FORMACIÓN PARA EL SECTOR PÚBLICO · CHILE

CONFIDENCIALIDAD, PROTECCIÓN DE DATOS Y RESPONSABILIDADES

Módulo 6 · Ley de Transparencia y Acceso a la Información Pública

Resumen profesional, guía de aplicación y actualización normativa 2026

PUNTO DE VIGENCIA 2026

Hasta el 30 de noviembre de 2026: Ley N.º 19.628 en su versión vigente.
Desde el 1 de diciembre de 2026: reforma de la Ley N.º 21.719 y nuevo marco de datos.
Fecha de actualización del material: 17 de julio de 2026.

RESUMEN EJECUTIVO +

Presentación

Este documento resume y desarrolla los contenidos esenciales del Módulo 6. Su propósito es apoyar a funcionarios, autoridades, equipos jurídicos, unidades de transparencia, control interno, tecnologías y responsables de datos en decisiones que equilibran publicidad, vida privada, seguridad y responsabilidad administrativa.

La transparencia es la regla y la reserva es excepcional. Sin embargo, una entrega irreflexiva puede exponer datos personales, información sensible o detalles de seguridad. La competencia profesional consiste en reconocer la información pública, identificar afectaciones, aplicar divisibilidad, preparar una versión pública técnicamente segura, documentar la decisión y cumplir plazos.

La actualización distingue los dos momentos normativos de 2026. La Ley N.º 19.628 mantiene su versión vigente hasta el 30 de noviembre. La reforma integral introducida por la Ley N.º 21.719 entra en vigor el 1 de diciembre de 2026. El documento también incorpora la Ley N.º 20.285, su Reglamento, referencias a seguridad y las sanciones de sus artículos 45, 46 y 47.

Extensión del recurso interactivo: 19,354 palabras educativas, seis unidades, simulador y actividades.

Resultados de aprendizaje

- Explicar los límites legítimos a la publicidad y aplicar las causales de reserva de manera fundada.
- Diferenciar datos personales, sensibles, funcionales, empresariales y de contexto.
- Aplicar divisibilidad, anonimización, seudonimización y tarjado seguro.
- Tramitar la comunicación y oposición de terceros conforme al artículo 20.
- Prevenir entregas incompletas, incidentes de seguridad y publicaciones excesivas.
- Reconocer responsabilidades y sanciones de los artículos 45, 46 y 47.
- Preparar una hoja de ruta institucional para la reforma de datos desde diciembre de 2026.

Índice de contenidos

1. Transparencia y límites legítimos

La publicidad es la regla; el secreto o reserva es excepcional, debe tener fundamento legal y aplicarse de manera estricta, proporcional y documentada.

1.1 La publicidad como regla constitucional y legal

El sistema chileno de acceso a la información pública parte de una presunción favorable a la publicidad. El artículo 8 de la Constitución vincula la transparencia con el ejercicio de la función pública, mientras la Ley N.º 20.285 transforma esa orientación constitucional en obligaciones concretas: publicar información relevante de manera permanente, responder solicitudes, justificar las negativas y permitir el control externo. La transparencia no es una concesión voluntaria de la autoridad, sino una condición de legitimidad democrática. Permite examinar cómo se adoptan decisiones, cómo se utilizan recursos y cómo se cumplen las funciones públicas.

La Ley N.º 20.285 define como pública la información contenida en actos, resoluciones, actas, expedientes, contratos y acuerdos, además de aquella elaborada con presupuesto público o que obre en poder de un órgano de la Administración, cualquiera sea su formato. Este criterio evita que la publicidad dependa de la tecnología, del nombre del archivo o del lugar donde se almacena. Un correo institucional, una base de datos, una grabación, un registro de plataforma o una planilla pueden estar sujetos al derecho de acceso cuando documentan el ejercicio de una función pública.

La regla de apertura se complementa con los principios de relevancia, libertad de información, máxima divulgación, facilitación, oportunidad, no discriminación, gratuidad, control y responsabilidad. Estos principios sirven para resolver dudas interpretativas. Cuando existen dos formas razonables de tramitar una solicitud, debe preferirse la que facilite el acceso sin desconocer una causal legal de protección. La autoridad no puede crear requisitos nuevos, exigir al solicitante que explique su interés ni denegar por mera incomodidad administrativa.

1.2 Fundamentos doctrinales, autores y aplicación práctica

La transparencia pública puede comprenderse desde varias tradiciones teóricas complementarias. Norberto Bobbio relacionó la democracia con la visibilidad del poder: las decisiones públicas deben poder ser conocidas, discutidas y controladas por la ciudadanía. Aplicada a una institución chilena, esta idea exige que la regla organizacional sea documentar, conservar y explicar; la opacidad sólo puede admitirse cuando una norma válida protege un bien específico. La publicidad, por tanto, no se reduce a publicar archivos, sino que permite evaluar razones, procedimientos, uso de recursos y responsabilidad de quienes ejercen autoridad.

Toby Mendel sistematizó el principio de máxima divulgación en el estudio comparado de la libertad de información. Su planteamiento sostiene que el acceso debe abarcar la mayor cantidad posible de información, que las excepciones han de ser limitadas y que corresponde a la autoridad justificar la negativa. En la práctica, este enfoque se traduce en buscar una versión pública, entregar información por partes, ofrecer formatos comprensibles y evitar que una causal se extienda a datos que no producen la afectación alegada. La Ley N.º 20.285 recoge una lógica compatible mediante máxima divulgación, facilitación y divisibilidad.

La protección de la privacidad aporta una segunda familia de fundamentos. Daniel Solove advierte que los riesgos no se limitan a revelar un dato íntimo aislado: también surgen por agregación, identificación, uso secundario, inseguridad, exclusión del titular o difusión fuera de contexto. Esta mirada ayuda a comprender por qué una base sin nombres todavía puede reidentificar personas al combinar edad, comuna, fecha, cargo y diagnóstico. Para una respuesta de transparencia, la aplicación consiste en

evaluar el conjunto de campos, las fuentes externas disponibles y los daños previsibles, no sólo borrar RUT o nombres.

Helen Nissenbaum desarrolló la idea de integridad contextual: la privacidad depende de que la información circule de acuerdo con normas apropiadas al contexto, considerando quién entrega, quién recibe, qué atributo se comunica y bajo qué condición. Un dato proporcionado para obtener una prestación social no queda automáticamente habilitado para difusión masiva. Al mismo tiempo, el contexto de control del gasto puede justificar publicar criterios, montos y decisiones. La aplicación práctica exige distinguir la finalidad original, el propósito de acceso, el rol público de las personas y la posibilidad de satisfacer el interés ciudadano con datos menos intrusivos.

Ann Cavoukian formuló los principios de privacidad desde el diseño, que proponen prevenir riesgos, configurar protección por defecto e integrar privacidad durante todo el ciclo de una solución. En transparencia, esta perspectiva evita improvisar el tarjado al final del plazo. La institución diseña desde el inicio formularios que no recolecten datos innecesarios, bases con campos separables, perfiles de acceso, plantillas de versión pública, registros de trazabilidad y controles de calidad. La protección deja de ser una corrección tardía y se convierte en una característica del proceso.

Estas teorías no reemplazan la legislación chilena ni la jurisprudencia del Consejo para la Transparencia. Funcionan como marcos de razonamiento para aplicar las normas. Bobbio ayuda a recordar por qué la apertura es democrática; Mendel orienta a maximizar la entrega; Solove permite reconocer riesgos acumulativos; Nissenbaum obliga a examinar la circulación contextual; Cavoukian impulsa controles preventivos. Frente a un expediente mixto, el método integrado es: comenzar desde la publicidad, identificar los flujos de datos y bienes protegidos, demostrar el daño, escoger la medida menos restrictiva, preparar una versión segura y dejar evidencia verificable de la decisión.

1.3 El carácter excepcional de la reserva

El derecho de acceso no es absoluto. La propia Constitución admite excepciones establecidas por una ley de quórum calificado cuando la publicidad afecte el debido cumplimiento de las funciones del órgano, los derechos de las personas, la seguridad de la Nación o el interés nacional. La Ley N.º 20.285 desarrolla estas hipótesis principalmente en su artículo 21. La consecuencia práctica es doble: primero, la reserva requiere una norma habilitante; segundo, la afectación debe ser explicada de manera concreta y no mediante fórmulas genéricas.

Invocar una causal no equivale a demostrarla. Una respuesta jurídicamente robusta identifica la información precisa que se protege, la norma aplicable, el bien jurídico amenazado, el daño razonablemente previsible y la relación entre divulgación y afectación. Expresiones como “información confidencial”, “antecedentes internos” o “por seguridad” son insuficientes si no se explica qué riesgo produciría el acceso. La carga argumentativa aumenta cuando la información se relaciona con gasto público, decisiones que afectan derechos o desempeño de autoridades.

El análisis de reserva debe evitar dos extremos. El primero es publicar sin revisar, exponiendo datos personales, secretos protegidos o vulnerabilidades de seguridad. El segundo es bloquear el expediente completo porque una parte contiene información protegida. La solución normalmente se encuentra en la divisibilidad, la anonimización, el tarjado o la entrega parcial. La reserva total es adecuada sólo cuando separar la información resulta imposible o cuando incluso los fragmentos aparentemente neutros permiten reconstruir el contenido protegido.

1.4 Causales del artículo 21 y daño específico

El artículo 21 de la Ley N.º 20.285 contiene las únicas causales generales que permiten denegar total o parcialmente. La primera protege el debido cumplimiento de las funciones del órgano, por ejemplo cuando la divulgación perjudica una investigación penal, una estrategia judicial, una deliberación previa o distrae indebidamente a los funcionarios frente a una solicitud extraordinariamente amplia. Esta causal no autoriza a proteger indefinidamente borradores ni deliberaciones una vez adoptada la decisión; debe analizarse la etapa del procedimiento y el daño actual.

La segunda causal protege derechos de las personas, especialmente su seguridad, salud, vida privada y derechos comerciales o económicos. Es central para este módulo porque conecta transparencia con protección de datos. No todo dato personal produce automáticamente reserva: debe evaluarse su naturaleza, contexto, finalidad, expectativa razonable de privacidad, participación del titular en la función pública y posibilidad de disociación. El nombre de una autoridad que actúa en ejercicio de su cargo normalmente tiene un nivel de publicidad mayor que la dirección particular de un beneficiario.

Las causales tercera y cuarta resguardan la seguridad de la Nación y el interés nacional. Deben aplicarse con especial rigor porque pueden abarcar antecedentes sensibles de defensa, orden público, seguridad pública, salud pública, relaciones internacionales o intereses económicos del país. La quinta causal remite a información declarada secreta o reservada por una ley de quórum calificado. En todos los casos, la respuesta debe indicar la causal exacta y explicar por qué la afectación es presente o probable, específica y suficientemente seria.

1.5 Principio de divisibilidad y acceso parcial

La divisibilidad obliga a entregar la parte pública de un documento y excluir sólo aquello protegido. Es una herramienta jurídica y técnica. Jurídica, porque limita el alcance de la reserva; técnica, porque exige preparar una versión pública que impida recuperar lo oculto. El tarjado visual sobre un PDF no sirve si el texto sigue seleccionable o permanece en capas, comentarios, metadatos o versiones anteriores. La anonimización debe ser irreversible o razonablemente resistente a la reidentificación según el contexto.

Un expediente de contratación puede contener resoluciones, criterios de evaluación y montos públicos junto con teléfonos particulares, cuentas bancarias, firmas manuscritas, datos de salud o antecedentes familiares. La respuesta adecuada no consiste en entregar todo ni en denegar todo. Debe crearse una copia pública, mantener el original bajo custodia, registrar qué campos se eliminaron y explicar la norma que justifica cada categoría de ocultamiento. El solicitante debe comprender que recibió una entrega parcial fundada y no una versión arbitrariamente incompleta.

La divisibilidad también se aplica a bases de datos. Puede eliminarse una columna, agrupar valores, usar rangos, sustituir identificadores por códigos, reducir precisión geográfica o temporal y aplicar umbrales mínimos. La elección depende del riesgo de reidentificación. Una base sin nombres puede seguir identificando personas si combina comuna pequeña, edad exacta, cargo único, fecha y diagnóstico. Por ello, la anonimización exige analizar el conjunto y las fuentes externas disponibles, no sólo borrar el RUT.

1.6 Test de daño, interés público y proporcionalidad

Aunque la ley no formula un único algoritmo, la práctica decisional utiliza razonamientos equivalentes a un test de daño: identificar el bien protegido, describir el daño, evaluar su probabilidad y gravedad, verificar el nexo causal y considerar medidas menos restrictivas. La mera posibilidad remota o especulativa no basta. El órgano debe demostrar por qué la publicidad produciría una afectación que supera el valor democrático del acceso.

El interés público puede fortalecer la necesidad de divulgar, especialmente cuando la información permite controlar gasto, conflictos de interés, prestaciones, seguridad de servicios o cumplimiento de obligaciones. Esto no significa que el interés periodístico o ciudadano elimine toda privacidad. La evaluación debe ponderar si el mismo objetivo se logra con una versión disociada, estadísticas agregadas o información contextual. La transparencia responsable busca maximizar el control social con el mínimo sacrificio necesario de derechos.

La proporcionalidad ordena escoger una medida idónea, necesaria y equilibrada. Si basta con ocultar datos de contacto, no corresponde denegar el documento completo. Si una tabla agregada permite comprender el desempeño sin revelar casos individuales, puede ser preferible. Si la entrega inmediata de detalles técnicos crea un riesgo de seguridad activo, puede corresponder reservarlos mientras subsiste el riesgo y divulgar posteriormente antecedentes generales. Toda decisión debe quedar trazable y ser revisable.

1.7 Profundización: Cómo documentar una causal de reserva

El expediente contiene partes públicas y fragmentos cuya divulgación podría afectar una investigación, derechos de terceros o seguridad. La dificultad no está en nombrar una causal, sino en explicar por qué opera respecto de antecedentes determinados y en el momento concreto de la solicitud.

Desde una perspectiva jurídica y de gestión, La Ley N.º 20.285 exige una negativa escrita y fundada. El artículo 21 enumera causales taxativas, mientras los principios de máxima divulgación y divisibilidad reducen el alcance de la restricción. La autoridad debe conectar norma, información, bien protegido y daño. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. El análisis comienza delimitando el fragmento, identificando el bien jurídico y describiendo el escenario de afectación. Después se evalúa probabilidad, gravedad, temporalidad y medidas menos restrictivas. Finalmente se decide entre entrega, entrega parcial, consulta a tercero o reserva. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error frecuente es usar frases estandarizadas sin hechos, o afirmar que el documento es “interno”. Esto impide al solicitante comprender la decisión y dificulta la defensa ante un amparo. También es incorrecto extender la reserva a anexos que no generan el mismo daño. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. La evidencia mínima incluye matriz de campos, informe de la unidad técnica, fundamento jurídico, versión pública y registro de revisión. Esta documentación demuestra que la decisión no fue automática y permite reevaluar si desaparece el riesgo. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento,

tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer, decidir, ejecutar, verificar y aprender.

1.8 Profundización: Publicidad de borradores y deliberaciones previas

Los equipos producen minutas, comentarios, correos y versiones preliminares antes de adoptar una resolución. Algunos antecedentes pueden formar parte de la deliberación protegida; otros son datos de base, informes terminados o documentos externos que conservan carácter público.

Desde una perspectiva jurídica y de gestión, La causal relativa a deliberaciones previas busca proteger un proceso decisorio real, no crear un archivo secreto permanente. Una vez adoptada la medida, sus fundamentos son públicos, sin perjuicio de otras causales que puedan subsistir. Debe demostrarse vínculo directo con una decisión pendiente. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. Se clasifica cada documento según función: antecedente factual, opinión, recomendación, borrador, decisión o comunicación logística. Se identifica la decisión pendiente y se analiza si divulgar afectaría efectivamente el proceso. Los datos objetivos separables pueden entregarse. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, Un error es considerar reservado todo correo anterior a una resolución. Otro es mantener la causal después de finalizada la decisión sin revisar. También se debilita la fundamentación cuando no se identifica qué política o medida estaba en preparación. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. La carpeta de decisión debe conservar cronología, versiones y acto final. Una tabla que relacione documento, etapa y función facilita entregar antecedentes objetivos y proteger sólo la deliberación estrictamente necesaria. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer,

decidir, ejecutar, verificar y aprender.

1.9 Profundización: Distracción indebida y gestión documental

Una solicitud puede abarcar miles de registros, formatos antiguos o información distribuida. La institución debe distinguir una carga realmente extraordinaria de la dificultad causada por desorden, falta de digitalización o ausencia de responsables.

Desde una perspectiva jurídica y de gestión, La causal de distracción indebida requiere demostrar que la atención afecta de forma relevante las funciones habituales. No basta calcular muchas horas sin explicar dotación, tareas, sistemas, período, búsqueda y alternativas. La facilitación obliga a explorar acotamiento o entrega progresiva. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. Se estima volumen, fuentes, pasos de búsqueda, necesidad de revisión y personal disponible. Se conversa con el solicitante para precisar período o variables, se ofrecen datos ya estructurados y se evalúan entregas parciales. El cálculo debe ser reproducible y razonable. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error es invocar la causal por una cifra grande sin intentar búsqueda, o trasladar al solicitante las consecuencias de una mala gestión documental. También es riesgoso prometer una entrega imposible y luego incumplir plazos. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. La evidencia incluye inventario de fuentes, muestra de registros, estimación por tarea, carga de la unidad y propuestas de facilitación. Los resultados deben alimentar mejoras de archivo y datos para reducir futuras cargas. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer, decidir, ejecutar, verificar y aprender.

1.10 Profundización: Reserva temporal y revisión periódica

Algunas afectaciones existen sólo mientras una investigación está abierta, una negociación se encuentra en curso o una vulnerabilidad permanece sin corregir. La respuesta debe reconocer que la sensibilidad puede cambiar.

Desde una perspectiva jurídica y de gestión, Las excepciones se interpretan según el daño actual. Mantener indefinidamente una protección cuya razón desapareció contradice máxima divulgación. La ley también regula la duración de actos formalmente declarados secretos o reservados y la posibilidad de reevaluación. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. La decisión registra hecho gatillante, fecha, responsable y condición de término. Cuando el riesgo cesa, se revisa la clasificación y se prepara una versión más amplia. En solicitudes posteriores no se copia la respuesta anterior sin verificar circunstancias. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error es convertir una reserva situacional en permanente o, a la inversa, divulgar anticipadamente por asumir que el tiempo transcurrido eliminó el daño. La revisión requiere consulta a la unidad competente y evidencia actual. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. Un registro de reservas temporales con alertas, causal, objeto y fecha de revisión permite gobernar el ciclo de vida. La reevaluación documentada mejora confianza y reduce litigios. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer, decidir, ejecutar, verificar y aprender.

Síntesis de la unidad. La aplicación profesional requiere una decisión trazable: identificar información, norma y riesgo; escoger la medida menos restrictiva; verificar técnicamente; fundamentar; entregar; conservar evidencia y revisar el aprendizaje institucional.

2. Datos personales y confidencialidad

La transparencia debe convivir con la vida privada, la autodeterminación informativa y el deber de secreto respecto de datos obtenidos desde fuentes no accesibles al público.

2.1 Régimen vigente hasta el 30 de noviembre de 2026

A la fecha de actualización de este recurso, la Ley N.º 19.628 mantiene su versión vigente hasta el 30 de noviembre de 2026. Esta ley autoriza el tratamiento de datos personales cuando existe habilitación legal o consentimiento, exige respetar la finalidad del tratamiento y reconoce derechos de información, modificación, eliminación o bloqueo en los casos previstos. Para los organismos públicos, el tratamiento debe relacionarse con materias de su competencia y con las finalidades que justificaron la recolección.

La ley define dato personal como información relativa a una persona natural identificada o identificable. Son datos sensibles aquellos que se refieren a características físicas o morales o a hechos de la vida privada o intimidad, como hábitos personales, origen racial, ideologías, opiniones políticas, creencias religiosas, estados de salud físicos o psíquicos y vida sexual. La sensibilidad no depende sólo del formato. Una conclusión administrativa, una fotografía, un audio o una inferencia automatizada puede revelar información sensible.

El artículo 7 de la Ley N.º 19.628 impone secreto a quienes trabajan en el tratamiento de datos provenientes de fuentes no accesibles al público y extiende la obligación más allá del término de sus funciones. En el sector público, este deber se combina con obligaciones estatutarias, probidad, seguridad de la información y reglas de acceso. La confidencialidad exige impedir accesos no autorizados; no significa declarar reservado todo antecedente que contenga datos personales.

2.2 Reforma de la Ley N.º 21.719 desde el 1 de diciembre de 2026

La Ley N.º 21.719, publicada el 13 de diciembre de 2024 y modificada antes de su vigencia, reforma integralmente el régimen chileno de datos personales y crea la Agencia de Protección de Datos Personales. Su entrada en vigor está prevista para el 1 de diciembre de 2026. El cambio fortalece derechos, obligaciones de responsables y encargados, supervisión, seguridad, responsabilidad demostrable y sanciones. Por ello, durante 2026 los organismos deben gestionar simultáneamente cumplimiento vigente y preparación institucional.

El nuevo régimen incorpora principios expresos como licitud y lealtad, finalidad, proporcionalidad, calidad, responsabilidad, seguridad, transparencia e información, y confidencialidad. Los datos deben limitarse a lo necesario, mantenerse exactos y conservarse sólo durante el tiempo requerido. El responsable debe poder demostrar cumplimiento, no limitarse a declarar buenas intenciones. Esto requiere inventarios, bases de licitud, políticas, contratos, registros, evaluación de riesgos, gestión de incidentes y mecanismos para responder derechos.

Para la transparencia pública, la reforma no elimina el derecho de acceso. Exige mejorar la capacidad de distinguir información pública de datos que requieren protección. La preparación debe incluir matrices de publicación, criterios de anonimización, perfiles de acceso, revisión de formularios, reducción de datos solicitados, protocolos de transferencia y documentación de decisiones. El funcionario que tramita solicitudes necesita comprender tanto la Ley N.º 20.285 como el régimen de datos para evitar entregas excesivas o denegaciones automáticas.

2.3 Datos de contexto, datos sensibles y expectativas de privacidad

En la práctica se suele hablar de datos personales de contexto para referirse a identificadores o datos de contacto que aparecen incidentalmente en documentos públicos: RUT, domicilio particular, teléfono personal, correo privado, fecha de nacimiento, nacionalidad, estado civil o firma manuscrita. La categoría ayuda a preparar versiones públicas, pero no reemplaza el análisis jurídico. Algunos datos pueden ser necesarios para identificar a un proveedor o verificar un beneficio; otros pueden ocultarse sin afectar el control social.

Los datos sensibles requieren mayor cautela porque su divulgación puede generar discriminación, daño reputacional, afectación de seguridad o invasión intensa de la vida privada. Los diagnósticos, licencias médicas, antecedentes de salud mental, condición de discapacidad, información biométrica o situaciones familiares no deben exponerse por rutina. Cuando existe un interés público legítimo, suele ser suficiente divulgar estadísticas, criterios, montos, decisiones o responsabilidades institucionales sin revelar la identidad del afectado.

La expectativa de privacidad varía según el rol y el contexto. Los datos funcionales de autoridades y funcionarios vinculados al ejercicio del cargo tienen mayor exposición que los aspectos de su vida privada. Sin embargo, ser funcionario no elimina la protección de domicilio, salud, familia, datos bancarios o seguridad personal. A la inversa, el hecho de que una persona sea particular no vuelve secreto todo vínculo contractual o beneficio financiado con recursos públicos. La clave es separar función pública, control del gasto y esfera privada.

2.4 Consentimiento, habilitación legal y finalidad

En organismos públicos, el consentimiento no siempre es la base adecuada. Muchas operaciones se realizan porque una ley atribuye competencia y ordena o autoriza el tratamiento. La institución debe identificar la habilitación, la finalidad y los datos estrictamente necesarios. Pedir consentimiento para una obligación legal puede ser engañoso si la persona no puede negarse sin perder un trámite. Del mismo modo, usar datos recogidos para una finalidad social con un propósito incompatible requiere una nueva base o una evaluación jurídica específica.

La finalidad funciona como límite material. Un dato recolectado para pagar una prestación no puede difundirse libremente en un portal. Un registro de asistencia laboral no debería reutilizarse para fines ajenos sin fundamento. Una base entregada por otro organismo debe usarse dentro del propósito autorizado. La transparencia puede justificar la comunicación de ciertos elementos, pero no transforma todo el banco de datos en fuente pública.

La respuesta a una solicitud debe distinguir entre acceso a información pública y acceso del titular a sus propios datos. Cuando una persona pide información sobre sí misma puede existir un canal especial de protección de datos o procedimiento sectorial. Cuando un tercero pide información sobre otra persona, deben analizarse el artículo 20 de la Ley N.º 20.285, la causal del artículo 21 N.º 2, la finalidad pública, la divisibilidad y las normas especiales aplicables.

2.5 Confidencialidad como conducta organizacional

La confidencialidad no se logra únicamente con cláusulas. Requiere controles de acceso, segregación de funciones, autenticación, registro de consultas, capacitación, acuerdos con proveedores, eliminación segura y respuesta a incidentes. Un archivo puede estar correctamente clasificado y aun así filtrarse por envío a un destinatario equivocado, uso de cuentas personales, enlaces abiertos, dispositivos sin cifrado o impresiones abandonadas.

Los equipos de transparencia deben aplicar el principio de necesidad de conocer. No todos los funcionarios necesitan acceder al expediente completo. Para preparar una respuesta, puede utilizarse una copia de trabajo con campos reducidos. Los borradores deben almacenarse en repositorios institucionales y eliminarse cuando corresponda. Las versiones públicas deben revisarse por una segunda persona en casos de alto riesgo.

La cultura de confidencialidad también exige comunicar con precisión. No debe prometerse secreto absoluto cuando la ley permite acceso, ni informarse al titular que sus antecedentes “jamás serán compartidos” si existe una obligación legal. Las políticas deben explicar quién trata datos, para qué, por cuánto tiempo, con quién se comunican y cómo ejercer derechos. La transparencia sobre el tratamiento es compatible con la reserva del contenido individual.

2.6 Profundización: Diferenciar dato personal de información sobre personas jurídicas

Los expedientes mezclan nombres de personas naturales, razones sociales, representantes, contactos y beneficiarios finales. Una clasificación imprecisa puede proteger indebidamente información empresarial o exponer datos de individuos.

Desde una perspectiva jurídica y de gestión, La Ley N.º 19.628 protege información relativa a personas naturales identificadas o identificables. Una persona jurídica no es titular bajo esa definición, aunque sus documentos pueden contener datos personales o secretos comerciales protegidos por otras normas. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. Se identifica quién es el sujeto de cada campo. La razón social, RUT de empresa, monto y contrato se analizan desde transparencia y derechos comerciales; el teléfono personal, firma, domicilio particular o datos del representante se evalúan como datos personales. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error es usar “protección de datos” para ocultar cualquier antecedente de una empresa, o publicar sin revisión una ficha societaria con datos personales de contacto. También debe evitarse confundir representante legal con titular de todos los datos del contrato. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. La matriz debe separar persona natural, persona jurídica, dato funcional y dato privado. Esta distinción mejora la consulta a terceros y permite respuestas más precisas. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información

eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer, decidir, ejecutar, verificar y aprender.

2.7 Profundización: Datos personales en actos administrativos

Resoluciones, decretos y certificados pueden contener información necesaria para producir efectos jurídicos junto con RUT, domicilios, correos, firmas o antecedentes sensibles. La publicación íntegra no siempre es necesaria para acreditar el acto.

Desde una perspectiva jurídica y de gestión, La publicidad del acto y sus fundamentos se armoniza con la protección de derechos mediante divisibilidad. Debe conservarse la información necesaria para comprender competencia, decisión, destinatario cuando sea relevante y fundamento, excluyendo datos incidentales o sensibles. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. Se analiza finalidad de publicación, audiencia y riesgo. En una versión pública puede mantenerse nombre y calidad cuando son esenciales, mientras se reduce el RUT, se elimina domicilio, se oculta firma manuscrita y se protege salud o información familiar. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error es reemplazar toda identidad por iniciales cuando impide verificar una decisión, o publicar todos los campos porque aparecen en el original. La versión pública debe ser útil y proporcional. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. Las plantillas de actos pueden separar campos publicables y restringidos desde su creación. Esta práctica evita tarjados manuales repetitivos y reduce errores. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer, decidir, ejecutar, verificar y aprender.

2.8 Profundización: Información de salud y licencias médicas

Las instituciones administran licencias, ausencias, compatibilidad laboral, accidentes y prestaciones. El control de dotación y gasto puede ser legítimo, pero el diagnóstico y la historia clínica pertenecen a una esfera especialmente protegida.

Desde una perspectiva jurídica y de gestión, La salud es dato sensible. La transparencia puede justificar fechas, duración, costo agregado, procedimientos o decisiones administrativas, pero rara vez necesita revelar diagnóstico, tratamiento, pronóstico o detalles íntimos. Normas sectoriales pueden reforzar el secreto. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. Se define el objetivo de control y la mínima información necesaria. Se prefieren estadísticas, rangos, códigos y actos con datos sensibles excluidos. Cuando la identidad de una autoridad sea relevante, se analiza el vínculo funcional sin divulgar detalles clínicos. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error es publicar certificados, imágenes o antecedentes médicos como respaldo de una resolución, o denegar toda información sobre gasto y gestión. Ambos extremos desconocen la posibilidad de una versión pública. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. El control incluye repositorios separados, accesos limitados, revisión por personal autorizado y registro de cada comunicación. Las copias de trabajo deben eliminarse según política. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer, decidir, ejecutar, verificar y aprender.

2.9 Profundización: Preparación para derechos bajo la reforma de 2026

La reforma fortalece derechos y exige procedimientos capaces de localizar, comprender, corregir, suprimir u oponerse al tratamiento en los casos aplicables. La institución debe evitar que cada solicitud dependa de búsquedas improvisadas.

Desde una perspectiva jurídica y de gestión, Desde el 1 de diciembre de 2026 el nuevo régimen exige principios reforzados, responsabilidad y supervisión de la Agencia. La transición debe respetar el régimen vigente hasta el 30 de noviembre y preparar procesos, roles y evidencia. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. Se crean canales, verificación de identidad, registro de plazos, responsables, búsqueda en sistemas, análisis de excepciones y respuesta comprensible. Los equipos de transparencia y datos coordinan cuando una petición puede corresponder a más de un derecho. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error es tratar toda petición del titular como solicitud de transparencia o exigir antecedentes excesivos para verificar identidad. También es riesgoso diseñar el proceso sin inventario de sistemas. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. Las pruebas de escritorio con casos simulados permiten medir tiempo, encontrar datos duplicados y corregir inconsistencias antes de la entrada en vigor. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer, decidir, ejecutar, verificar y aprender.

Síntesis de la unidad. La aplicación profesional requiere una decisión trazable: identificar información, norma y riesgo; escoger la medida menos restrictiva; verificar técnicamente; fundamentar; entregar; conservar evidencia y revisar el aprendizaje institucional.

3. Seguridad de la información y prevención

Proteger datos e información reservada exige medidas técnicas, organizativas y documentales proporcionales al riesgo y al impacto de una divulgación indebida.

3.1 Seguridad, confidencialidad, integridad y disponibilidad

La seguridad de la información suele organizarse en torno a confidencialidad, integridad y disponibilidad. Confidencialidad significa que sólo acceden personas autorizadas; integridad, que la información no se altera sin autorización y conserva su exactitud; disponibilidad, que puede utilizarse cuando la función pública lo requiere. A estas dimensiones se agregan trazabilidad, autenticidad y resiliencia. La transparencia depende de todas ellas: una institución no puede responder correctamente si perdió archivos, si desconoce cuál versión es auténtica o si sus registros fueron modificados.

La protección debe ser proporcional al riesgo. Una nómina pública de unidades institucionales no requiere el mismo nivel que una base de víctimas, antecedentes de salud, claves, vulnerabilidades o datos biométricos. La evaluación considera volumen, sensibilidad, número de titulares, posibilidad de discriminación, consecuencias económicas, riesgo físico y facilidad de reidentificación. La medida adecuada surge de ese diagnóstico, no de una lista genérica.

La Ley Marco de Ciberseguridad N.º 21.663 y la Ley N.º 21.459 sobre delitos informáticos forman parte del entorno normativo de seguridad, aunque su aplicación concreta depende del órgano y del incidente. Para este módulo, su enseñanza principal es que la reserva de detalles técnicos puede justificarse cuando su divulgación aumenta un riesgo real, pero no autoriza a ocultar información general sobre gobernanza, gasto, políticas, resultados o medidas correctivas que pueda publicarse sin exponer vulnerabilidades explotables.

3.2 Clasificación y ciclo de vida documental

Clasificar información permite aplicar controles consistentes. Una matriz sencilla puede distinguir información pública, de uso interno, confidencial o reservada por causal legal. La etiqueta debe estar asociada a reglas: quién accede, cómo se comparte, cuánto se conserva, cómo se elimina y quién puede reclasificar. Marcar todo como confidencial destruye la utilidad del sistema; no marcar nada expone a la institución.

El ciclo de vida comienza en la recolección. Deben solicitarse sólo los datos necesarios, validar su calidad, registrar la fuente y definir conservación. Durante el uso, se controla acceso y transmisión. En la publicación o entrega, se revisa divisibilidad y anonimización. Al finalizar la finalidad, se elimina, bloquea o archiva conforme a normas de gestión documental. Cada etapa puede generar obligaciones de transparencia y protección diferentes.

La gestión de versiones es crítica. El original debe preservarse con integridad, mientras la copia pública se prepara en un espacio controlado. El nombre del archivo debe permitir distinguir “original”, “trabajo” y “versión pública”. Antes de entregar, se revisan propiedades, comentarios, historial, capas ocultas, adjuntos, enlaces, firmas, miniaturas y texto extraíble. Una captura o impresión a PDF puede reducir algunos riesgos, pero no reemplaza la revisión técnica.

3.3 Anonimización, seudonimización y tarjado seguro

Anonimizar busca impedir que una persona sea identificada de manera razonable, considerando la información disponible y los medios previsibles. Seudonimizar reemplaza identificadores por códigos, pero permite reidentificar con información separada; por ello, sigue siendo tratamiento de datos personales. Tarjar consiste en ocultar campos en una copia pública. Cada técnica tiene objetivos y riesgos distintos.

Para bases de datos, la anonimización puede combinar supresión, generalización, perturbación, agrupación y umbrales. Eliminar el nombre no basta si existe una combinación única. Por ejemplo, “mujer de 63 años, directora de una unidad de tres personas, comuna pequeña, licencia en fecha exacta” puede identificar a alguien. Deben probarse escenarios de enlace con fuentes públicas y preguntarse si un observador razonable podría reconstruir identidad o atributo sensible.

El tarjado seguro debe eliminar el contenido subyacente, no cubrirlo con un rectángulo. Después del proceso se intenta seleccionar, copiar, buscar y extraer el texto; se revisan metadatos y se abre el documento en otro visor. Cuando se publican planillas, conviene exportar sólo la hoja y columnas autorizadas, evitando fórmulas, hojas ocultas, comentarios y nombres definidos. El control de calidad debe quedar registrado.

3.4 Gestión de incidentes y errores de entrega

Un incidente puede consistir en acceso no autorizado, pérdida, alteración, envío erróneo, publicación excesiva, ransomware, credenciales expuestas o divulgación de una versión sin anonimizar. La reacción debe ser rápida y coordinada. Primero se contiene: retirar enlace, revocar permisos, solicitar eliminación, bloquear cuenta o aislar sistema. Luego se preserva evidencia, se evalúa alcance, se informa a responsables y se activa el procedimiento institucional.

La evaluación identifica qué datos se afectaron, cuántas personas, durante cuánto tiempo, quién accedió, si hubo descarga, si existen riesgos físicos, económicos o discriminatorios y qué medidas reducen el daño. Debe documentarse sin alterar evidencia. Según la normativa vigente y sectorial, pueden existir obligaciones de notificación o comunicación. La entrada en vigor de la Ley N.º 21.719 refuerza la necesidad de procedimientos formales y responsabilidad demostrable.

El aprendizaje posterior es indispensable. No basta con culpar al funcionario que presionó “enviar”. Se revisan causas: interfaz confusa, ausencia de doble control, permisos excesivos, capacitación insuficiente, presión de plazo o falta de herramienta de anonimización. Las medidas correctivas deben ser verificables: cambiar configuración, actualizar procedimiento, entrenar, limitar acceso, automatizar revisión o modificar plantilla.

3.5 Seguridad útil, no seguridad como excusa

La seguridad puede transformarse en una excusa para negar información si no se distingue detalle explotable de información de rendición de cuentas. Un informe de auditoría tecnológica puede contener direcciones IP, arquitectura, credenciales, rutas, vulnerabilidades sin corregir y pruebas de concepto; esos elementos requieren protección. Sin embargo, objetivos, alcance, metodología general, hallazgos agregados, nivel de riesgo, presupuesto y estado de medidas correctivas pueden ser divulgables.

La decisión debe considerar temporalidad. Un detalle reservado durante la corrección puede perder sensibilidad después de mitigarse el riesgo. También puede entregarse una versión pública preparada por el área técnica, en lugar de negar el informe completo. La respuesta debe explicar el daño específico y la medida menos restrictiva adoptada.

La transparencia fortalece seguridad cuando permite controlar gobernanza, inversión, cumplimiento, aprendizaje de incidentes y responsabilidad. La seguridad fortalece transparencia cuando preserva registros confiables y evita que el temor a filtraciones lleve a sistemas cerrados. El objetivo institucional es un equilibrio maduro: apertura por diseño y protección por diseño.

3.6 Profundización: Control de acceso basado en roles

Una unidad suele compartir expedientes entre transparencia, jurídica, personal, tecnología y jefaturas. El acceso indiscriminado incrementa el riesgo de filtración y dificulta atribuir acciones.

Desde una perspectiva jurídica y de gestión, La confidencialidad exige limitar acceso a quienes lo necesitan para una función. La responsabilidad demostrable y las buenas prácticas de seguridad requieren perfiles, autenticación, revisión periódica y trazabilidad. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. Se definen roles de consulta, edición, aprobación y publicación. Se eliminan cuentas compartidas, se aplica mínimo privilegio, se revisan permisos al cambiar funciones y se protegen descargas. Los accesos de emergencia quedan registrados. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error es otorgar acceso a carpetas completas por comodidad o mantener permisos de funcionarios que cambiaron de unidad. Las cuentas compartidas impiden saber quién descargó o modificó. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. Los reportes de permisos, bitácoras, revisiones trimestrales y actas de baja constituyen evidencia. Los hallazgos deben generar correcciones, no sólo informes. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer, decidir, ejecutar, verificar y aprender.

3.7 Profundización: Metadatos y contenido oculto

Un documento aparentemente limpio puede contener comentarios, historial, autores, rutas locales, capas, hojas ocultas, fórmulas o adjuntos. Estos elementos pueden revelar datos personales, estrategias o información reservada.

Desde una perspectiva jurídica y de gestión, La obligación de proteger no se limita a lo visible. Una entrega incluye todo lo que el archivo permite recuperar razonablemente. Por ello, el control técnico forma parte de la diligencia en la versión pública. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. Se inspeccionan propiedades, comentarios, control de cambios, objetos incrustados, hojas y columnas ocultas, texto alternativo y miniaturas. Luego se exporta o sanea y se prueba búsqueda, copia y extracción en otra aplicación. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error más conocido es cubrir texto con figuras. Otro es entregar la planilla original creyendo que un filtro elimina filas. Los filtros y ocultamientos son reversibles. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. Una lista de verificación firmada, herramienta institucional de saneamiento y muestra de prueba aportan evidencia. Los documentos de alto riesgo requieren segunda revisión. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer, decidir, ejecutar, verificar y aprender.

3.8 Profundización: Copias, respaldos y eliminación segura

La preparación de respuestas genera originales, copias de trabajo, versiones públicas, correos y descargas temporales. Sin reglas, la información sensible se multiplica y permanece en equipos personales.

Desde una perspectiva jurídica y de gestión, La conservación debe responder a finalidad, obligaciones archivísticas y seguridad. Eliminar demasiado pronto afecta trazabilidad; conservar indefinidamente aumenta exposición. Se necesita un calendario diferenciado. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. El original se mantiene en expediente oficial. Las copias de trabajo usan repositorios controlados, nombres claros y fecha de eliminación. Los respaldos se protegen y se prueban. La eliminación considera papel, discos, nube y cachés. Cada paso debe responder una

pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error es guardar versiones en escritorio, mensajería personal o memorias USB, o suponer que mover a papelera elimina. También es incorrecto destruir evidencia durante un incidente o procedimiento pendiente. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. La evidencia incluye política de retención, registros de eliminación, inventario de copias y pruebas de restauración. La unidad debe conocer quién autoriza excepciones. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer, decidir, ejecutar, verificar y aprender.

3.9 Profundización: Evaluación de proveedores tecnológicos

Servicios de nube, firma, correo masivo, análisis documental o inteligencia artificial pueden tratar información por cuenta del órgano. El contrato y la configuración determinan gran parte del riesgo.

Desde una perspectiva jurídica y de gestión, El organismo sigue siendo responsable de decidir finalidad y de asegurar que el proveedor actúe bajo instrucciones, con confidencialidad, seguridad y reglas de retorno o eliminación. Normas sectoriales y la reforma de datos agregan exigencias. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. Antes de contratar se revisan ubicación, subcontratistas, cifrado, autenticación, registros, continuidad, incidentes, portabilidad y eliminación. El contrato define uso permitido, prohibición de entrenamiento no autorizado y asistencia en derechos. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error es aceptar términos de consumo para expedientes públicos o cargar documentos reales en herramientas gratuitas. También es riesgoso no planificar salida del proveedor. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar

fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. Cuestionarios, informe de riesgo, cláusulas, evidencias de certificación y pruebas de configuración forman el expediente de diligencia. La evaluación se actualiza cuando cambia el servicio. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer, decidir, ejecutar, verificar y aprender.

Síntesis de la unidad. La aplicación profesional requiere una decisión trazable: identificar información, norma y riesgo; escoger la medida menos restrictiva; verificar técnicamente; fundamentar; entregar; conservar evidencia y revisar el aprendizaje institucional.

4. Procedimiento de decisión y entrega

Una buena respuesta no depende de intuiciones: sigue un proceso trazable que identifica el objeto, consulta a terceros, aplica divisibilidad y controla la versión final.

4.1 Paso 1: comprender la solicitud y localizar información

La tramitación comienza leyendo literalmente la solicitud y delimitando qué se pide, en qué período, formato y unidad. No debe confundirse una pregunta, reclamo o petición de pronunciamiento con una solicitud de documentos o información existente. Si falta claridad, la subsanación debe ser específica y facilitadora, no una barrera. El órgano debe buscar en las unidades y sistemas razonablemente vinculados y dejar evidencia de la búsqueda.

Localizar información incluye identificar custodios, soportes, versiones y sistemas. Una respuesta “no existe” requiere una búsqueda seria y, cuando corresponde, explicar las razones de inexistencia. Si la información está en otro órgano, debe analizarse la derivación conforme a la ley. Si está permanentemente disponible, puede indicarse fuente, lugar y forma de acceso, verificando que el enlace sea directo, funcional y contenga efectivamente lo solicitado.

Desde el inicio se detectan riesgos: datos de terceros, secretos comerciales, antecedentes de seguridad, investigaciones, deliberaciones o volumen extraordinario. Esta detección no decide la reserva; activa revisiones y plazos internos. La institución debe evitar esperar hasta el último día para consultar a terceros o preparar una versión pública.

4.2 Paso 2: identificar terceros y aplicar el artículo 20

Cuando los documentos contienen información que puede afectar derechos de terceros, el artículo 20 de la Ley N.º 20.285 obliga a comunicarles la solicitud dentro de dos días hábiles, adjuntando copia del requerimiento y señalando su derecho a oponerse. El tercero dispone de tres días hábiles desde la notificación y debe expresar causa. Si se opone oportunamente, el órgano queda impedido de entregar mientras no exista resolución en contrario del Consejo para la Transparencia.

La comunicación no debe revelar al tercero datos innecesarios del solicitante. Tampoco corresponde activar el artículo 20 de forma masiva por cualquier mención nominal. Debe existir posibilidad de afectación de derechos. La institución conserva responsabilidad por identificar información pública y por tramitar correctamente. La oposición del tercero no convierte automáticamente la información en reservada; habilita un procedimiento en que el Consejo puede revisar la decisión.

Si no existe oposición, se entiende que el tercero accede a la publicidad, pero igualmente deben protegerse datos cuya divulgación esté prohibida por otras normas o que no sean necesarios. El silencio no siempre sanea una entrega excesiva. La respuesta final debe registrar notificaciones, fechas, oposición y tratamiento de datos.

4.3 Paso 3: construir matriz de campos

Una matriz de campos transforma un expediente complejo en decisiones verificables. Para cada elemento se registra: descripción, fuente, finalidad, carácter público, dato personal, sensibilidad, causal potencial, interés público, técnica de protección y decisión. Esto reduce inconsistencias y facilita la revisión por jurídica, transparencia, seguridad o protección de datos.

Por ejemplo, en una nómina de beneficiarios pueden existir nombre, comuna, monto, fundamento del beneficio, RUT, domicilio, teléfono, cuenta bancaria y diagnóstico. No todos reciben la misma respuesta. El monto agregado y criterios suelen ser públicos; el RUT completo, domicilio, teléfono y cuenta

normalmente se eliminan; el diagnóstico se protege; la identidad puede requerir análisis según el programa, norma especial y riesgo. La matriz permite justificar cada columna.

La decisión debe evitar el automatismo “dato personal igual reserva”. La ley de transparencia exige afectación y permite divisibilidad. A la vez, debe evitar el automatismo “uso de recursos públicos igual publicación total”. El control del gasto puede lograrse con montos, criterios, contratos, identificadores de proveedor o datos agregados sin exponer información íntima.

4.4 Paso 4: preparar y verificar la versión pública

La preparación debe realizarse sobre una copia. Se eliminan o transforman los campos protegidos, se agrega una marca que identifique la versión pública y, si resulta útil, una leyenda de tarjado con base normativa. El documento conserva estructura suficiente para comprenderlo. No se debe reemplazar tanta información que la entrega sea ilusoria.

La verificación tiene dos capas. La revisión jurídica confirma que sólo se excluyó lo necesario y que la causal es correcta. La revisión técnica intenta recuperar información oculta, examina metadatos y abre el archivo en diferentes aplicaciones. En bases, se revisan hojas ocultas, filtros, fórmulas, nombres de archivo y datos incrustados. En imágenes, se observan reflejos, credenciales, pantallas y geolocalización.

Antes de enviar, se compara la solicitud con la respuesta: ¿se contestó cada punto?, ¿el formato es utilizable?, ¿los enlaces funcionan?, ¿la resolución explica las exclusiones?, ¿se respetaron plazos y notificaciones?, ¿se certifica la entrega? Este control previene respuestas incompletas que pueden originar amparos y sanciones.

4.5 Paso 5: fundamentar, entregar y conservar trazabilidad

Una denegación total o parcial debe ser escrita, fundada, citar la causal legal y explicar los motivos del caso. La respuesta debe diferenciar información inexistente, no poseída, derivada, publicada, entregada, tarjada y reservada. Mezclar estas categorías genera confusión y debilita la defensa institucional.

La trazabilidad comprende solicitud original, registro de ingreso, derivaciones, búsquedas, comunicaciones internas, notificación a terceros, oposiciones, matriz de análisis, versión original, versión pública, resolución, comprobante de entrega y eventuales incidentes. Estos antecedentes permiten responder un amparo, mejorar el proceso y atribuir responsabilidades.

La conservación debe respetar normas archivísticas y de datos. No corresponde guardar indefinidamente copias de trabajo con datos sensibles por simple comodidad. Debe existir un expediente oficial, controles de acceso y reglas de eliminación. La trazabilidad no exige duplicación desordenada; exige evidencia suficiente, íntegra y localizable.

4.6 Profundización: Búsqueda razonable y declaración de inexistencia

El órgano puede no encontrar la información porque nunca se generó, fue eliminada conforme a norma, está en otra unidad o la búsqueda fue insuficiente. La respuesta debe distinguir estas hipótesis.

Desde una perspectiva jurídica y de gestión, El derecho recae sobre información que obre en poder del órgano. Una declaración de inexistencia debe basarse en gestiones verificables y no en una consulta informal. La derivación procede cuando se identifica otro órgano competente según las reglas legales. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando

intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. Se determina qué unidades, sistemas, archivos y custodios son pertinentes. Se usan términos, fechas e identificadores, se registra resultado y se consulta a responsables. Si la información debió existir, se explica la situación y se activan controles internos. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error es responder “no existe” porque una persona no la conoce, o crear un documento nuevo cuando la solicitud pide información existente. También debe evitarse derivar sin competencia clara. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. La bitácora de búsqueda incluye fecha, unidad, sistema, consulta, responsable y resultado. Permite demostrar diligencia ante un amparo. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer, decidir, ejecutar, verificar y aprender.

4.7 Profundización: Subsanación que facilita y no obstruye

Algunas solicitudes son ambiguas, mezclan períodos o no identifican información. La subsanación debe ayudar a precisar, sin exigir motivos ni conocimientos técnicos innecesarios.

Desde una perspectiva jurídica y de gestión, El principio de facilitación excluye requisitos que obstruyan. La institución debe explicar qué falta y ofrecer ejemplos o categorías disponibles. No corresponde pedir al solicitante que cite leyes o conozca la estructura interna. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. La comunicación formula una pregunta concreta, indica el efecto del plazo y propone alternativas: período, unidad, tipo de documento o formato. Si una parte es clara, se analiza si puede tramitarse mientras se precisa el resto. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia

debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error es enviar una plantilla genérica o declarar inadmisible sin oportunidad real. También es problemático usar subsanación para ganar tiempo cuando la solicitud ya es comprensible. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. Se conserva la comunicación y respuesta, y se mide cuántas subsanaciones terminan en abandono. Tasas altas pueden indicar formularios o portales confusos. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer, decidir, ejecutar, verificar y aprender.

4.8 Profundización: Notificación a terceros sin exponer al solicitante

El artículo 20 exige comunicar la solicitud a personas potencialmente afectadas. Esa comunicación debe contener lo necesario para ejercer oposición, pero no difundir datos adicionales del solicitante.

Desde una perspectiva jurídica y de gestión, El tercero necesita conocer qué información se pide y por qué podría afectarle. El órgano debe respetar plazos de dos y tres días hábiles y registrar notificación. La oposición requiere causa y produce el efecto legal previsto. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. Se prepara una copia del requerimiento con datos innecesarios reducidos, identifica documentos o campos y explica plazo, canal y consecuencias. Se controla recepción y se incorpora la oposición al expediente. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error es notificar tarde, usar correo no acreditable, pedir al tercero que decida sobre información institucional completa o revelar domicilio del solicitante. Tampoco se debe tratar la oposición como decisión final automática. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. La evidencia incluye carta, comprobante, cómputo de plazo, oposición y resolución. Un tablero de alertas previene vencimientos. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer, decidir, ejecutar, verificar y aprender.

4.9 Profundización: Control de integridad de la entrega

Una respuesta puede ser jurídicamente correcta pero materialmente inútil si faltan anexos, los archivos están corruptos o el enlace no funciona. La obligación comprende entrega efectiva.

Desde una perspectiva jurídica y de gestión, La Ley N.º 20.285 exige proporcionar la información en la forma y medio solicitados cuando sea posible y contar con un sistema que certifique entrega. Una orden firme debe cumplirse de manera íntegra y oportuna. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. Se usa una lista de documentos, conteo de archivos, tamaño, formato y hash cuando el riesgo lo amerita. Se prueba descarga desde una cuenta distinta, se verifica accesibilidad y se conserva comprobante. Los enlaces tienen vigencia suficiente. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error es enviar un enlace a la portada, adjuntar versiones equivocadas o limitar permisos al remitente. También es riesgoso usar servicios personales sin control institucional. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. El expediente conserva inventario, comprobante y copia exacta de lo entregado. Esta evidencia es clave ante reclamos por respuesta incompleta. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer, decidir, ejecutar, verificar y aprender.

Síntesis de la unidad. La aplicación profesional requiere una decisión trazable: identificar información, norma y riesgo; escoger la medida menos restrictiva; verificar técnicamente; fundamentar; entregar; conservar evidencia y revisar el aprendizaje institucional.

5. Responsabilidad administrativa y sanciones

El incumplimiento puede originar multas especiales de transparencia, procedimientos disciplinarios y otras responsabilidades según la conducta y el daño.

5.1 Principio de responsabilidad

La Ley N.º 20.285 reconoce expresamente el principio de responsabilidad: el incumplimiento de las obligaciones de transparencia origina responsabilidades y da lugar a sanciones. La regla busca que los deberes no dependan sólo de buena voluntad. La autoridad, jefatura o jefe superior tiene un rol central, pero la gestión institucional también involucra funcionarios que buscan, custodian, revisan, publican y entregan información.

La responsabilidad administrativa se configura cuando un funcionario infringe deberes u obligaciones y la conducta es susceptible de una medida disciplinaria, luego de un procedimiento con garantías. Deben determinarse hechos, participación, deber infringido, culpabilidad y circunstancias. No toda equivocación produce automáticamente la sanción más grave; tampoco la orden de una jefatura justifica ejecutar una actuación manifiestamente contraria a la ley.

En transparencia y datos, una misma situación puede activar regímenes distintos. La denegación infundada tiene sanción especial; la filtración de datos puede generar disciplina interna, responsabilidad civil, infracciones de datos o incluso consecuencias penales si concurren elementos de un delito. La autoridad debe coordinar sin confundir procedimientos ni duplicar sanciones por el mismo fundamento.

5.2 Artículo 45: denegación infundada

El artículo 45 sanciona a la autoridad o jefatura o jefe superior que deniega infundadamente el acceso, contraviniendo la obligación de proporcionar información salvo oposición o causal legal. La multa corresponde al 20% al 50% de la remuneración. El elemento central es la falta de fundamento. Puede existir cuando se invoca una causal inexistente, se usa una fórmula genérica, se omite demostrar afectación o se deniega información que podía entregarse parcialmente.

Para prevenir esta infracción, la institución debe usar plantillas que obliguen a describir hechos y daño, revisión jurídica en casos complejos, matrices de decisión y capacitación. Una resolución extensa no es necesariamente fundada; debe conectar la norma con la información concreta. Copiar párrafos sin explicar el caso puede seguir siendo insuficiente.

La buena fe, la consulta interna y la existencia de un criterio razonado pueden ser relevantes en la evaluación, pero no sustituyen el cumplimiento. El órgano debe actualizar criterios conforme a decisiones del Consejo y sentencias. Repetir una práctica previamente objetada incrementa el riesgo disciplinario.

5.3 Artículo 46: incumplir una decisión firme

El artículo 46 sanciona la no entrega oportuna de información en la forma decretada una vez ordenada por resolución firme, con multa de 20% a 50% de la remuneración. Si la autoridad persiste, se aplica el duplo de la sanción y suspensión del cargo por cinco días. Aquí ya existe una decisión obligatoria, por lo que el margen de interpretación es reducido.

El cumplimiento debe ser íntegro, oportuno y en la forma indicada. Entregar archivos distintos, ilegibles, incompletos, con enlaces caídos o después del plazo puede equivaler a incumplimiento. Si surge una imposibilidad material real, debe informarse de inmediato, documentarse y gestionarse por las vías

procedentes; no corresponde guardar silencio.

Una práctica preventiva es asignar responsable, fecha límite, lista de documentos, control de calidad y comprobante. El sistema de seguimiento debe alertar antes del vencimiento y escalar a jefatura. La ejecución de decisiones del Consejo no puede quedar como tarea informal sin dueño.

5.4 Artículo 47: transparencia activa

El artículo 47 sanciona el incumplimiento injustificado de las normas de transparencia activa con multa de 20% a 50% de las remuneraciones del infractor. La transparencia activa exige mantener información permanente y actualizarla al menos mensualmente según la ley e instrucciones. No basta con tener un portal; debe estar disponible, completo, actualizado, accesible y coherente.

Los errores típicos incluyen enlaces rotos, meses ausentes, archivos ilegibles, datos desactualizados, categorías incompletas, formatos no reutilizables y publicación de datos personales innecesarios. La calidad exige tanto apertura como protección. Publicar de más puede vulnerar derechos; publicar de menos puede constituir incumplimiento.

La prevención requiere calendario, responsables por ítem, validación automática, revisión de enlaces, control de datos personales y evidencia de actualización. Las unidades de control interno tienen el deber de velar por la observancia. Una auditoría mensual breve suele ser más efectiva que corregir todo después de una fiscalización.

5.5 Procedimiento sancionatorio y medidas institucionales

Las sanciones del Título VI son aplicadas por el Consejo para la Transparencia previa investigación sumaria o sumario administrativo ajustado al Estatuto Administrativo. La Contraloría puede instruir cuando el Consejo lo solicita. Las sanciones firmes deben publicarse en los sitios del Consejo y del órgano dentro de cinco días hábiles. Esta publicidad refuerza el efecto preventivo y de rendición de cuentas.

La institución debe separar la investigación de la mejora. Aunque un sumario determine responsabilidades individuales, la organización debe corregir causas sistémicas. Un fallo repetido en anonimización puede revelar falta de herramienta, perfiles excesivos o ausencia de doble revisión. La medida disciplinaria no sustituye la gestión de riesgo.

Las buenas prácticas incluyen mapa de roles, protocolo de escalamiento, registro de criterios, capacitación anual, ejercicios de incidente, auditoría de versiones públicas, revisión de decisiones del Consejo y métricas: tiempo de respuesta, tasa de amparos, decisiones revocadas, incidentes de datos, enlaces rotos y cumplimiento de órdenes. La responsabilidad demostrable convierte aprendizaje en evidencia.

5.6 Profundización: Diferenciar error, negligencia y conducta deliberada

Los incumplimientos pueden originarse en una equivocación aislada, falta de diligencia, desconocimiento, presión, omisión reiterada o intención de ocultar. El procedimiento disciplinario debe establecer hechos y culpabilidad, no asumirlos.

Desde una perspectiva jurídica y de gestión, La responsabilidad administrativa requiere infracción de deberes y un procedimiento con garantías. Las sanciones especiales de transparencia se aplican según sus elementos, mientras otros estatutos pueden operar por deberes de custodia, probidad o obediencia reflexiva. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando

intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. La investigación reconstruye decisiones, advertencias, roles, instrucciones, capacitación, controles disponibles y acciones posteriores. Se distingue falla individual de defecto sistémico y se consideran agravantes o atenuantes conforme al régimen aplicable. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error institucional es buscar un culpable antes de preservar evidencia o sancionar a quien detectó el incidente. También es incorrecto atribuir toda responsabilidad a la jefatura si hubo manipulación deliberada de un funcionario, o al funcionario si el sistema impedía cumplir. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. Correos, bitácoras, versiones, manuales, registros de capacitación y entrevistas sustentan conclusiones. Las medidas correctivas se gestionan paralelamente sin prejuzgar. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer, decidir, ejecutar, verificar y aprender.

5.7 Profundización: Ocultamiento mediante entrega incompleta

Una respuesta puede aparentar cumplimiento y, sin embargo, omitir anexos, columnas, períodos o documentos conocidos. La entrega incompleta puede ser error o una forma de denegación material.

Desde una perspectiva jurídica y de gestión, La Ley de Transparencia exige responder la solicitud y fundamentar cualquier exclusión. Si se omite información sin explicación, el solicitante no puede impugnar adecuadamente. Cuando existe una orden firme, el cumplimiento parcial puede activar el artículo 46. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. Se compara solicitud, inventario y entrega. Toda exclusión queda identificada: inexistencia, derivación, reserva o tarjado. La jefatura aprueba casos de alto riesgo y el comprobante detalla archivos. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué

medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error es suponer que entregar “algo” evita responsabilidad, o eliminar columnas sin leyenda. También es problemático cambiar el formato de manera que dificulte análisis sin razón de costo o seguridad. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. La matriz de cobertura, control de pares y copia exacta entregada permiten demostrar integridad. Los amparos por entrega parcial deben analizarse como señal de proceso. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer, decidir, ejecutar, verificar y aprender.

5.8 Profundización: Cumplimiento de decisiones del Consejo

Una resolución firme requiere coordinación rápida entre jurídica, transparencia, unidad dueña y tecnología. Las demoras internas no suspenden el plazo.

Desde una perspectiva jurídica y de gestión, El artículo 46 sanciona no entregar oportunamente en la forma decretada y agrava la persistencia. La responsabilidad recae en la autoridad o jefatura señalada, por lo que debe existir gobernanza clara para ejecutar. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. Al recibir la decisión se registra fecha de firmeza, plazo, alcance y formato. Se asignan tareas, se prepara versión, se valida, se entrega y se informa cumplimiento. Cualquier dificultad se escala de inmediato. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error es esperar instrucciones informales, reabrir el debate jurídico sin vía procedente o entregar una versión diferente. También es riesgoso no verificar que la resolución esté firme y los terceros hayan sido considerados. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se

acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. Un registro de órdenes, alertas y responsables demuestra control. La auditoría debe revisar cumplimiento y causas de retraso. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer, decidir, ejecutar, verificar y aprender.

5.9 Profundización: Transparencia activa con protección de datos

Los portales deben actualizar información exigida, pero pueden exponer datos personales si se publican documentos originales sin versión pública. Cumplir cantidad sin revisar calidad crea otra infracción o daño.

Desde una perspectiva jurídica y de gestión, El artículo 47 sanciona incumplimiento injustificado de transparencia activa. Al mismo tiempo, la protección de datos y derechos de las personas exige minimizar y tarjar. Ambas obligaciones se integran. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. Cada ítem tiene dueño, calendario, fuente y regla de publicación. Se revisan enlaces, formato, fecha, campos y metadatos. Los cambios de personal o sistema activan una revisión de permisos y plantillas. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error es copiar archivos desde un sistema interno al portal sin saneamiento, o mantener enlaces rotos por meses. También es insuficiente publicar imágenes ilegibles cuando existe información estructurada. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. La evidencia incluye checklist mensual, capturas, reportes automáticos, revisión de datos y correcciones. La unidad de control interno utiliza indicadores y muestreo. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer, decidir, ejecutar, verificar y aprender.

Síntesis de la unidad. La aplicación profesional requiere una decisión trazable: identificar información, norma y riesgo; escoger la medida menos restrictiva; verificar técnicamente; fundamentar; entregar; conservar evidencia y revisar el aprendizaje institucional.

6. Hoja de ruta 2026 y casos aplicados

El año 2026 exige cumplir el régimen vigente y preparar la entrada en vigor de la reforma de datos sin debilitar el derecho de acceso.

6.1 Dos momentos normativos en 2026

Entre el 1 de enero y el 30 de noviembre de 2026, la gestión de datos personales se rige por la versión vigente de la Ley N.º 19.628 y por normas sectoriales. Desde el 1 de diciembre entra en vigor la reforma introducida por la Ley N.º 21.719 y comienza a operar el nuevo marco institucional. Un curso actualizado debe indicar la fecha de cada regla y evitar presentar como vigente anticipadamente una obligación diferida.

La transición no significa esperar. Los inventarios, análisis de brechas, reducción de datos, seguridad, contratos, procedimientos de derechos y gobernanza requieren meses. Los equipos de transparencia deben participar porque administran publicaciones y entregas de alto impacto. La preparación debe preservar continuidad: las solicitudes siguen tramitándose y los plazos de la Ley N.º 20.285 no se suspenden por el proyecto de adecuación.

Una matriz de transición puede clasificar tareas en cumplimiento actual, preparación obligatoria y mejora recomendada. Por ejemplo, guardar secreto de datos no públicos es obligación vigente; documentar bases, riesgos y responsables es una mejora inmediata y requisito de madurez; adecuar procedimientos a la Agencia es preparación para el nuevo régimen.

6.2 Plan de adecuación institucional

La primera fase es gobernanza: designar patrocinio, equipo multidisciplinario y responsables. La segunda es conocimiento: inventariar bancos, flujos, publicaciones, proveedores, transferencias y bases legales. La tercera es riesgo: priorizar tratamientos sensibles, masivos, biométricos, de niños, salud, beneficios, seguridad y monitoreo. La cuarta es control: ajustar accesos, contratos, retención, avisos, derechos, incidentes y anonimización.

La quinta fase es integración con transparencia. Cada ítem de transparencia activa y cada tipo frecuente de solicitud debe tener una regla de publicación y protección. Se definen campos públicos, campos a revisar y campos normalmente excluidos, sin convertir la matriz en una decisión automática. La sexta fase es prueba: ejercicios de solicitud, simulación de incidente, recuperación de texto tarjado y revisión de enlaces.

La séptima fase es evidencia. Se conservan inventarios, actas, decisiones, registros de capacitación, resultados de pruebas, planes de corrección y métricas. La responsabilidad demostrable se sostiene con documentos vivos. Un manual que nadie aplica no demuestra cumplimiento.

6.3 Caso aplicado: nómina de beneficiarios

Una municipalidad recibe una solicitud por la nómina de beneficiarios de un programa social, con nombres, RUT, domicilio, monto, diagnóstico social y cuenta bancaria. El objetivo de control del gasto es legítimo, pero la entrega íntegra causaría una afectación intensa. La unidad debe identificar la norma del programa, revisar si la identidad es públicamente exigible y preparar alternativas.

Una respuesta proporcional podría entregar criterios, número de beneficiarios, montos por comuna o tramo, ejecución presupuestaria y procedimiento de selección. Según el caso y jurisprudencia aplicable, podría entregarse identidad con datos de contexto tarjados, o reemplazarla por códigos si existe riesgo especial. El diagnóstico y cuenta bancaria deben protegerse. Si la identidad puede afectar derechos, se

evalúa el artículo 20.

La lección es que control social no equivale a exposición total. El solicitante debe poder verificar diseño, gasto y selección, mientras la institución reduce datos íntimos. La decisión se documenta campo por campo.

6.4 Caso aplicado: informe de ciberseguridad

Un servicio recibe una solicitud de un informe de pruebas de penetración. El documento incluye resumen ejecutivo, alcance, gasto, vulnerabilidades, direcciones IP, rutas, credenciales de prueba y plan de corrección. Negar todo por “seguridad” sería excesivo; entregar todo podría facilitar ataques.

El órgano debe coordinar transparencia, jurídica y seguridad. Puede entregar una versión con resumen, objetivos, proveedor, costo, metodología general, niveles de riesgo y estado de mitigación, reservando temporalmente detalles explotables. La resolución explica qué fragmentos se excluyen, qué daño producirían y por qué no basta otra medida. Cuando el riesgo desaparece, la reserva puede reevaluarse.

La lección es diferenciar rendición de cuentas de información operacional sensible. La seguridad exige precisión, no opacidad general.

6.5 Caso aplicado: expediente disciplinario

Una persona solicita un sumario terminado. El expediente contiene cargos, pruebas, declaraciones, datos de salud, domicilios, firmas y la sanción. La publicidad puede ser relevante para controlar la actuación administrativa, especialmente una vez finalizado el procedimiento, pero existen derechos de involucrados y testigos.

La unidad revisa si el procedimiento está concluido, la calidad de los participantes, el interés público y las normas especiales. Prepara una versión pública que conserva actos, fundamentos, decisiones y sanciones, mientras protege datos de contacto, salud, identidad de terceros vulnerables o antecedentes no necesarios. Si corresponde, comunica a terceros.

La lección es que el expediente no es indivisible. La versión pública debe permitir comprender hechos, razonamiento y resultado sin reproducir datos íntimos irrelevantes.

6.6 Profundización: Inventario de tratamientos y publicaciones

La adecuación comienza sabiendo qué datos existen, para qué se usan, dónde están, quién accede, con quién se comparten y qué se publica. Sin inventario, los riesgos permanecen invisibles.

Desde una perspectiva jurídica y de gestión, La reforma de datos refuerza responsabilidad y principios. La Ley de Transparencia exige conocer información para publicarla o entregarla. Un inventario común permite coordinar ambos sistemas. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. Se levantan procesos, sistemas, formularios, bases, planillas, portales, proveedores y flujos. Para cada uno se registra finalidad, base, categorías, titulares, retención, seguridad, transferencias y exposición pública. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué

medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error es hacer un inventario sólo tecnológico o copiar una lista de bases sin validar con usuarios. También es riesgoso excluir archivos compartidos, correos y tratamientos manuales. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. La evidencia debe tener dueño y fecha de actualización. Los cambios de proyecto, proveedor o norma activan revisión. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer, decidir, ejecutar, verificar y aprender.

6.7 Profundización: Matriz de brechas con prioridad de riesgo

No todas las brechas pueden corregirse al mismo tiempo. Deben priorizarse tratamientos cuyo fallo cause mayor daño: salud, menores, biometría, beneficios, seguridad, grandes volúmenes o decisiones automatizadas.

Desde una perspectiva jurídica y de gestión, La proporcionalidad y seguridad orientan recursos. La transición debe mantener cumplimiento vigente y preparar obligaciones futuras sin paralizar servicios ni plazos de acceso. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. Cada brecha se valora por impacto, probabilidad, urgencia legal, dependencia y esfuerzo. Se asigna responsable, presupuesto, fecha y evidencia de cierre. Las medidas rápidas reducen permisos, datos y exposición. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error es priorizar sólo lo visible o comprar herramientas antes de definir proceso. También es problemático declarar “cumplido” por tener política sin verificar aplicación. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos

públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. El tablero incluye semáforo, riesgo residual y prueba de eficacia. La alta dirección revisa los riesgos críticos y acepta formalmente los residuales cuando corresponde. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer, decidir, ejecutar, verificar y aprender.

6.8 Profundización: Capacitación por roles

Una charla general no prepara a todos por igual. Quien publica, quien administra bases, quien desarrolla sistemas y quien responde solicitudes enfrentan decisiones diferentes.

Desde una perspectiva jurídica y de gestión, La responsabilidad demostrable exige que las personas comprendan obligaciones relevantes. La Ley de Transparencia atribuye deberes y sanciones; la confidencialidad se sostiene con conducta cotidiana. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. Se diseñan rutas: inducción común, taller de tarjado, gestión de terceros, seguridad de envío, decisiones de reserva, incidentes y liderazgo. Se usan casos reales anonimizados y evaluación práctica. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error es medir sólo asistencia o usar ejemplos ajenos al servicio. También es insuficiente capacitar una vez antes de un cambio normativo y no reforzar después. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. La evidencia incluye objetivos, contenidos, evaluación, resultados, brechas y reentrenamiento. Los incidentes y amparos alimentan nuevos casos. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer,

decidir, ejecutar, verificar y aprender.

6.9 Profundización: Plan de primeros cien días del nuevo régimen

La entrada en vigor no es el final del proyecto. Los primeros meses revelarán solicitudes, interpretaciones, incidentes y ajustes de la nueva institucionalidad.

Desde una perspectiva jurídica y de gestión, Desde el 1 de diciembre de 2026 deben operar procedimientos compatibles con el marco reformado. La institución debe seguir respondiendo transparencia y observar instrucciones que emita la autoridad competente. La decisión no puede descansar en etiquetas aisladas: debe reconocer la finalidad del derecho de acceso, la excepcionalidad de la reserva y la obligación paralela de proteger a las personas. Cuando intervienen varias normas, se identifica cuál regula la publicidad, cuál protege el dato o secreto y cuál atribuye competencia. Esa lectura conjunta evita conclusiones simplistas y permite explicar la decisión a una persona no especialista.

El método recomendado es el siguiente. El plan define mesa de seguimiento, canal de consultas, revisión semanal de casos, métricas, escalamiento y actualización documental. Se monitorean derechos, incidentes, contratos y publicaciones de alto riesgo. Cada paso debe responder una pregunta verificable: qué información existe, quién podría verse afectado, qué daño se prevé, qué parte es separable, qué medida reduce el riesgo y qué evidencia respalda la conclusión. La matriz no reemplaza el juicio profesional, pero obliga a exteriorizarlo. Si dos unidades discrepan, la diferencia debe resolverse antes de la entrega y quedar registrada.

En la ejecución práctica, El error es cerrar el proyecto al publicar políticas o esperar que todas las respuestas estén resueltas de antemano. La implementación necesita aprendizaje controlado y capacidad de corrección. La unidad debe asignar responsables y plazos internos más breves que el plazo legal. También debe comprobar que la medida elegida funciona técnicamente. Por ejemplo, una decisión correcta de tarjar fracasa si el texto sigue recuperable; una reserva bien fundada fracasa si se omite entregar anexos públicos; una notificación a terceros fracasa si no se acredita recepción o se realiza fuera de plazo.

Los riesgos de una gestión débil son concretos. Informes de treinta, sesenta y cien días documentan volumen, tiempos, problemas y decisiones. La dirección aprueba correcciones y comunica criterios. Además del amparo o sanción, pueden existir daño a titulares, pérdida de confianza, costos de respuesta, obligación de retirar publicaciones y dificultades probatorias. La prevención más eficaz combina procedimiento, tecnología, revisión de pares y cultura. Ninguna herramienta compensa una finalidad mal definida, y ninguna capacitación compensa permisos abiertos o ausencia de trazabilidad.

Para aplicar este contenido en el puesto de trabajo, conviene realizar un ejercicio con un expediente real anonimizado. El equipo identifica campos, propone una decisión, intenta recuperar información eliminada y redacta una respuesta fundada. Después compara el resultado con la solicitud original y con la evidencia de búsqueda. Este ciclo transforma la norma en competencia observable: reconocer, decidir, ejecutar, verificar y aprender.

Síntesis de la unidad. La aplicación profesional requiere una decisión trazable: identificar información, norma y riesgo; escoger la medida menos restrictiva; verificar técnicamente; fundamentar; entregar; conservar evidencia y revisar el aprendizaje institucional.

7. Matriz de decisión rápida

La siguiente matriz no reemplaza el análisis del caso. Funciona como guía inicial para organizar campos y decidir qué información puede publicarse, qué debe excluirse en una versión pública y qué puede requerir una causal de reserva.

Tipo de antecedente	Decisión inicial	Control necesario
Acto, monto, contrato, criterio o fundamento público	Entregar o publicar	Verificar integridad, actualidad y formato utilizable.
RUT, domicilio, teléfono, correo privado o cuenta bancaria	Tarjar salvo necesidad legal específica	Eliminar contenido subyacente y metadatos.
Salud, biometría, creencias, vida sexual o información social íntima	Proteger; evaluar agregación o anonimización	Revisar sensibilidad, finalidad, norma sectorial y reidentificación.
Información que podría afectar derechos de terceros	Evaluar artículo 20	Notificar en dos días hábiles; registrar oposición y plazo.
Vulnerabilidad activa, credencial, arquitectura explotable	Reserva parcial potencial	Explicar daño específico y entregar resumen no explotable.
Documento mixto	Aplicar divisibilidad	Conservar original y producir versión pública revisada.

8. Sanciones y controles preventivos

Norma	Conducta	Sanción legal	Control preventivo
Art. 45	Denegación infundada	Multa de 20% a 50% de la remuneración	Fundamentación concreta, matriz de daño y revisión jurídica.
Art. 46	No entregar oportunamente en la forma decretada por resolución firme	Multa de 20% a 50%; persistencia: duplo y suspensión por cinco días	Registro de órdenes, responsable, alertas, inventario y comprobante.
Art. 47	Incumplimiento injustificado de transparencia activa	Multa de 20% a 50% de las remuneraciones del infractor	Calendario mensual, dueños de ítems, revisión de enlaces y datos personales.

Regla de gestión: una sanción individual no reemplaza la corrección sistémica. Cada incidente o amparo debe producir una revisión de causas, controles, responsabilidades, tecnología y capacitación.

9. Casos complementarios

9.1 Solicitudes masivas y distracción indebida

Una solicitud extensa no se deniega por su tamaño en forma automática. El órgano debe demostrar cómo su atención distraería indebidamente a funcionarios de sus labores habituales, considerando volumen, formato, organización, recursos y posibilidad de acotar. Debe dialogar con el solicitante, ofrecer entregas parciales o fases y evitar usar la causal cuando la dificultad proviene de una gestión documental deficiente. La inexistencia de sistemas no transforma la información en reservada, aunque puede ser un antecedente para analizar esfuerzo.

9.2 Correos electrónicos institucionales

Los correos pueden contener información pública cuando documentan decisiones, instrucciones, contratos o uso de recursos. También pueden incluir conversaciones privadas, datos personales, deliberaciones previas y antecedentes de terceros. La unidad debe buscar por cuentas, fechas y términos razonables, separar mensajes pertinentes y aplicar divisibilidad. No corresponde entregar buzones completos ni denegar todo por el solo hecho de tratarse de correo.

9.3 Firmas manuscritas y firma electrónica

La firma de una autoridad en un acto público cumple una función de autenticidad, pero su imagen puede facilitar fraude si se difunde sin necesidad. Debe distinguirse la identificación de quien firma, normalmente pública, de la reproducción gráfica de una firma manuscrita. En versiones públicas puede mantenerse nombre, cargo y constancia de firma electrónica, mientras se oculta la imagen cuando el riesgo lo justifica.

9.4 Niños, niñas y adolescentes

Los datos de menores requieren especial cautela por su vulnerabilidad y riesgo de estigmatización. La rendición de cuentas de programas educacionales, sanitarios o sociales suele lograrse con estadísticas, criterios, cobertura y resultados, no con nóminas nominales. La anonimización debe considerar comunas pequeñas, diagnósticos, establecimiento y edad, porque combinaciones pueden reidentificar.

9.5 Datos de funcionarios públicos

La función pública aumenta la publicidad de nombre, cargo, remuneraciones y actuaciones vinculadas al puesto, conforme a las reglas aplicables. No elimina la privacidad respecto de salud, domicilio, familia, cuentas, claves, biometría o antecedentes ajenos al desempeño. La decisión debe conectar cada dato con la necesidad de control institucional.

9.6 Proveedores y secretos comerciales

Los contratos, montos, adjudicación, cumplimiento y multas son relevantes para controlar gasto. Sin embargo, una oferta puede contener fórmulas, procesos, listas de clientes o información comercial cuya divulgación produzca afectación. Debe consultarse a terceros cuando corresponda y analizarse si la información es realmente secreta, tiene valor por ser secreta y fue objeto de medidas razonables de protección. La sola declaración del proveedor no decide.

9.7 Datos abiertos

Publicar datos abiertos aumenta reutilización, pero requiere un diseño que reduzca riesgo. Deben definirse licencia, diccionario, calidad, actualización y anonimización. La ausencia de nombre no basta. Se aplican umbrales, agrupación, reducción de precisión y pruebas de reidentificación. Si los datos cambian, debe revisarse el riesgo periódicamente.

9.8 Uso de herramientas de inteligencia artificial

Una herramienta externa puede recibir documentos con datos personales o reservados. Antes de usarla, el órgano debe evaluar proveedor, contrato, ubicación, retención, entrenamiento, seguridad y base jurídica. No se deben cargar expedientes reales en servicios no autorizados. La IA puede apoyar clasificación o detección, pero la decisión de reserva debe ser revisada por una persona responsable y quedar explicada.

9.9 Transferencia por correo y enlaces

El canal de entrega debe ser proporcional. Para archivos con datos autorizados puede requerirse enlace con expiración, autenticación o cifrado. Debe verificarse destinatario y evitar copiar direcciones innecesarias. El comprobante de entrega no debe revelar información protegida. Un error de destinatario se trata como incidente, no como simple equivocación administrativa.

9.10 Información estadística

La estadística es una vía potente de transparencia, pero los grupos pequeños pueden revelar identidades. Deben usarse umbrales, rangos, supresión complementaria y revisión de cruces. Publicar “un caso” en una comuna pequeña junto con edad y cargo puede identificar. La calidad de anonimización se evalúa antes de cada publicación y cuando aparecen nuevas fuentes externas.

10. Glosario técnico

Acceso parcial
Entrega de la parte pública de un documento, excluyendo únicamente la información protegida por una causal legal.

Agencia de Protección de Datos Personales
Organismo creado por la Ley N.º 21.719 para supervisar y proteger los derechos en materia de datos personales desde la entrada en vigor del nuevo régimen.

Amparo
Reclamación ante el Consejo para la Transparencia por denegación, ausencia de respuesta o entrega insatisfactoria.

Anonimización
Proceso que impide identificar razonablemente a una persona a partir de los datos y del contexto disponible.

Base de licitud
Fundamento jurídico que autoriza un tratamiento de datos, como ley, competencia pública o consentimiento válido cuando corresponde.

Causal de reserva
Hipótesis legal que permite denegar total o parcialmente por afectación a bienes protegidos.

Confidencialidad
Propiedad que limita el acceso y divulgación a personas, fines y condiciones autorizadas.

Consentimiento
Manifestación libre, específica e informada del titular para autorizar un tratamiento cuando la ley lo exige y resulta aplicable.

Dato personal
Información relativa a una persona natural identificada o identificable.

Dato sensible
Dato que revela aspectos íntimos o de especial riesgo, como salud, creencias, ideología, biometría o vida sexual.

Divisibilidad
Principio que obliga a entregar la información pública y excluir sólo la parte legalmente protegida.

Encargado del tratamiento
Persona o entidad que trata datos por cuenta del responsable y bajo sus instrucciones.

Finalidad
Propósito determinado que justifica la recolección, uso, comunicación y conservación de datos.

Fuente accesible al público
Registro o conjunto cuya consulta puede ser realizada legítimamente por cualquier persona bajo las condiciones legales.

Incidente de seguridad
Evento que compromete confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la información.

Información pública
Información que obra en poder del Estado o fue elaborada con presupuesto público, salvo excepción legal.

Integridad
Propiedad que asegura que la información permanece completa, exacta y no alterada sin autorización.

Interés público
Valor social de conocer información para controlar decisiones, recursos, derechos, seguridad o probidad.

Minimización
Tratamiento limitado a datos adecuados, pertinentes y necesarios para la finalidad.

Máxima divulgación
Principio de entrega en los términos más amplios posibles, excluyendo sólo lo protegido.

Oposición de tercero
Derecho del afectado a oponerse fundadamente a la entrega dentro del procedimiento del artículo 20.

Principio de responsabilidad
Regla según la cual el incumplimiento de obligaciones de transparencia genera responsabilidades y sanciones.

Responsabilidad demostrable
Capacidad de acreditar con evidencia que se cumplen principios, obligaciones y controles.

Responsable del tratamiento
Organismo o persona que decide finalidades y medios del tratamiento de datos.

Secreto o reserva
Limitación excepcional y legal a la publicidad de determinada información.

Seudonimización
Sustitución de identificadores por códigos, manteniendo separada la información que permite reidentificar.

Tarjado
Eliminación segura de fragmentos protegidos en una copia destinada a acceso público.

Test de daño
Análisis que identifica el daño probable, su gravedad y el nexo con la divulgación.

Transparencia activa
Publicación permanente y actualización periódica de información exigida por la ley.

Transparencia pasiva
Procedimiento de solicitud y respuesta para acceder a información pública.

Trazabilidad
Capacidad de reconstruir accesos, cambios, decisiones, versiones y entregas.

Versión pública
Copia preparada para acceso, con exclusiones justificadas y técnicamente irreversibles.

11. Fuentes oficiales

Las referencias se presentan para consulta y verificación del texto vigente. La jurisprudencia y normas sectoriales deben revisarse según el caso.

Constitución Política de la República de Chile, artículos 8 y 19 N.º 4
https://www.bcn.cl/leychile/navegar?idNorma=242302

Ley N.º 20.285, sobre Acceso a la Información Pública
https://www.bcn.cl/leychile/navegar?idNorma=276363

Decreto Supremo N.º 13 de 2009, Reglamento de la Ley de Transparencia
https://www.bcn.cl/leychile/navegar?idNorma=1001095

Ley N.º 19.628, sobre Protección de la Vida Privada, versión vigente hasta 30-11-2026
https://www.bcn.cl/leychile/navegar?idNorma=141599

Ley N.º 21.719, reforma de protección de datos y creación de la Agencia
https://www.bcn.cl/leychile/navegar?idNorma=1209272

Ley N.º 21.663, Ley Marco de Ciberseguridad
https://www.bcn.cl/leychile/navegar?idNorma=1202434

Ley N.º 21.459, sobre delitos informáticos
https://www.bcn.cl/leychile/navegar?idNorma=1177743

DFL N.º 29 de 2004, Estatuto Administrativo
https://www.bcn.cl/leychile/navegar?idNorma=236392

Consejo para la Transparencia: procedimientos disciplinarios y sanciones
https://www.consejotransparencia.cl/informes/procedimientos-sancionatorios-y-sanciones/

Advertencia de uso. Este material tiene finalidad educativa y no sustituye asesoría jurídica ni el análisis de antecedentes concretos. En caso de duda, consulte el texto oficial vigente, decisiones del Consejo para la Transparencia, sentencias y normas especiales.