el mismo tratamiento que una base comercial, ni reducir el régimen a empresas que venden informes: deben examinarse el uso, los flujos y la reglamentación.

Ley 25.326 — Artículo 1 — Texto completo

"ARTICULO 1° — (Objeto).

La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.

Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal.

En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas."

Aplicación a la clase: la norma protege a las personas respecto del tratamiento de sus datos, no solamente la seguridad técnica de los archivos. La expresión "personas de existencia ideal" corresponde al texto legal transcripto y se vincula con las personas jurídicas.

Fuente oficial — Ley 25.326, texto actualizado, artículo 1.

Idea didáctica: la protección no se limita a datos secretos. Un dato verdadero también puede utilizarse indebidamente.

II. Definiciones — Qué protegemos y qué significa tratar

Explicación para construir el concepto

"La ley no protege solamente un archivo: protege a las personas frente a lo que podemos hacer con la información sobre ellas. Primero preguntamos si alguien es identificable; después analizamos si el tratamiento está permitido. Que un dato sea personal no significa que esté prohibido usarlo".

Determinado es alguien ya identificado. Determinable es alguien que podemos llegar a identificar: el paciente 348 sigue siendo identificable si otra tabla vincula ese número con su identidad. No hace falta que cada empleado vea la tabla de correspondencias para que el sistema siga tratando datos personales.

Privacidad y protección de datos se relacionan, pero no son sinónimos de secreto. Que una persona publique su profesión no significa que autorice cualquier perfil, combinación o uso comercial de esa información.

- Lectura normativa — Ley 25.326, art. 2: definiciones seleccionadas, transcripción literal

"— Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables."

"— Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual."

"— Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso."

"— Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias."

"— Responsable de archivo, registro, base o banco de datos: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos."

"— Titular de los datos: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley."

"— Usuario de datos: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos."

"— Disociación de datos: Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable."

Son definiciones seleccionadas, no la totalidad del artículo. La terminología "existencia ideal" se conserva por fidelidad al texto legal.

Fuente oficial — Ley 25.326, art. 2.

Comprobación rápida — Cuatro datos de TurnoApp

da	
una cuenta	te vincular a alguien
ılado al paciente 348 e	) elimina la vinculación; revela salud
ıimato	nculación o comprobación de valores
turnos por mes	ıo si no permite individualizar; una celda ede revelar información

No corregir "sensible" por la impresión de que un dato es delicado: pedir que se identifique la categoría legal. Un dato fuera de esa enumeración también puede generar riesgos graves.

1. Dato personal — art. 2 de la Ley 25.326

Es información de cualquier tipo referida a personas determinadas o determinables.

No hace falta que aparezcan nombre y apellido. Si el dato puede vincularse razonablemente con una persona, directamente o combinado con otra información, hay que analizarlo como dato personal.

Ejemplos:

- Nombre, DNI, correo y teléfono.
- Foto identificable.
- Identificador de cliente relacionado con una tabla de usuarios.
- Historial de compras asociado a una cuenta.
- Dirección IP, identificador de dispositivo o ubicación cuando permitan identificar o vincular a una persona según el contexto.

No toda IP identifica por sí sola a una persona concreta. Tampoco es correcto descartarla automáticamente porque "es un dato técnico".

Pregunta: "Si en un log guardo user_id, ubicación, hora y compras, pero no el nombre, ¿realmente dejé de tratar datos personales?".

2. Dato sensible — art. 2

La ley enumera datos que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical, salud o vida sexual.

Ejemplos:

- Diagnóstico o medicación.
- Afiliación sindical.

- Información que revele una convicción religiosa.
- Datos de consultas que, por su contexto, revelen salud o vida sexual.

Distinción importante: contraseña, cuenta bancaria o DNI requieren protección reforzada por su riesgo, pero no integran por ese solo motivo la enumeración legal de datos sensibles del art. 2.

La biometría tampoco aparece expresamente nombrada en esa enumeración. Su evaluación exige considerar finalidad, capacidad identificadora, información que revela y criterios complementarios; no trasladar sin aclaración la clasificación del GDPR a la ley argentina.

3. Tratamiento

Tratar no es solamente almacenar. El art. 2 incluye recolección, conservación, modificación, relacionamiento, evaluación, bloqueo, destrucción y comunicaciones a terceros.

También tratamos cuando:

- Exportamos un CSV.
- Ejecutamos una consulta.
- Copiamos producción a desarrollo.
- Enviamos un archivo al soporte.
- Integramos una herramienta de analítica.
- Cargamos información en un servicio de IA.
- Eliminamos registros.

Una operación de solo lectura también puede tener relevancia jurídica.

4. Base de datos

Conjunto organizado de datos personales, electrónico o no. Puede ser una base SQL, una planilla, un CRM o un archivo organizado en papel.

Cambiar PostgreSQL por una planilla no elimina las obligaciones.

5. Disociación, anonimización y seudonimización

La ley define disociación como un tratamiento que impide asociar la información a una persona determinada o determinable.

Para explicar técnicamente:

- Seudonimización: sustituimos identificadores, pero conservamos una posibilidad de vinculación.
- Anonimización efectiva: la información no permite identificar a una persona considerando el contexto y las posibilidades de reidentificación.
- Cifrado: protege el acceso, pero permite recuperar el dato con la clave; no equivale a anonimizar.

Ejemplo: reemplazar DNI por su hash no garantiza anonimato. Si el universo de valores es previsible, puede ser posible probar combinaciones. Si hay una tabla de correspondencias, la vinculación continúa.

6. Quién hace qué

- Titular del dato: la persona a la que la información se refiere.
- Responsable de la base: quien es titular del archivo o banco, según la definición legal.
- Prestador de tratamiento por cuenta de terceros: empresa o profesional que procesa información para otro; art. 25.
- Personal autorizado: participa en el tratamiento y debe respetar permisos y confidencialidad.

En el GDPR se utilizan las categorías de responsable y encargado con definiciones propias. Sirven para comparar, pero no deben presentarse como transcripción literal de la Ley 25.326.

Ser dueño de los servidores no convierte al proveedor en dueño de los derechos sobre la información de las personas.

III. Principios jurídicos traducidos a requisitos de software

TurnoApp — Escena 2: un formulario no se justifica con "por las dudas"

"El cliente nos pide que conservemos religión y GPS permanente porque podrían servir para futuros productos. La pregunta no es si la columna ocupa poco espacio: es si el dato es adecuado y necesario para la finalidad actual".

La finalidad es el para qué; la necesidad vincula cada dato con ese para qué; la proporcionalidad impide recolectar más de lo justificado. La seguridad responde cómo proteger lo que corresponde tratar, pero no legitima una recolección excesiva.

Ejemplo de razonamiento completo: "Para avisar una reprogramación necesitamos un canal de contacto. No hemos demostrado que hagan falta simultáneamente correo, teléfono, acceso a contactos y ubicación continua. Elegimos el canal suficiente y documentamos la decisión".

- Lectura normativa — Ley 25.326, art. 4 completo

"ARTICULO 4° — (Calidad de los datos).

1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.
3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.
4. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario.
5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley.
6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.
7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados."

- Fuente oficial — Ley 25.326, art. 4.

Del principio a una tarea verificable

noApp **o**

permanente si no hay necesidad y tráfico; no basta ocultar el

de turnos a publicidad sin análisis tegraciones y pruebas de los

ón de contacto a mensajería ción y registro de actualización

or categoría ı y ejecución comprobada del

os vinculados al titular ıd y entrega comprensible

Transición oral: "Ya sabemos qué datos tienen sentido. Ahora falta responder algo diferente: ¿qué nos habilita a tratarlos y qué debemos informar?".

1. Calidad, pertinencia y no exceso — art. 4

Los datos deben ser ciertos, adecuados, pertinentes y no excesivos respecto de la finalidad.

"Si mi app organiza turnos, cada campo del formulario debe tener una explicación. No alcanza con 'quizás después nos sirva'".

Ejemplo:

- Nombre y un canal de contacto pueden ser necesarios.
- DNI: justificar según identificación y contexto asistencial; no pedirlo por costumbre.
- Ubicación permanente: no se justifica solamente para elegir una sucursal.
- Contactos del teléfono: no se justifican para reservar un turno.

Traducción técnica: inventario de campos con finalidad, necesidad, acceso y conservación. Minimizar también reduce exposición y costo de respuesta.

2. Finalidad — art. 4.3

Los datos no pueden utilizarse para fines distintos o incompatibles con los que motivaron su obtención.

Dar un teléfono para recordar un turno no autoriza automáticamente publicidad de terceros. Una excepción de consentimiento para prestar el servicio no habilita cualquier uso posterior.

Pregunta guía: "¿Este uso resulta compatible con la razón por la que recibimos el dato? ¿Qué fundamento concreto lo permite?".

3. Exactitud y actualización — art. 4

El sistema debe permitir corregir información y evitar que un error siga propagándose.

Ejemplo: un teléfono incorrecto puede revelar un turno médico a otra persona. Actualizar no es solo una mejora de experiencia de usuario: puede prevenir una afectación de confidencialidad.

Requisito técnico: identificar réplicas, cachés, integraciones y procesos que deban recibir la corrección.

4. Conservación limitada — arts. 4.7 y 16

Los datos deben destruirse cuando dejan de ser necesarios o pertinentes. A la vez, pueden existir obligaciones legales de conservación o derechos de terceros que impidan una supresión inmediata.

No enseñar “guardar todo para siempre” ni “borrar todo ante cualquier pedido”.

Definir:

- Dato o categoría.
- Finalidad.
- Plazo o criterio de conservación.
- Fundamento.
- Acceso durante la conservación.
- Procedimiento de eliminación o disociación.

La baja de una cuenta no necesariamente autoriza borrar documentación fiscal o sanitaria que deba conservarse. La respuesta debe discriminar qué se elimina y qué se conserva restringido, por qué y durante cuánto tiempo.

5. Información — art. 6

- Lectura normativa — Ley 25.326, art. 6 completo

  “ARTICULO 6° — (Información).

  Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:

  a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios;

  b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable;

c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente;

d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;

e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos."

Fuente oficial — Ley 25.326, art. 6.

Explicación oral: "Informar no es lo mismo que pedir autorización. Aunque un tratamiento no necesite consentimiento por una excepción aplicable, eso no borra automáticamente los deberes de información, calidad y seguridad. Un aviso describe la práctica; no la vuelve lícita por el solo hecho de publicarla".

Antes de recolectar, informar en forma expresa y clara:

- Finalidad y destinatarios o sus categorías.
- Existencia de la base e identidad y domicilio del responsable.
- Qué respuestas son obligatorias y cuáles facultativas.
- Consecuencias de aportar, negar o proporcionar datos inexactos.
- Posibilidad de ejercer acceso, rectificación y supresión.

Una política extensa escondida al pie no reemplaza un aviso comprensible en el punto de recolección.

6. Seguridad y confidencialidad — arts. 9 y 10

Seguridad: adoptar medidas técnicas y organizativas necesarias frente a alteración, pérdida y consulta o tratamiento no autorizado.

Confidencialidad: las personas que intervienen deben guardar secreto; la obligación subsiste después de terminar la relación.

"Que alguien tenga una cuenta válida no significa que pueda consultar a cualquier paciente. Autenticación y autorización no son lo mismo".

IV. Consentimiento — Cuándo corresponde y qué no resuelve

Tres preguntas que no se reemplazan entre sí

1. ¿El dato y la finalidad son admisibles y necesarios?
2. ¿Qué fundamento habilita este tratamiento: consentimiento o una excepción aplicable?
3. ¿Qué información y garantías debemos proporcionar de todas maneras?

"Un consentimiento no arregla cualquier problema. Si para reservar un turno exijo aceptar que el proveedor use diagnósticos para su producto, no resolví el régimen de datos sensibles, la finalidad ni la libertad de elección. Solo agregué una pantalla".

TurnoApp — Escena 3: recordatorio no es publicidad

El teléfono se aporta para avisar sobre la reserva. Después el proveedor propone usarlo para promociones de un tercero.

Pregunta al grupo: "¿Estamos ante el mismo uso?".

Respuesta esperada: no se debe presumir. La publicidad y la comunicación a terceros requieren un análisis propio; una habilitación para gestionar el turno no autoriza indiscriminadamente los demás usos. Tampoco corresponde exigir

consentimiento para cada operación necesaria de una relación contractual si una excepción legal resulta aplicable. Deben analizarse los hechos y las reglas específicas.

- Lectura normativa — Ley 25.326, art. 5 completo

"ARTICULO 5° — (Consentimiento).

1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.

- El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley.

1. No será necesario el consentimiento cuando:

- a) Los datos se obtengan de fuentes de acceso público irrestricto;

b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;

c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;

d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;

e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones

del artículo 39 de la Ley 21.526."

Fuente oficial — Ley 25.326, art. 5.

Regla del art. 5

El consentimiento debe ser libre, expreso e informado y constar por escrito o por un medio equiparable según las circunstancias. Si se presenta junto a otras declaraciones, debe figurar de forma expresa y destacada.

No basta un campo booleano si después no podemos reconstruir:

- Qué se informó.
- Qué finalidad se autorizó.
- Qué acción realizó la persona.
- Qué versión del texto se mostró.
- Cuándo ocurrió.

Estos son criterios de evidencia y diseño: no una lista literal de columnas impuesta por la ley.

Excepciones del art. 5.2

La ley prevé, entre otras:

- Fuentes de acceso público irrestricto.
- Funciones estatales u obligación legal.
- Listados limitados a los datos que enumera el inciso c.
- Relación contractual, científica o profesional, cuando el dato sea necesario para su desarrollo o cumplimiento.
- Operaciones e información financiera en los términos del inciso e.

Las excepciones no eliminan los demás principios. "Está en internet" no demuestra por sí solo acceso público irrestricto ni vuelve lícita cualquier finalidad.

No importar el "interés legítimo" del art. 6 del GDPR como si fuera una habilitación general autónoma idéntica en el art. 5 argentino. El art. 11 argentino utiliza esa expresión en su régimen de cesión, con requisitos propios.

Datos sensibles — arts. 7 y 8

- Lectura normativa — Ley 25.326, arts. 7 y 8 completos

"ARTICULO 7° — (Categoría de datos).

1. Ninguna persona puede ser obligada a proporcionar datos sensibles.
2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.
3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.
4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas."

- “ARTICULO 8° — (Datos relativos a la salud).

  Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional.”

  Fuente oficial — Ley 25.326, arts. 7 y 8.

Lectura conjunta: no aislar la prohibición del art. 7 para concluir que una clínica nunca puede tratar salud, ni aislar el art. 8 para concluir que puede usar esos datos para cualquier negocio. En TurnoApp hay que distinguir atención sanitaria, administración del turno y reutilización comercial del proveedor. Son operaciones y finalidades diferentes.

El tratamiento tiene restricciones específicas. No se resuelve con agregar una casilla “acepto datos sensibles”.

El art. 7 regula supuestos limitados y prohíbe obligar a proporcionar esos datos. El art. 8 permite a establecimientos sanitarios y profesionales de salud tratar información de pacientes en las condiciones legales y respetando el secreto profesional.

Ejemplo: una clínica puede necesitar información de salud para atender. Eso no habilita a un proveedor a reutilizar historias clínicas para entrenar un producto propio.

Mini-casos para discutir

- Tienda que solicita domicilio para entregar: evaluar necesidad contractual; no exigir consentimiento adicional para todo por reflejo.
- Misma tienda que vende perfiles de compradores: finalidad y cesión requieren análisis independiente.
- App de turnos que exige habilitar publicidad para reservar: cuestionar libertad, necesidad y separación de finalidades.

V. Derechos — Funcionalidades que el sistema debe poder ejecutar

TurnoApp — Escena 4: llega un reclamo realista

Una paciente escribe: "Quiero saber qué guardan sobre mí; mi teléfono está mal y quiero cerrar la cuenta".

"No llegó una sola orden de borrar. Llegaron pedidos distintos: acceso, corrección y una solicitud de baja que exige determinar qué supresión procede. El sistema debe poder identificarlos y tramitarlos sin confundir sus plazos".

Circuito orientativo: recibir y registrar; verificar identidad de manera proporcionada; separar pedidos; fijar vencimientos conforme a la ley; buscar en los sistemas pertinentes; ejecutar o justificar límites; responder de forma segura y dejar evidencia.

La automatización ayuda a no perder solicitudes; no debe decidir por sí sola que toda supresión es improcedente. Si hay documentación que deba conservarse, identificar cuál, con qué fundamento y con qué restricción de uso.

- Lectura normativa — Ley 25.326, arts. 14 y 15 completos

"ARTICULO 14. — (Derecho de acceso).

1. El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes.
2. El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente.

- Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley.

1. El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto.
2. El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales."

- "ARTICULO 15. — (Contenido de la información).

1. La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen.
2. La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado.
3. La información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin."

- Fuente oficial — Ley 25.326, arts. 14 y 15.

- Lectura normativa — Ley 25.326, art. 16 completo

"ARTICULO 16. — (Derecho de rectificación, actualización o supresión).

1. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos.
2. El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.
3. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data prevista en la presente ley.
4. En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato.
5. La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.
6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión.

7. Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos."

- Fuente oficial — Ley 25.326, art. 16.

Diferencias

	uelve	**rincipal**
	ı de mí?	›s desde intimación fehaciente,
ualización	› errado o desactualizado?	.s hábiles, art. 16.2
ente	le conservarse?	tes de los apartados 5 y 7

No enseñar que se debe esperar una formalidad para corregir un error ya advertido: el art. 16.2 contempla también ese supuesto. El inicio legal del plazo de acceso y el canal operativo de recepción deben distinguirse sin usar esa diferencia para obstaculizar el derecho.

<aside>
⚖️

Referencia correcta: el acceso está regulado en el art. 14; rectificación, actualización, supresión y confidencialidad, en el art. 16. No atribuir todos esos derechos al art. 14.

</aside>

1. Acceso — arts. 14 y 15

Previa acreditación de identidad, la persona puede conocer sus datos.

El responsable debe informar dentro de diez días corridos de haber sido intimado fehacientemente. La gratuidad del acceso opera a intervalos no inferiores a seis meses, salvo interés legítimo.

La respuesta debe ser clara, comprensible y no revelar datos de terceros. Un JSON crudo lleno de códigos internos puede no satisfacer el deber de claridad.

Diseño:

- Canal identificable.
- Verificación proporcionada de identidad.
- Búsqueda en sistemas pertinentes.
- Exportación comprensible.
- Revisión de información de terceros.
- Entrega segura y constancia de respuesta.

No pedir una foto de DNI automáticamente si existe otro mecanismo suficiente: la verificación también debe minimizar datos.

2. Rectificación y actualización — art. 16

Plazo máximo: cinco días hábiles desde el reclamo o desde que se advierte el error o falsedad.

Durante la verificación, bloquear o indicar que el dato está bajo revisión en los términos legales. Si hubo cesión o transferencia, notificar la corrección o supresión al cesionario dentro del quinto día hábil de realizada.

3. Supresión y confidencialidad

Analizar procedencia y excepciones. Una obligación legal de conservación puede impedir la supresión, pero no autoriza mantener todos los usos ni accesos.

Requisito: un circuito que responda fundadamente y ejecute la decisión, no solamente un botón que desactive el inicio de sesión.

4. Publicidad — art. 27

- Lectura normativa — Ley 25.326, art. 27, apartados 2 y 3

  "2. En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno.

  1. El titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo."
- Se transcriben solamente los apartados sobre derechos; el apartado 1 regula los tratamientos publicitarios comprendidos.

  Fuente oficial — Ley 25.326, art. 27.

La persona puede solicitar en cualquier momento el retiro o bloqueo de su nombre en las bases publicitarias comprendidas.

"ARCO" es una sigla didáctica frecuente, pero en Argentina conviene explicar las reglas concretas. No afirmar que existe una oposición general idéntica a la del GDPR por utilizar esa sigla.

5. Hábeas data y AAIP

Explicación oral: "El derecho es lo que puedo exigir; el hábeas data es una herramienta judicial para hacerlo efectivo. La autoridad administrativa controla el cumplimiento del régimen, pero no es un tribunal. No son dos nombres para el mismo trámite".

- Lectura normativa — Ley 25.326, art. 29.1, incisos a y f, y art. 33.1

  Art. 29.1, funciones seleccionadas del órgano de control:

  "a) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza;"

  "f) Imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la presente ley y de las reglamentaciones que se dicten en su consecuencia;"

  Art. 33.1:

  "1. La acción de protección de los datos personales o de hábeas data procederá:

  a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos;

b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización."

Fuente oficial — Ley 25.326, arts. 29 y 33.

El hábeas data es una vía judicial de protección; la AAIP es autoridad administrativa de control. No son la misma institución ni se debe presentar la denuncia administrativa como requisito previo universal para acudir a la justicia.

La AAIP orienta, fiscaliza, administra registros y puede aplicar sanciones en su competencia. Un incumplimiento puede generar también responsabilidad civil y, si se cumplen sus presupuestos, penal: no todo incidente constituye delito.

VI. Registro — Qué significa inscribir una base

Explicación oral

"El registro no es subir la tabla de pacientes al Estado. Es declarar información sobre el responsable y la base alcanzada. Tampoco es un sello que convierta en correcta cualquier práctica".

En TurnoApp, el inventario de finalidades, datos, accesos, destinatarios y conservación es útil para diseñar, para responder derechos y para evaluar la inscripción. No decidir el alcance por el nombre comercial del producto ni por la tecnología de almacenamiento.

- Lectura normativa — Ley 25.326, art. 3 completo, art. 21.1 y art. 24 completo

"ARTICULO 3° — (Archivos de datos – Licitud).

La formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos, observando en su operación los principios que establece la presente ley y las reglamentaciones que se dicten en su consecuencia.

Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública."

Art. 21, apartado 1:

"1. Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control."

"ARTICULO 24. — (Archivos, registros o bancos de datos privados).

Los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal deberán registrarse conforme lo previsto en el artículo 21."

El art. 21.2 enumera la información registral; se explica debajo sin presentarla como transcripción. El alcance debe completarse con la reglamentación y el procedimiento de la AAIP.

Fuente oficial — Ley 25.326, arts. 3, 21 y 24.

Arts. 3, 21 y 24 de la Ley 25.326, decreto reglamentario y régimen administrativo de la AAIP.

El art. 21 refiere a archivos públicos y privados destinados a proporcionar informes; el art. 24 contempla particulares que formen archivos que no sean de uso exclusivamente personal. Para aplicar el régimen, leer ambos y su reglamentación: no decidir solo porque una base no se vende o no es SQL.

En el procedimiento oficial se distingue:

- Inscribir al responsable.
- Registrar las bases alcanzadas y sus características.

Se informa finalidad, categorías, destinatarios, seguridad, conservación y mecanismos de ejercicio de derechos. No se entrega por esa inscripción una copia de todos los registros personales.

La inscripción no certifica que toda práctica sea lícita ni subsana exceso de datos, mala seguridad o cesiones ilegítimas.

Pregunta: "¿Qué datos del inventario técnico necesitamos para completar correctamente la información registral?".

VII. Seguridad desde la arquitectura

TurnoApp — Escena 5: una cuenta válida accede a otro paciente

Recepción inicia sesión correctamente, cambia el identificador de paciente en una petición y obtiene un diagnóstico que no necesita para su tarea.

Pregunta: "¿Falló la contraseña?".

Respuesta esperada: no necesariamente. Autenticación verifica quién accede; autorización determina qué puede hacer y sobre qué recursos. Deben

controlarse rol, vínculo con el registro y operación en el servidor. Un identificador difícil de adivinar ayuda en ciertos riesgos, pero no reemplaza autorización.

Prueba de aceptación orientativa: una cuenta de recepción intenta consultar un diagnóstico y el servidor rechaza la operación sin devolver el dato. También se prueba que pueda ejecutar las operaciones de agenda legítimamente autorizadas.

- Lectura normativa — Ley 25.326, arts. 9 y 10 completos

  "ARTICULO 9° — (Seguridad de los datos).

  1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.
  2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad."
- "ARTICULO 10. — (Deber de confidencialidad).

  1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos.

2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública."

- Fuente oficial — Ley 25.326, arts. 9 y 10.

La norma fija el deber. La matriz de roles, el control de recursos y las pruebas son una propuesta para cumplirlo; no son una transcripción de herramientas exigidas literalmente.

Obligación legal y elección técnica

El art. 9 establece un deber de seguridad. La Resolución AAIP 47/2018 contiene medidas recomendadas; no presentar cada herramienta de esta sección como mandato textual expreso de la ley.

La selección depende de naturaleza, contexto y riesgos. La ausencia de una marca o algoritmo en el texto legal no elimina la obligación de proteger.

Controles para explicar

- Mínimo privilegio y roles: recepción ve agenda; no necesita el detalle de una historia clínica.
- Autorización en el servidor: ocultar un botón en frontend no protege un endpoint.
- Cifrado en tránsito y reposo: proteger también claves, copias y rutas de exportación.
- Contraseñas: no texto plano ni cifrado reversible como diseño ordinario; usar funciones apropiadas para contraseñas, como Argon2id, con sal y parámetros adecuados.
- MFA para accesos privilegiados y revocación de credenciales.

- Consultas parametrizadas, validación y control de entradas: relevantes para seguridad, no sustituyen finalidad ni consentimiento.
- Backups cifrados y pruebas de restauración.
- Logs suficientes para investigar, sin almacenar contraseñas, tokens completos o datos de salud innecesarios.
- Datos sintéticos en desarrollo; una copia real requiere evaluación, autorización y controles.
- Actualización de dependencias y revisión de permisos.
- Exportaciones controladas y limitadas.

Borrado lógico y backups

Soft delete no equivale a supresión si el dato sigue disponible para usos ordinarios.

Diseñar tratamiento de réplicas, archivos y copias. Si una restauración recupera datos ya suprimidos, el procedimiento debe evitar reactivarlos indebidamente. Documentar plazos, restricciones y fundamentos; no prometer borrado instantáneo de toda copia si la arquitectura no lo permite.

Respuesta a incidentes

TurnoApp — Escena 6: aparece una exportación pública

Soporte detecta un archivo con correos y especialidades médicas accesible mediante un enlace público. Todavía no se sabe quién lo descargó.

Intervención: “Distingan tres tiempos: detener la exposición, investigar el alcance y decidir las comunicaciones que correspondan. No necesitamos saber todo para restringir el enlace; sí necesitamos documentar lo que sabemos y no sabemos”.

Respuesta esperada: restringir acceso; preservar evidencia pertinente sin divulgar más datos; identificar archivo, período y personas potencialmente afectadas; escalar; evaluar riesgos y régimen aplicable. No anunciar automáticamente "no hubo afectados" por falta de prueba de descarga. No afirmar automáticamente que rige el plazo europeo de 72 horas.

Secuencia orientativa:

- Contener el acceso o exposición.
- Preservar evidencia y registrar decisiones.
- Determinar datos, personas, sistemas y período afectados.
- Escalar al equipo responsable.
- Evaluar riesgos y obligaciones de comunicación según régimen aplicable.
- Corregir y verificar.
- Revisar la causa y evitar repetición.

No destruir logs indiscriminadamente para "limpiar" el incidente. Tampoco retrasar la contención para completar primero un informe perfecto.

Una brecha puede afectar confidencialidad, integridad o disponibilidad; no solamente implica publicación de una base robada.

VIII. Proveedores, nube y transferencias internacionales

TurnoApp — Escena 7: el hosting es un tercero, no una solución jurídica automática

La clínica encarga el servicio; el proveedor administra la aplicación; un servicio externo aloja datos y otro envía mensajes. Dibujar esas cuatro piezas y flechas antes de hablar de contratos.

No toda intervención de un proveedor es igual a entregar una base para que la explote por cuenta propia. Distinguir tratamiento por cuenta de otro, cesión y transferencia internacional; pueden concurrir varios análisis en un mismo flujo.

Pregunta: "¿Que el paciente se relacione con la clínica autoriza al desarrollador a reutilizar sus datos para entrenar su propia IA?".

Respuesta esperada: no. El acceso técnico no equivale a autorización para una finalidad propia; tampoco basta que el contrato diga genéricamente "mejora del servicio". Deben analizarse finalidad, datos sensibles y habilitación aplicable.

- Lectura normativa — Ley 25.326, art. 25 completo

  "ARTICULO 25. — (Prestación de servicios informatizados de datos personales).

  1. Cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación.
  2. Una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años."
- Fuente oficial — Ley 25.326, art. 25.

- Lectura normativa — Ley 25.326, art. 11, apartados 1, 2 y 4: cesión

  "1. Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el

interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo.

1. El consentimiento para la cesión es revocable."

- "4. El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate."

No es el artículo completo: el apartado 3 contiene excepciones al consentimiento y debe consultarse al resolver un caso. La referencia al interés legítimo no autoriza a omitir los demás requisitos.

Fuente oficial — Ley 25.326, art. 11 completo.

- Lectura normativa — Ley 25.326, art. 12 completo

"ARTICULO 12. — (Transferencia internacional).

1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no propocionen niveles de protección adecuados.
2. La prohibición no regirá en los siguientes supuestos:

- a) Colaboración judicial internacional;

b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo anterior;

c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable;

d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte;

e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico."

La grafía "propocionen" se reproduce del texto oficial consultado. La lectura operativa debe completarse con el decreto 1558/2001 y los mecanismos de la AAIP: este artículo no agota el régimen.

Fuente oficial — Ley 25.326, art. 12.

Prestación por terceros — art. 25

El prestador no puede usar los datos para una finalidad distinta de la prevista en el contrato ni cederlos por su cuenta.

Revisar:

- Instrucciones y finalidad.
- Accesos, seguridad y confidencialidad.
- Proveedores posteriores y autorizaciones pertinentes.
- Asistencia en derechos e incidentes.
- Destino de datos al finalizar.
- Ubicaciones y transferencias.

El art. 25.2 establece destrucción al finalizar la prestación, con una excepción de conservación autorizada expresamente para posibles encargos ulteriores, bajo seguridad y hasta dos años en ese supuesto. No es un permiso general de conservación por dos años para cualquier base.

Transferencia internacional — art. 12 y reglamentación

La ley restringe las transferencias a países u organismos sin nivel adecuado y contempla excepciones. El decreto 1558/2001 y mecanismos complementarios permiten analizar garantías y supuestos habilitantes.

La normativa de la AAIP incluye mecanismos contractuales; la Resolución 198/2023 aprobó cláusulas modelo vinculadas a la Red Iberoamericana de Protección de Datos.

Antes de contratar un servicio:

- Identificar dónde se almacena.
- Averiguar desde dónde puede acceder soporte.
- Revisar backups y subprestadores.
- Verificar el destino y el mecanismo jurídico aplicable.
- Documentar la decisión.

La nube no es un territorio sin jurisdicción. El domicilio comercial del proveedor no prueba que todos los tratamientos ocurran allí. Un acceso desde el exterior también puede ser relevante y merece evaluación.

IX. GDPR — Comparar sin mezclar regímenes

TurnoApp — Escena 8: el producto quiere salir al exterior

Hasta ahora el caso se desarrolló en Argentina. El proveedor propone ofrecer la aplicación a clínicas y personas que se encuentran en España.

"No reemplazamos una ley por otra porque nos guste más. Primero determinamos qué regímenes alcanzan a cada tratamiento y por qué. Tener servidores en otro país, vender a un cliente europeo y dirigir servicios a personas en la Unión son hechos distintos".

Para los diez minutos de exposición: explicar sigla y alcance; comparar diseño por defecto; cerrar con notificación a la autoridad y comunicación a las personas. Los detalles del DPO y las transcripciones quedan como consulta.

no trabajado

para todo? excepciones, con reglas condiciones pertinentes

so es sensible? as complementarias ales con regulación propia

decisiones de diseño? o y seguridad, entre otros resamente diseño y defecto

ca en 72 horas? regla general a la Ley diciones; art. 34 regula otra

La comparación ayuda a evitar trasplantes automáticos de conceptos, plazos y excepciones; no certifica cumplimiento.

¿Qué es el GDPR?

GDPR es la sigla en inglés de General Data Protection Regulation. En español se denomina Reglamento General de Protección de Datos y se abrevia RGPD. Su identificación normativa es Reglamento (UE) 2016/679.

Es una norma de la Unión Europea que protege a las personas físicas respecto del tratamiento de sus datos personales y regula la libre circulación de esos datos. Establece reglas para las organizaciones que recolectan, almacenan, consultan, utilizan o comparten información personal.

Por ejemplo, una aplicación que registra nombres, correos, ubicaciones o compras no maneja solamente información técnica: trata datos de personas y debe evaluar qué reglas le corresponden.

¿Para qué sirve?

Busca proteger los derechos de las personas frente al uso de su información. Establece principios, derechos y obligaciones:

- Recoger datos para finalidades determinadas y limitarse a los necesarios.
- Explicar de manera transparente cómo se utilizan.
- Contar con una base jurídica que permita el tratamiento: el consentimiento es una de ellas, pero no la única.
- Mantener los datos seguros y no conservarlos indefinidamente sin justificación.
- Permitir que las personas ejerzan sus derechos, dentro de las condiciones y límites del Reglamento.
- Demostrar cumplimiento e incorporar protección desde el diseño del sistema.

No es solamente una norma de ciberseguridad. Una base puede estar bien protegida contra ataques y, aun así, incumplir el GDPR si recoge datos excesivos o los utiliza sin una base jurídica válida.

¿Por qué se llama “reglamento”?

En el sistema jurídico de la Unión Europea, un reglamento es una norma obligatoria y directamente aplicable en los Estados miembros. No es una recomendación ni equivale a un simple reglamento administrativo argentino. En determinadas materias admite normas nacionales complementarias.

¿Qué relación tiene con Argentina?

No es una ley argentina ni reemplaza a la Ley 25.326. Sin embargo, puede alcanzar a organizaciones situadas fuera de Europa cuando se cumplen las condiciones de su ámbito territorial, explicadas en el apartado siguiente.

Ejemplo: una empresa argentina que dirige una aplicación de suscripción a personas que se encuentran en España debe evaluar si queda alcanzada. En cambio, que su página pueda abrirse desde España no basta, por sí solo, para afirmar que se aplica.

También un cliente europeo puede exigir garantías contractuales a un proveedor argentino. Es importante distinguir esas obligaciones contractuales de la aplicación directa del GDPR.

Explicación breve para dar oralmente

“El GDPR es el marco europeo de protección de datos personales. No se ocupa solamente de evitar que roben una base: también exige justificar para qué usamos la información, pedir únicamente lo necesario y respetar los derechos de las personas. Lo estudiamos porque muchas aplicaciones y proveedores trabajan con distintos países, pero sin confundirlo con la ley argentina”.

Fuente oficial — Reglamento (UE) 2016/679, EUR-Lex.

1. Ámbito territorial — art. 3

- Lectura normativa — GDPR, art. 3.1 y letras a y b del apartado 2

  Art. 3.1:

  "1. El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no."

  Art. 3.2, actividades contempladas:

  "a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o"

  "b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión."

  Son fragmentos, no todo el artículo. Para aplicar el apartado 2 deben leerse también sus condiciones introductorias: se refiere al tratamiento por responsables o encargados no establecidos en la Unión en los supuestos allí previstos. No se resuelve por nacionalidad ni por una visita accidental a la web.

  Fuente oficial — GDPR, art. 3.

Puede alcanzar tratamientos relacionados con establecimientos en la Unión y, bajo sus condiciones, a organizaciones fuera de ella que ofrecen bienes o servicios a personas que se encuentran en la Unión o monitorean allí su comportamiento.

No depende solamente de nacionalidad. Tener un visitante europeo accidental tampoco basta, por sí solo, para afirmar todo el ámbito de aplicación.

2. Privacidad desde el diseño y por defecto — art. 25

- Lectura normativa — GDPR, art. 25.2 completo

> "2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas."

> El apartado 1 regula garantías al determinar los medios y durante el tratamiento; el apartado 3 se refiere a certificación. No se transcriben aquí.

> Fuente oficial — GDPR, art. 25.

Explicación oral: "Desde el diseño es pensar la protección cuando decidimos cómo funcionará el sistema. Por defecto es que su configuración inicial ya limite el tratamiento a lo necesario. No basta permitir al usuario arreglar después una configuración excesiva".

Desde el diseño: incorporar garantías al definir medios y durante el tratamiento, no después del lanzamiento.

Por defecto: limitar a lo necesario cantidad de datos, extensión del tratamiento, conservación y accesibilidad.

Ejemplos:

- Perfil privado inicialmente.
- Campos opcionales realmente opcionales.
- Ubicación no activada permanentemente.
- Analítica no esencial evaluada y configurada conforme al régimen aplicable.
- Permisos internos restrictivos.

En Argentina, estos criterios ayudan a concretar calidad, necesidad y seguridad. No atribuir la fórmula literal del art. 25 europeo a la Ley 25.326.

3. Delegado de protección de datos — art. 37

- Lectura normativa — GDPR, art. 37.1 completo

"1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos

personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10."

Es el apartado 1, no todo el artículo. El apartado 4 contempla también otros supuestos de designación conforme al Derecho aplicable. DPO significa Data Protection Officer: delegado de protección de datos, no administrador de base.

Fuente oficial — GDPR, art. 37.

No es obligatorio para toda empresa. El GDPR prevé supuestos como autoridades u organismos públicos, con su excepción judicial; observación habitual y sistemática a gran escala como actividad principal; o tratamiento a gran escala de categorías especiales o ciertos datos penales como actividad principal.

El DPO asesora y supervisa; no reemplaza la responsabilidad de la organización ni equivale al administrador de base.

4. Brechas — arts. 33 y 34

- Lectura normativa — GDPR, arts. 33.1, 33.2 y 34.1

Art. 33:

"1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas

físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

1. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento."

- Art. 34:

"1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida."

Son apartados seleccionados. El art. 33 regula también contenido, información gradual y documentación. El art. 34 establece contenido, excepciones y actuación de la autoridad. Sus excepciones incluyen protección que vuelva ininteligibles los datos, medidas posteriores que eliminen la probabilidad del alto riesgo y esfuerzo desproporcionado, supuesto que requiere comunicación pública o equivalente. Consultar las condiciones completas al resolver.

Fuente oficial — GDPR, arts. 33 y 34.

Aplicación al incidente: primero determinar si ese tratamiento de TurnoApp está alcanzado por el GDPR. Si lo está, evaluar por separado notificación a autoridad y comunicación a personas. "72 horas" no significa que pueda esperarse sin motivo hasta el último momento ni que todas las comunicaciones tengan el mismo plazo.

Notificación a la autoridad, sin dilación indebida y, de ser posible, a más tardar en 72 horas desde que se tiene constancia, salvo que sea improbable un riesgo para derechos y libertades. Si se supera, explicar motivos. El encargado informa al responsable sin dilación indebida.

Comunicación a las personas: se vincula al alto riesgo, con condiciones y excepciones propias.

No enseñar "cualquier incidente se notifica a todo el mundo en 72 horas". Tampoco presentar ese plazo como obligación general que surja de la Ley 25.326: verificar normas sectoriales, contratos y regímenes aplicables.

X. Doctrina y jurisprudencia

Doctrina — Autodeterminación informativa

Giulio Adinolfi, "Autodeterminación informativa, consideraciones acerca de un principio general y un derecho fundamental", Cuestiones Constitucionales, núm. 17, julio–diciembre de 2007.

El artículo permite explicar que la tutela de datos no se limita al secreto: comprende el control sobre la circulación de información personal y su relación con la autonomía. Es doctrina comparada orientadora, no una norma argentina ni una explicación del GDPR, que es posterior.

Paráfrasis didáctica: "El problema no es solamente quién sabe algo de mí, sino qué puede hacer con esa información y qué herramientas tengo para conocerlo y cuestionarlo".

No se presenta esa frase como cita textual del autor.

Explicación docente — Control no significa propiedad absoluta

Autodeterminación informativa permite explicar la posibilidad de conocer y cuestionar el tratamiento de información sobre uno mismo. No significa que la persona pueda prohibir cualquier tratamiento ni que los datos funcionen jurídicamente igual que una cosa de su propiedad.

Aplicación: una paciente puede exigir conocer y corregir información; una obligación legal puede justificar conservar determinada documentación. Hay que hacer efectivos los derechos y justificar sus límites, no elegir entre "la empresa es dueña de todo" y "la persona puede borrar todo siempre".

Pregunta: "¿Por qué también puede afectarme una clasificación verdadera sobre mí?". Respuesta orientativa: porque el uso, el contexto, la circulación y las consecuencias pueden afectar derechos aunque el dato sea exacto. La exactitud no agota el análisis de licitud.

Jurisprudencia — Halabi: por qué una arquitectura también plantea un problema constitucional

CSJN, "Halabi, Ernesto c/ P.E.N. — ley 25.873 — dto. 1563/04 s/ amparo ley 16.986", 24/02/2009, Fallos: 332:111.

Fuente primaria: texto de la sentencia publicado por la CSJN. El análisis se concentra en los fundamentos de la mayoría, especialmente considerandos 1, 7, 9–14, 20 y 22–26. Existen disidencias parciales; no se atribuye unanimidad a todos los fundamentos.

1. Hechos — ¿Qué se discutía?

Ernesto Halabi, abogado y usuario de telecomunicaciones, promovió amparo contra la ley 25.873 y el decreto 1563/04. Alegó afectación de privacidad, intimidad y confidencialidad de las comunicaciones con sus clientes.

La normativa contemplaba recursos para captar y derivar comunicaciones y registrar datos de usuarios y tráfico. El considerando 22 describe, entre otros elementos, una conservación de diez años. Ese plazo pertenece a la normativa cuestionada; no es un plazo general que esta clase recomiende.

La objeción no era solamente que alguien hubiera publicado un mensaje: alcanzaba la estructura de captación, registro y utilización de información y la insuficiente determinación de sus límites.

2. Recorrido procesal — ¿Qué llegó a la Corte?

Las instancias anteriores habían declarado la inconstitucionalidad de las normas y la Cámara había extendido los efectos a otros usuarios.

Precisión decisiva: según el considerando 7, el agravio del Estado ante la Corte se dirigía exclusivamente contra el alcance erga omnes de la sentencia: sus efectos más allá de quienes litigaron. El considerando 23 señala que el tramo de inconstitucionalidad había quedado firme por falta de impugnación.

No conviene resumir el caso como si la Corte hubiera revisado de nuevo, sin límites, todos los aspectos de la ley. Confirmó la sentencia en lo que fue materia del recurso y desarrolló fundamentos sobre tutela colectiva e intimidad.

3. Dos aportes diferentes

Dimensión sustantiva: protección de intimidad y comunicaciones frente a injerencias arbitrarias. Los considerandos 23–26 examinan garantías, determinación legal y límites de la restricción.

Dimensión procesal: cómo proteger derechos individuales afectados de modo homogéneo por un mismo hecho o régimen. La mayoría distingue derechos individuales, bienes colectivos e intereses individuales homogéneos. No son categorías intercambiables.

Los considerandos 12–14 desarrollan causa fáctica común, pretensión centrada en efectos comunes y condiciones relacionadas con acceso a justicia e interés en la protección. El considerando 20 señala recaudos como identificación del colectivo, representación adecuada, notificación y publicidad.

Explicación oral: "Cada persona conserva su derecho a la intimidad. Pero si el mismo sistema compromete a muchas de la misma manera, la respuesta judicial no necesariamente tiene que fragmentarse en miles de juicios idénticos. Eso no vuelve colectiva cualquier demanda con muchas personas".

4. Pasajes para leer y explicar

Considerando 23 — Fragmento textual:

> "las comunicaciones a las que se refiere la ley 25.873 y todo lo que los individuos transmiten por las vías pertinentes integran la esfera de intimidad personal y se encuentran alcanzadas por las previsiones de los artículos 18 y 19 de la Constitución Nacional."

Explicación: el soporte tecnológico no deja las comunicaciones fuera de la protección constitucional. No hace falta que el texto histórico nombre una aplicación.

Considerando 25 — Fragmento textual:

> "que dicho medio no sea más extenso que lo indispensable para el aludido logro."

Explicación: es una condición del estándar que la mayoría recuerda para examinar restricciones. Un objetivo legítimo no justifica cualquier extensión del medio. No es una frase que, aislada, habilite o prohíba todos los tratamientos.

Considerando 26 — Fragmento textual:

> "las normas tampoco prevén un sistema específico para la protección de las comunicaciones en relación con la acumulación y tratamiento automatizado de los datos personales."

Explicación: el riesgo está también en acumular y tratar información, no únicamente en difundirla. El mismo considerando advierte la relación entre datos de navegación y contenidos.

5. Preguntas y respuestas orientativas

- "Si no leo el mensaje, ¿el registro de comunicaciones es siempre inocuo?". No. Relaciones, horarios y navegación pueden revelar aspectos de la vida; hacen falta contexto y garantías.
- "¿Combatir delitos vuelve válida cualquier captación?". No. La finalidad no reemplaza requisitos legales, determinación y límites.
- "¿Qué conecta con TurnoApp?". La enseñanza sobre límites y garantías de una infraestructura que acumula información. No una orden concreta sobre el formulario de la clínica.
- "¿Halabi declara ilícita toda base masiva?". No. Sería una generalización no autorizada por la sentencia.

6. Límite de la analogía

TurnoApp es un caso didáctico de tratamiento en un servicio privado de salud; Halabi trata normas de telecomunicaciones, intimidad y alcance colectivo del pronunciamiento. Para consentimiento, salud, proveedores y conservación debemos volver a las normas específicas.

Conexión final: "La técnica hace posible concentrar información; el derecho pregunta quién puede hacerlo, para qué, bajo qué límites y con qué protección efectiva".

Ampliación opcional — Decisiones automatizadas

No exponer si falta tiempo. Sirve para distinguir el texto de una norma de las generalizaciones que no autoriza.

- Lectura normativa — Ley 25.326, art. 20 completo

  "ARTICULO 20. — (Impugnación de valoraciones personales).

  1. Las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas, no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado.
  2. Los actos que resulten contrarios a la disposición precedente serán insanablemente nulos."
- Fuente oficial — Ley 25.326, art. 20.

Esta regla se refiere a decisiones judiciales y actos administrativos, con sus presupuestos. No presentarla como prohibición general de toda recomendación automática en una app privada ni como copia del régimen europeo. Un perfil privado puede plantear otros problemas, pero no se resuelven ampliando por intuición este artículo.

XI. Taller integrador — Auditoría de TurnoApp

Consigna para estudiantes

Una clínica contrata TurnoApp para gestionar turnos. El proveedor propone:

usuarios

id

nombre

dni

email

telefono

domicilio_completo

fecha_nacimiento

diagnostico

religion

ubicacion_gps_permanente

contactos_telefono

password

acepta_todo = true

Además:

- Todo el personal comparte una cuenta administradora.
- La contraseña se almacena en texto plano.
- El recordatorio muestra el diagnóstico en la notificación del teléfono.
- El programador descarga producción a su computadora personal.
- Un proveedor publicitario recibe correos y especialidades consultadas.
- El hosting tiene copias en el exterior, sin revisar destinos.
- La política dice “usamos tus datos para mejorar tu experiencia”.
- No existe canal para ejercer derechos.

- La cuenta se puede desactivar, pero todos los datos se conservan indefinidamente.

Trabajo central — 15 minutos, grupos de 3 o 4

El caso es el mismo trabajado durante la exposición. No hace falta redescubrir todos sus problemas ni programar una solución.

Distribución orientativa: 3 minutos para elegir hallazgos; 8 para completar la tabla; 4 para decidir y redactar la prioridad.

Entregables obligatorios — Una sola hoja

1. Elegir tres hallazgos distintos: uno sobre datos o finalidad; uno sobre seguridad o proveedores; uno sobre derechos o conservación.
2. Completar una fila por hallazgo: dato o flujo, artículo o principio, cambio propuesto y forma concreta de comprobarlo.
3. Elegir cuál de los tres impediría lanzar en esas condiciones y justificarlo en dos oraciones.

No se exige un esquema completo de base de datos, política de privacidad ni auditoría exhaustiva. No inventar que todo dato clínico debe borrarse al cerrar una cuenta ni que el consentimiento habilita cualquier uso.

Puesta en común — Cinco minutos para todo el curso

Escuchar dos grupos durante un minuto cada uno. Usar los tres minutos restantes para contrastar justificación y evidencia. Los demás entregan su hoja; no se prometen exposiciones individuales de todos los grupos.

Ampliaciones opcionales — Fuera de los 15 minutos

- Clasificar todos los campos y revisar el modelo de datos.

- Identificar más riesgos y priorizarlos.
- Diseñar el circuito completo de derechos.
- Redactar un aviso e identificar información pendiente.
- Revisar un flujo internacional y los documentos necesarios.

Estas ampliaciones no forman parte de la exigencia mínima de hoy.

Plantilla de respuesta

organizativo

ompartida s autorizaciones les y logs rmisos y

XII. Guía docente de resolución

1. Clasificación y finalidad

Nombre, DNI, correo, teléfono, domicilio y nacimiento son personales. DNI, domicilio y fecha de nacimiento requieren justificar necesidad según el servicio; no son automáticamente imprescindibles.

Diagnóstico es salud y dato sensible. Religión es sensible y no tiene finalidad demostrada en esta app.

Ubicación permanente y contactos implican tratamiento personal y aparecen excesivos para reservar turnos. Las especialidades consultadas, según contexto, pueden revelar información de salud.

Contraseña: credencial de alto riesgo; no calificarla de sensible legal solamente por su importancia.

2. Hallazgos esperados

- Datos excesivos: art. 4.
- Religión sin fundamento demostrado: arts. 4 y 7.
- Aceptación premarcada y genérica: arts. 5 y 6.
- Finalidad publicitaria no evaluada: arts. 4, 5 y 11.
- Proveedor que reutiliza información: art. 25.
- Cuenta compartida y permisos indiscriminados: arts. 9 y 10.
- Contraseñas expuestas: art. 9.
- Diagnóstico visible en notificaciones: confidencialidad y minimización.
- Copia de producción sin control: arts. 9, 10 y régimen del prestador.
- Transferencias no evaluadas: art. 12 y reglamentación.
- Conservación indefinida: arts. 4.7 y 16.
- Falta de derechos y canal: arts. 6, 14, 15 y 16.

3. Modelo orientativo mejorado

usuarios

id

nombre

email_o_telefono_necesario

password_hash

estado

turnos

id

paciente_id

profesional_id

fecha_hora

estado

preferencias_comunicacion

usuario_id

canal_recordatorios

preferencia_publicidad_separada

evidencias_de_consentimiento

usuario_id

finalidad

version_del_aviso

fecha_hora

accion_afirmativa

solicitudes_de_derechos

id

usuario_id

tipo

fecha_recepcion

vencimiento_aplicable

estado

respuesta

No es un esquema clínico completo ni impone consentimiento donde haya una excepción legal aplicable. Las evidencias de consentimiento se usan cuando esa sea la habilitación pertinente.

Separar información clínica en un módulo con acceso específico cuando sea necesaria y exista fundamento para tratarla. Evaluar DNI y otros identificadores según el contexto real, fuera de automatismos.

El nombre de una especialidad también puede revelar salud: separar tablas no vuelve inocua la información.

4. Cambios prioritarios

No lanzar con contraseñas en texto plano, acceso indiscriminado o envíos de datos de salud a publicidad sin fundamento.

Si ya hubo exposición: contener, preservar evidencia y evaluar alcance. La migración a hashes no resuelve por sí sola que contraseñas anteriores hayan quedado comprometidas; puede requerir restablecimiento y otras medidas.

Luego:

- Minimizar el formulario.
- Desactivar flujos no justificados.
- Definir permisos individuales.
- Establecer canales y responsables de derechos.
- Revisar nube, contratos y transferencias.
- Documentar conservación y registro aplicable.

5. Aviso breve — Ejercicio, no política completa

"[Responsable y domicilio] utilizará los datos identificados como obligatorios para gestionar sus turnos y enviar recordatorios por el canal elegido. Si no aporta esos datos, no podremos completar la reserva. Los campos señalados como opcionales no condicionan el servicio. La información será accesible al personal autorizado y a los prestadores identificados en la política completa, dentro de sus funciones. Puede solicitar acceso, rectificación, actualización o supresión, cuando corresponda, mediante [canal]. Consulte aquí los destinatarios, las condiciones de conservación y las transferencias previstas: [enlace]".

Completar con hechos reales antes de usar: responsable, domicilio, campos, finalidades, destinatarios, conservación, transferencias y canal. No prometer "no compartimos datos" si existen hosting, mensajería o soporte externos.

6. Criterio de devolución

Valorar coherencia entre riesgo, artículo, medida y evidencia; no cantidad de herramientas mencionadas. La guía completa es un banco de respuestas: no se exige que cada grupo produzca todo lo incluido en ella.

Ejemplo de entrega mínima suficiente

	:o	**eba**
e sin finalidad ı y no exceso	:ión y revisar lo ya	vados y prueba sin adas
administradora	ıales y permisos por	cepción no accede al
todo sin criterio	ivación, supresión servación justificada	ıd con eliminación o a por categoría

Prioridad posible: impedir el lanzamiento con accesos indiscriminados a salud. No hay una única prioridad correcta para todos los grupos: también pueden justificar contraseñas en texto plano o un envío de salud a publicidad sin fundamento.

Rúbrica formativa — 10 puntos, sin imponer una nota de aprobación

ıcretos y distintos, conectados con el caso

ıio pertinente y explicado, no solo número

cia da el riesgo y prueba observable

ınada según impacto y exposición

"Agregar cifrado" no obtiene por sí solo una buena valoración si el problema era una finalidad ilegítima. Una respuesta puede reconocer que falta información y especificar qué dato necesita para decidir.

Preguntas para la puesta en común:

- ¿Por qué cifrar no corrige la recolección excesiva?
- ¿Cómo se comprueba que un rol no puede consultar diagnósticos?
- ¿Qué pasa con la corrección en sistemas integrados?
- ¿Qué dato conservarían por obligación legal y con qué acceso?
- ¿Qué documento permite justificar una transferencia?

XIII. Cierre

"Hoy no vimos solamente una ley para agregar al final del proyecto. Vimos decisiones que cambian un formulario, una tabla, un permiso, una API y un contrato.

Un sistema responsable no pide todo lo que puede pedir. Recoge lo necesario, explica para qué, limita quién accede, permite corregir y define cuándo dejar de conservar.

La protección de datos empieza antes del primer registro: empieza cuando decidimos qué sistema vamos a construir".

Evaluación de salida — últimos cinco minutos

Responder:

- Un ejemplo de dato que siga siendo personal aunque se quite el nombre.
- Una diferencia entre acceso y rectificación, incluidos sus plazos legales.
- Un cambio de arquitectura que reduzca un riesgo jurídico sin depender de una nueva casilla de consentimiento.

Respuestas mínimas esperadas: identificador vinculable; acceso diez días corridos y rectificación cinco hábiles bajo los presupuestos legales; minimización, permisos por rol, segregación o conservación controlada.

Actividad posterior sugerida — Sin fecha de entrega fijada

Elegir una app, sin vulnerar accesos ni recolectar datos de terceros. Revisar los permisos y la información pública de privacidad. Identificar tres datos o flujos, finalidad declarada, un riesgo y una mejora concreta. No afirmar que una práctica interna existe solo por sospecharla.

XIV. Apunte breve para estudiantes

- Dato personal: información sobre alguien determinado o determinable.
- Dato sensible: categoría definida por la ley; no es sinónimo de cualquier dato riesgoso.
- Tratar incluye leer, copiar, analizar, compartir y borrar.

- Principios: finalidad, calidad, necesidad, información, conservación, seguridad y confidencialidad.
- Consentimiento: libre, expreso e informado, con excepciones legales y límites.
- Sensibles: régimen específico; una casilla no lo habilita todo.
- Acceso: art. 14; diez días corridos desde intimación fehaciente.
- Rectificación, actualización y supresión procedente: art. 16; cinco días hábiles bajo sus condiciones.
- Nube: revisar proveedores, destinos, accesos y transferencias.
- GDPR: alcance propio; no trasladar automáticamente sus obligaciones a Argentina.
- Cifrado, hashing y seudonimización no equivalen a anonimización.
- Privacidad desde el diseño: convertir garantías jurídicas en requisitos verificables.

XV. Fuentes y alcance de verificación

Material preparado para la clase del 22/10/2026 a partir de los textos consultados. No se presenta como certificación exhaustiva de toda la normativa sectorial ni de todas las modificaciones posibles a esa fecha.

Normativa y fuentes oficiales

- Ley 25.326 — texto actualizado oficial. Base principal: arts. 1 a 16, 20, 21, 24, 25, 27, 29 y 33.
- Decreto 1558/2001 — reglamentación.
- AAIP — Registrar bases de datos personales privadas.
- AAIP — Trámites del Registro Nacional.
- AAIP — Compilación institucional de normativa. Documento con referencia temporal a julio de 2024: utilizado para identificar normas complementarias, no como actualización integral a octubre de 2026.

- Resolución AAIP 198/2023 — cláusulas contractuales modelo. Referencia complementaria identificada; no se desarrolla aquí un examen cláusula por cláusula.
- GDPR — texto oficial en EUR-Lex. Consulta enfocada en arts. 3, 25, 33, 34 y 37.

Doctrina y jurisprudencia

- Giulio Adinolfi — artículo doctrinal, 2007. Consulta de pasajes pertinentes al concepto de autodeterminación informativa.
- CSJN — Halabi, sentencia del 24/02/2009, Fallos: 332:111. Fuente primaria para el apartado jurisprudencial; consulta de los fundamentos de la mayoría indicados en esa sección. El documento incluye disidencias parciales, que no se desarrollan exhaustivamente.
- MPD — Halabi, reseña oficial. Referencia complementaria, no sustituto del texto de la sentencia.

Precisiones para la exposición

- No confundir los arts. 14 y 16.
- No importar la clasificación completa de sensibles ni las bases de licitud europeas a la ley argentina.
- No afirmar que toda empresa necesita DPO.
- No atribuir a la Ley 25.326 un plazo general de 72 horas para cualquier brecha.
- No equiparar inscripción con certificación de cumplimiento.
- No presentar recomendaciones técnicas como herramientas literalmente impuestas por la ley.
- Verificar reglas sanitarias y de conservación específicas antes de convertir el caso didáctico en una implementación real.