Protección de datos personales en las relaciones laborales

Ley N° 19.628, reformada por la Ley N° 21.719 — vigencia: 1 de diciembre de 2026

Pablo Reyes Carreño
Jefe Departamento Jurídico (S)

Agosto 2026

Lineamiento de la invitación

- Una aproximación a la normativa sobre protección de datos personales y al impacto que estas reformas tendrán en las relaciones laborales.

Objetivos:

- Comprender el nuevo marco legal de protección de datos y su entrada en vigencia.
- Identificar los datos personales tratados en la relación laboral: postulación, contratación, ejecución y término.
- Precisar las obligaciones del empleador como responsable del tratamiento y los derechos de las y los trabajadores.
- Anticipar riesgos de incumplimiento, sanciones y brechas operativas por cerrar.

Estructura de la Ley Nº 19628 (Dic 2026)

- **Título Preliminar:** Define el objeto, el ámbito de aplicación y los conceptos clave (definiciones).
- **Título I:** Trata sobre los derechos del titular de datos personales (acceso, rectificación, supresión, oposición, portabilidad, etc.).
- **Título II:** Regula el tratamiento de los datos personales, el consentimiento , las obligaciones del responsable (como el deber de seguridad) y las categorías especiales de datos (datos sensibles , datos de salud , biométricos y de niños, niñas y adolescentes).
- **Título III:** Contiene las normas específicas para el tratamiento de datos sobre obligaciones de carácter económico, financiero, bancario o comercial.
- **Título IV:** Regula cómo los órganos públicos deben tratar los datos personales.
- **Título V:** Establece las reglas para la transferencia internacional de datos personales.
- **Título VI:** Crea y define la **Agencia de Protección de Datos Personales**, detallando su naturaleza, funciones, atribuciones y organización.
- **Título VII:** Es el **régimen sancionatorio**. Detalla las infracciones (leves, graves, gravísimas) , las sanciones , los procedimientos (tutela de derechos y sancionatorio) y el modelo de prevención.
- **Título VIII:** Regula el tratamiento de datos por parte de organismos con autonomía constitucional (como el Congreso Nacional, el Poder Judicial, la Contraloría, etc.).
- **Disposiciones transitorias:** Normas para la implementación y entrada en vigencia de la ley y sus modificaciones.

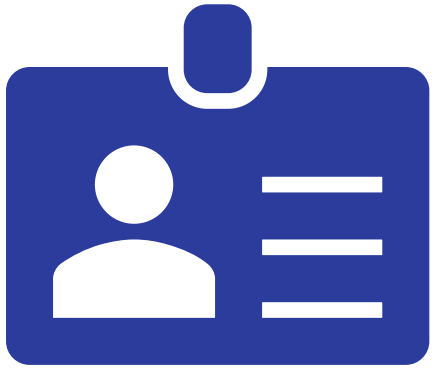
□ Conceptos clave

Dato personal



- Es cualquier información vinculada o referida a una persona natural identificada o identificable.
- Se considera "identificable" a toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante identificadores: nombre, el número de cédula de identidad, o el análisis de elementos propios de su identidad física, fisiológica, genética, psíquica, económica, cultural o social

Datos personales sensibles



Se refieren a las características físicas o morales de las personas, o a hechos o circunstancias de su vida privada o intimidad. Específicamente, revelan:

Origen étnico o racial.

Afiliación política, sindical o gremial.

Situación socioeconómica.

Convicciones ideológicas o filosóficas.

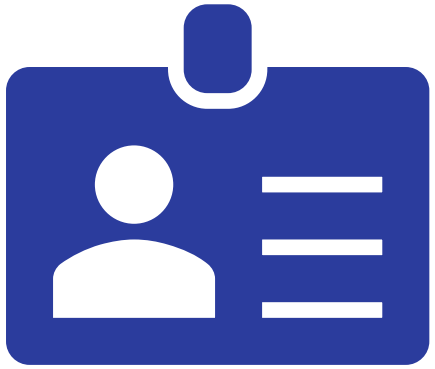
Creencias religiosas.

Datos relativos a la salud.

Perfil biológico humano y datos biométricos.

Información relativa a la vida sexual, orientación sexual e identidad de género.

Tratamiento de datos



- Es cualquier operación o conjunto de operaciones o procedimientos técnicos, ya sean automatizados o no, que permitan recolectar, procesar, almacenar, comunicar, transmitir o utilizar datos personales

Titular de datos

Es la persona natural, identificada o identificable, a quien conciernen o se refieren los datos personales.



Responsable de datos

Es toda persona natural o jurídica, pública o privada, que **decide acerca de los fines y medios** del tratamiento de datos personales

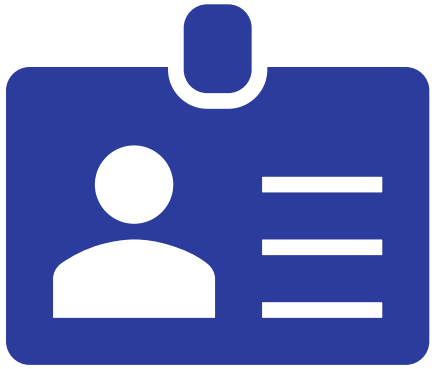


Tercero mandatario o encargado

Es la persona natural o jurídica que trata datos personales **por cuenta del responsable** de datos



Consentimiento



Es toda manifestación de voluntad **libre, específica, inequívoca** e informada, otorgada mediante una declaración o una clara acción afirmativa, por la cual el titular autoriza el tratamiento de sus datos personales.

Agencia de Protección de Datos Personales

Se refiere a la Agencia de Protección de Datos Personales



Principios relativos a la protección de datos

Licitud y lealtad | Finalidad | Proporcionalidad (minimización) | Calidad | Responsabilidad | Seguridad | Transparencia e información | Confidencialidad

Fines y naturaleza

- Moldean e informan todo el resto de la normativa
- Se contiene un catálogo específico
- Son **inmediatamente obligatorios y exigibles por sí mismos**.
  - **Son Autoejecutables:** El responsable de datos (la empresa u organismo) no puede excusarse diciendo que "la ley no era clara" o que "esperaba un reglamento" para saber cómo aplicar, por ejemplo, el principio de proporcionalidad.
  - **Fundamentan la Fiscalización:** La Agencia de Protección de Datos puede fiscalizar y auditar a un responsable basándose *directamente* en la posible vulneración de uno de estos principios.
  - **Son la Causa Directa de Sanciones:** La ley es explícita en esto. Los artículos 33 y 34 establecen que las infracciones (leves, graves o gravísimas) se configuran cuando el responsable infringe los principios señalados en el Artículo 3°.

1. Principio de Licitud y Lealtad

Artículo: Art. 3°, letra a).

Definición Legal: Los datos personales solo pueden tratarse de manera lícita y leal. El responsable (quien trata los datos) deberá ser capaz de **acreditar la licitud** del tratamiento que realiza.

Efecto Práctico: Se prohíbe el tratamiento de datos de forma oculta, engañosa o ilegal. La carga de la prueba recae en la empresa u organismo: si la Agencia le pregunta "demuéstreme por qué tiene derecho a usar estos datos", debe tener una respuesta legal sólida (ej. el consentimiento, un contrato, etc.).

2. Principio de Finalidad

Artículo: Art. 3°, letra b).

Definición Legal: Los datos deben ser recolectados con **fines específicos, explícitos y lícitos**. El tratamiento debe limitarse estrictamente al cumplimiento de estos fines. No se pueden tratar datos para fines distintos a los informados originalmente, salvo excepciones muy acotadas (como un nuevo consentimiento o que lo exija la ley).

Efecto Práctico: Este principio combate el "uso indebido" de los datos. Si una persona entrega sus datos para una compra (finalidad: gestionar el pago y envío), la empresa no puede, por regla general, usar esos mismos datos para un fin distinto, como venderlos a un tercero para marketing.

3. Principio de Proporcionalidad

Artículo: Art. 3°, letra c).

Definición Legal: Los datos que se traten deben limitarse estrictamente a aquellos que resulten **necesarios, adecuados y pertinentes** para los fines del tratamiento. Además, pueden ser conservados solo por el tiempo necesario para cumplir esos fines, luego deben ser **suprimidos o anonimizados**.

Efecto Práctico: Esto se conoce como "minimización de datos". Si solo se necesita el correo electrónico para un boletín informativo, no es proporcional solicitar el domicilio o la cédula de identidad. Impide que las empresas acumulen datos "por si acaso" y los obliga a tener un ciclo de vida, borrándolos cuando ya no los necesitan.

4. Principio de Calidad

Artículo: Art. 3°, letra d).

Definición Legal: Los datos personales deben ser **exactos, completos, actuales y pertinentes** en relación con los fines para los que son tratados.

Efecto Práctico: Obliga al responsable a mantener sus bases de datos limpias y actualizadas. Es la base del derecho de rectificación del titular: si los datos no son de calidad (ej. una dirección antigua, una deuda mal registrada), el titular puede exigir su corrección.

5. Principio de Responsabilidad

Artículo: Art. 3°, letra e).

Definición Legal: Quienes realicen tratamiento de datos personales serán **legalmente responsables** del cumplimiento de todos los principios y obligaciones de la ley.

Efecto Práctico: Este es el principio de *accountability* o responsabilidad proactiva. El responsable no puede excusarse diciendo que "no sabía" o que fue culpa de un tercero. Es el sujeto pasivo de las fiscalizaciones y sanciones de la Agencia.

6. Principio de Seguridad

Artículo: Art. 3°, letra f).

Definición Legal: El responsable debe garantizar **estándares adecuados de seguridad**, protegiendo los datos contra tratamiento no autorizado, pérdida, filtración, daño accidental o destrucción. Las medidas deben ser apropiadas a la naturaleza de los datos tratados.

Efecto Práctico: Obliga a implementar medidas técnicas (ej. cifrado, firewalls) y organizativas (ej. políticas de acceso, capacitación) para prevenir brechas de seguridad. No se exige la misma seguridad para una base de datos de correos de marketing que para una base de datos con fichas médicas (datos sensibles).

7. Principio de Transparencia e Información

Artículo: Art. 3°, letra g).

Definición Legal: El responsable debe entregar al titular toda la información necesaria para el ejercicio de sus derechos. Las políticas y prácticas sobre el tratamiento de datos deben estar **permanentemente accesibles**, ser precisas, claras, inequívocas y gratuitas.

Efecto Práctico: Este es el fundamento de las "Políticas de Privacidad". No basta con tener una; debe ser fácil de encontrar, fácil de entender y gratuita. Prohíbe las políticas ocultas o redactadas en lenguaje legal incomprensible.

8. Principio de Confidencialidad

Artículo: Art. 3°, letra h).

Definición Legal: El responsable y quienes tengan acceso a los datos (como empleados o encargados) deben **guardar secreto o confidencialidad** sobre los mismos. Este deber subsiste **incluso después de concluida la relación** con el titular.

Efecto Práctico: Impone un deber de secreto profesional. Un fiscalizador no puede divulgar la situación financiera de un empleador, ni siquiera después de renunciar. Este deber es esencial para la confianza en el sistema.

Protección de datos personales en las relaciones laborales

Ley N° 19.628, reformada por la Ley N° 21.719 — vigencia: 1 de diciembre de 2026

La crisis del consentimiento en el empleo

- **Asimetría y subordinación:** en la relación laboral no puede garantizarse que el consentimiento sea verdaderamente libre.
- El trabajador tiene temor fundado de que negarse le acarree consecuencias desfavorables en su contratación o permanencia (AEPD, 2021 y 2023).
- Consecuencia: el consentimiento **deja de ser la base de licitud idónea** para tratar datos del personal.

Fuentes: AEPD (2021, 2023); Agote y Arriola (2024); Ley N° 19.628 reformada, art. 12; Bastidas (2026).

¿Cuál es entonces la base de licitud?

- La Ley N° 19.628, reformada por la Ley N° 21.719, regula el consentimiento en el **artículo 12** y las demás bases de licitud en el **artículo 13**.
- **Regla general en el empleo: la ejecución del contrato de trabajo**, que habilita el tratamiento de la información necesaria para la relación laboral.
- **Cumplimiento de obligaciones legales** del empleador: previsionales, tributarias, de seguridad y salud, y el registro de asistencia del artículo 33 del Código del Trabajo.
- **Interés legítimo:** exige un examen riguroso de idoneidad, necesidad y proporcionalidad, optando por la alternativa menos invasiva.

Fuentes: Ley N° 19.628, reformada por la Ley N° 21.719, arts. 12 y 13; art. 33 del Código del Trabajo; AEPD (2021); Bastidas (2026).

El estándar del Grupo de Trabajo del Artículo 29

- **Dictamen 2/2017, sobre el tratamiento de datos en el trabajo** (complementa el Dictamen 8/2001): en la mayoría de los tratamientos en el trabajo la base jurídica no puede ser el consentimiento del trabajador, por la naturaleza de la relación empleador-trabajador.
- **Directrices sobre el consentimiento (WP 259):** no puede obtenerse en el mismo acto de aceptar el contrato o unas condiciones generales.
- **Chile:** el artículo 12 de la Ley N° 19.628, reformada por la Ley N° 21.719, exige un consentimiento **libre, informado, específico e inequívoco**, lo que desplaza a la autorización genérica firmada al inicio del contrato de trabajo.

Fuentes: GT29, Dictámenes 2/2017 y 8/2001; Directrices WP 259 rev. 01; Ley N° 19.628 reformada, art. 12.

Aplicaciones del Dictamen 2/2017

- **Reclutamiento y redes sociales:** la empresa no está legitimada para solicitar "amistad" a candidatos ni acceso al contenido de sus perfiles, ni a la información que comparten con terceros.
- **Entrevista de trabajo:** las respuestas del candidato no equivalen a un consentimiento para tratar esos datos.
- **Control de comunicaciones públicas:** solo si el empleador demuestra necesidad para un interés legítimo, ausencia de medios menos invasivos e información previa sobre su alcance.
- **Geolocalización de vehículos:** debe ser proporcional al riesgo y no registrar la ubicación fuera del horario de trabajo.

Fuente: GT29, Dictamen 2/2017 sobre el tratamiento de datos en el trabajo (WP 249).

Minimización: el límite al control empresarial

- **Regla:** los datos deben ser adecuados, pertinentes y estrictamente limitados a lo necesario para la finalidad perseguida.
- El empleador **no puede recopilar información superflua, excesiva o invasiva**, aunque cuente con una base de licitud.
- Esto redefine los límites del **control tecnológico**: dispositivos personales y geolocalización, biometría, y videovigilancia.

Fuentes: art. 5.1.c del RGPD; AEPD (2021).

Videovigilancia y captación de sonido

- Las cámaras están estrictamente limitadas por el **principio de proporcionalidad**.
- Se prohíbe terminantemente su instalación en **espacios de descanso, vestuarios y servicios higiénicos**.
- La **grabación continua de sonido** es, por regla general, desproporcionada y lesiva del derecho a la intimidad: capta de forma indiscriminada conversaciones ajenas al interés laboral y coarta la libertad del trabajador.

Fuente: AEPD (2021).

Teletrabajo: los límites del monitoreo

- La digitalización trajo herramientas de **monitoreo constante** de la actividad del trabajador; las agencias europeas les han impuesto límites severos.
- **CNIL, deliberación sancionadora SAN-2023-021:** las capturas de pantalla recurrentes y el conteo permanente de minutos de inactividad según el movimiento del teclado o el ratón constituyen una vigilancia desproporcionada e intrusiva.
- No existe un interés legítimo que la justifique: **el teletrabajo no habilita la vigilancia constante**, deben usarse medios alternativos menos invasivos.

Fuente: CNIL, deliberación sancionadora SAN-2023-021 (2023).

Gestión algorítmica del trabajo

Transparencia, explicabilidad y límites a la inteligencia artificial

Gestión algorítmica del trabajo

- Los algoritmos ya intervienen en **reclutamiento, asignación de tareas, evaluación de desempeño y despidos**: la gestión de personas queda entrelazada con la protección de datos.
- **Transparencia y explicabilidad ex post:** el derecho a la explicación del artículo 22 del RGPD, reforzado por la Directiva de Trabajo en Plataformas Digitales.
- El trabajador tiene derecho a conocer los **parámetros principales y la lógica** de la decisión automatizada que le afecta.

Fuentes: art. 22 RGPD; Directiva UE de plataformas; Coddou y Padilla (2024); Todolí Signes (2024).

Límites al uso de IA en el lugar de trabajo

- El Reglamento Europeo de Inteligencia Artificial **prohíbe los sistemas que infieran emociones o estados de ánimo** en el lugar de trabajo.
- Se combinan así tres capas de exigencia: **protección de datos, normativa laboral y regulación de la IA**.
- **Lectura para Chile:** el estándar de proporcionalidad, información previa y no discriminación es exigible desde ya por la vía de los derechos fundamentales del trabajador.

Fuentes: Reglamento Europeo de IA; Agote y Arriola (2024); Todolí Signes (2024).

España: la dimensión colectiva y el algoritmo

- En el derecho español el eje se desplaza desde el individuo hacia una **gobernanza colectiva** de los datos y de la transparencia algorítmica, mediada por sindicatos y representantes.
- **Ley Rider y Estatuto de los Trabajadores (España):** la representación legal de los trabajadores debe conocer los parámetros, reglas e instrucciones de los algoritmos que inciden en el empleo y en las condiciones de trabajo.
- Ese deber español alcanza también a los **sistemas semiautomatizados de apoyo a la decisión**, no solo a las decisiones plenamente automatizadas. **En Chile se limita el uso de sistemas automatizados salvo fines específicos (8 bis).**

Fuentes: Real Decreto-ley 9/2021 (Ley Rider); art. 64.4 d) ET; Baz Rodríguez (2024); Todolí Signes (2024).

España: consulta previa a los representantes

- En España, implantar o revisar un sistema algorítmico o de IA de control que provoque **cambios relevantes en la organización del trabajo** obliga a informar y consultar de forma previa.
- Los representantes legales pueden emitir un **informe no vinculante** antes de la puesta en marcha del sistema.

Fuentes: art. 64.5 ET; Directiva 2002/14/CE; Agote y Arriola (2024); Todolí Signes (2024).

Acciones actuales de la Dirección del Trabajo

Adecuación doctrinal y primeros pronunciamientos sobre vigilancia algorítmica

Qué está haciendo la DT

- **Equipo de trabajo para la adecuación doctrinal:** se conformó un equipo dedicado al estudio y actualización de los dictámenes, a fin de ajustarlos al nuevo marco de protección de datos personales.
- **Pronunciamiento sobre vigilancia algorítmica:** Ordinario N° 2000-49883, de 7 de agosto de 2026, sobre el uso de sistemas de reconocimiento y análisis de imagen en el lugar de trabajo.
- La doctrina administrativa se convierte así en la vía de entrada del estándar de protección de datos a la **fiscalización laboral**.

Fuente: Dirección del Trabajo, Ordinario N° 2000-49883, de 7 de agosto de 2026.

Ordinario N° 2000-49883: resguardos exigidos

- Las imágenes, rasgos faciales y gestos captados por el sistema se vinculan con **datos biométricos** y con la garantía constitucional de protección de los datos personales, por lo que exigen resguardos reforzados.
- Finalidad **preventiva determinada, explícita y legítima**, limitada a los datos estrictamente necesarios para cumplirla.
- Reserva, custodia y seguridad de los datos, con **acceso limitado a personas estrictamente autorizadas**.
- Período de conservación estrictamente necesario y **eliminación segura** de los registros una vez cumplida la finalidad.
- **Información previa, suficiente y clara** a los trabajadores sobre el funcionamiento del mecanismo y el tratamiento de los datos que genere.

Fuente: Dirección del Trabajo, Ordinario N° 2000-49883, de 7 de agosto de 2026, considerando 4.

Control de licencias médicas: criterio de la SUSESO

- **Dictamen N° O-01-S-02791-2026, de 1 de julio de 2026:** las COMPIN e Isapres no pueden usar geolocalización activa, reconocimiento facial ni biometría para verificar el cumplimiento del reposo médico.
- No existe **habilitación legal expresa**: son datos sensibles y su uso exige una regulación legal específica que fije alcance, finalidades y garantías.
- El **consentimiento del afiliado no amplía las facultades de fiscalización**: solo caben los mecanismos ya contemplados en la ley y en las instrucciones de la SUSESO.
- Criterio convergente con el de la Dirección del Trabajo: el tratamiento biométrico o de geolocalización con fines de fiscalización **exige base legal suficiente**.

Fuente: Superintendencia de Seguridad Social, Dictamen N° O-01-S-02791-2026, de 1 de julio de 2026.

Síntesis: hacia un tratamiento lícito de datos en la relación laboral

1. Un alto estándar de protección de datos: la DT y el empleador

A. Datos sensibles y vínculo de vulnerabilidad

- Las inspecciones del trabajo procesan miles de datos de trabajadores y empleadores diariamente, y acceden a información altamente personal y profesional: salarios, contratos, despidos, situaciones de salud y la condición de sancionado.
- El tratamiento de estos datos impacta directamente en derechos fundamentales.
- La Inspección del Trabajo se relaciona con una de las partes, los trabajadores, que puede encontrarse en situación de mayor debilidad frente al empleador, lo que obliga a extremar las cautelas y la seguridad de la información.
- El empleador queda sujeto al mismo estándar: trata esos mismos datos respecto de una parte subordinada, durante toda la relación laboral y después de su término.

Fuentes: Ley N° 19.628, reformada por la Ley N° 21.719, art. 3°; AEPD (2021).

Minimización y confidencialidad en la relación laboral

B. Principios de minimización y confidencialidad

- Las autoridades de control han enfatizado que la información recolectada debe limitarse a fines legítimos y ser imprescindible para el desarrollo de la función pública.
- En la empresa rige el mismo criterio: solo los datos necesarios para la finalidad laboral declarada, y el deber de reserva se mantiene tras el término del contrato.

Fuentes: Ley N° 19.628, reformada por la Ley N° 21.719, arts. 3° y 12; AEPD (2021).

2. Responsabilidad proactiva del empleador

- La ley chilena transita desde un modelo puramente reactivo (responder a infracciones) a uno de **responsabilidad proactiva** (conocido en otras legislaciones como *accountability*). Esto impone a las organizaciones el deber no solo de cumplir la ley, sino de poder demostrar ese cumplimiento.
- La ley establece la **responsabilidad proactiva** de dos maneras:
  - **Principio de Responsabilidad (Art. 3°):** Se establece como un principio rector que quienes realicen tratamiento de datos son "legalmente responsables del cumplimiento de los principios contenidos en este artículo y de las obligaciones y deberes de conformidad a la ley".
  - **Deber General de Prevención (Art. 48):** La ley obliga a *todos* los responsables de datos (sean personas naturales o jurídicas, públicas o privadas) a adoptar acciones destinadas a "prevenir la comisión de las infracciones" establecidas en la ley.
- Para materializar este deber, la ley crea un mecanismo específico, voluntario (sector privado) obligatorio (sector público (art 44, 49): el Modelo de Prevención de Infracciones.
- En la relación laboral esto se traduce en una carga concreta: el empleador debe poder acreditar la base de licitud de cada tratamiento de datos del personal, no basta con afirmar que cumple.

Fuente: Ley N° 19.628, reformada por la Ley N° 21.719, arts. 3°, 44, 48 y 49.

Autoridades referentes

Agencia de Protección de Datos

- Fiscaliza el cumplimiento de la Ley N° 19.628.
- Sanciona y lleva el Registro Nacional de Sanciones y Cumplimiento.
- Certifica los modelos de prevención de infracciones.

Dirección del Trabajo

- Fiscaliza la legislación laboral y los derechos fundamentales del trabajador.
- Interviene cuando el tratamiento ocurre dentro de la relación de trabajo.

Fuentes: Ley N° 19.628, reformada por la Ley N° 21.719; Código del Trabajo.

Gestión del Departamento Jurídico

Emisión de dictámenes en los primeros 4 meses | Proyección para otorgar certeza jurídica

Fundamentos de la gestión de dictámenes

La calidad de un dictamen no depende solo de la capacidad técnica de quien lo redacta: exige un proceso ordenado, trazable y sujeto a control.



Oportunidad en la respuesta.



Consistencia doctrinaria.



Solidez del razonamiento jurídico.



Comunicación comprensible para los destinatarios.

Objetivo: trazabilidad y priorización

El objetivo es que cada solicitud cuente con un estado conocido, un responsable y una próxima acción definida.

La gestión no depende del seguimiento personal de cada funcionario, sino de un sistema institucional.

Permite conocer la situación real de la cartera de dictámenes.

Facilita advertir los asuntos detenidos.

Prioriza según urgencia, impacto institucional o relevancia doctrinaria.

Gestión Documental

Diseño de instrucciones para el ciclo documental | Del papel al archivo digital

Del papel al archivo digital

Esta transformación no consiste simplemente en escanear documentos: el propósito es avanzar desde un modelo con fuerte componente en papel hacia un archivo digital de gestión.

Controlar el ciclo documental del Departamento.

Construir expedientes digitales íntegros, ordenados y trazables.

Convertir el archivo en una herramienta de gestión, no solo de almacenamiento.

Expediente digital íntegro y trazable

Contenido asociado al expediente

- Documentos de ingreso
- Antecedentes y fuentes jurídicas
- Versiones del proyecto
- Observaciones y visaciones
- Decisión final

Trazabilidad exigida

- Quién intervino
- Qué modificación realizó
- En qué momento
- Cuál es el estado efectivo del asunto

Alcance del avance: diseño, implementación y medición

Una gestión responsable distingue lo diseñado, lo implementado y los efectos efectivamente medidos.



COMPLETADO

Diseñado

Instrucciones y modelo de control del ciclo documental



EN CURSO

Implementación

Migración desde el archivo en papel hacia el archivo digital



PENDIENTE DE EVALUACIÓN

Efectos medidos

Resultados que deberán evaluarse durante la implementación