

GUÍA DE PROTECCIÓN DE DATOS PERSONALES

Oficina de Datos

Instituto de Seguridad Laboral

Ministerio del Trabajo y Previsión Social

Marco normativo: Ley 19.628 y sus modificaciones introducidas por la
Ley 21.719, vigentes a partir del 1 de diciembre de 2026.

ÍNDICE

PRESENTACIÓN	3
1. QUÉ SON LOS DATOS PERSONALES	4
1.1 Definición básica	4
1.2 Datos sensibles: categoría especial de protección	5
2. PRINCIPIOS QUE RIGEN EL TRATAMIENTO DE DATOS	5
3. LICITUD DEL TRATAMIENTO: POR QUÉ EL ISL PUEDE TRATAR DATOS PERSONALES	6
3.1 Bases de habilitación aplicables al ISL	6
3.2 La pregunta esencial: ¿para qué se tratan estos datos?	7
4. ACCESO Y COMUNICACIÓN DE DATOS PERSONALES.....	8
4.1 Criterios para autorizar acceso.....	8
4.2 Acceso a las plataformas institucionales SPM, SGLME, u otras donde se contengan datos como en la Resolución de Calificación y la Licencia Médica	9
4.3 Comunicación de datos a terceros y otras instituciones	9
5. BUENAS PRÁCTICAS PARA PROTEGER DATOS PERSONALES EN TU ÁREA.....	11
5.1 Lista de verificación para funcionarias y funcionarios	11
5.2 Ante una solicitud de datos: qué preguntar antes de responder	11
6. LEY 19.628 Y LEY 21.719: QUÉ CAMBIA Y CUÁNDO.....	12
6.1 Cuadro comparativo de cambios relevantes	12
7. DERECHOS DE LAS PERSONAS TITULARES DE DATOS.....	13
8. SITUACIONES DE ALERTA: CUÁNDO DETENERSE Y CONSULTAR.....	15
9. GLOSARIO ESENCIAL	16
10. PREGUNTAS FRECUENTES	18
ANEXO 1 - DATOS SENSIBLES TRATADOS EN ISL.....	22

PRESENTACIÓN

Esta guía está dirigida a todas las funcionarias y funcionarios del Instituto de Seguridad Laboral (ISL), sin importar su área ni cargo. No es un manual técnico-jurídico: es una herramienta práctica para que cada persona que trabaja en el ISL comprenda qué son los datos personales, por qué debemos protegerlos y **qué puede y qué no debe hacer** en su trabajo diario.

Para facilitar su lectura, esta guía incluye en sus últimas páginas un glosario con las definiciones de los principales conceptos y siglas utilizados. Consúltalo cada vez que encuentres un término que no conozcas o necesites aclarar su significado.

El ISL administra el Seguro Social contra Riesgos de Accidentes del Trabajo y Enfermedades Profesionales establecido en la Ley 16.744. Para cumplir esta función, trata diariamente datos personales de trabajadores, empleadores, beneficiarios y otras personas relacionadas con sus procesos. Entre ellos se encuentran datos de identificación, contacto, antecedentes laborales, información previsional y datos sensibles relativos a la salud. Estos datos deben utilizarse exclusivamente para finalidades institucionales autorizadas.

Actualmente se encuentra vigente la Ley 19.628 sobre uso, almacenamiento y cuidado de datos personales. Sin embargo, la Ley 21.719 sobre protección y tratamiento de datos personales introduce modificaciones sustanciales a esta normativa, las que comenzarán a regir el **1 de diciembre de 2026**. Esta guía distingue entre las obligaciones actualmente vigentes, las nuevas exigencias legales y las buenas prácticas que el ISL puede implementar anticipadamente.

Por qué es importante implementar lo establecido en la Ley 21.719

Cada vez que accedes a una plataforma institucional, gestionas un expediente o compartes información de un trabajador, estás tomando una decisión sobre datos personales. Esta guía te entrega más herramientas para tomar esa decisión de manera informada.

1. QUÉ SON LOS DATOS PERSONALES

1.1 Definición básica

Un dato personal es cualquier información que permite identificar -o hacer identificable- a una persona natural. No se limita al nombre o al RUT: incluye todo dato que, solo o combinado con otros, apunta a una persona específica.

Tipo de dato	Ejemplos en contexto ISL
Identificadores directos	Nombre completo, RUT, correo institucional, teléfono personal
Identificadores indirectos	Cargo + dependencia + fecha de ingreso (combinados, identifican a alguien)
Datos de salud (sensibles)	Diagnósticos en DIAT/DIEP, historiales en SPM, calificaciones, incapacidades laborales y licencias médicas.
Datos laborales	Contrato, remuneración, evaluaciones ocupacionales de salud y de vigilancia.
Datos vinculados a empleadores	Datos de empleadores que sean personas naturales; representantes legales; personas de contacto; trabajadores asociados a accidentes, cotizaciones o prestaciones.
Datos biométricos	Huella digital para control de asistencia (si aplica)

Importante: la información relativa exclusivamente a una persona jurídica no constituye, por sí sola, un dato personal. Sí lo es cuando identifica o permite identificar a una persona natural vinculada con ella.

1.2 Datos sensibles: categoría especial de protección

Algunos datos merecen una protección reforzada porque su exposición puede generar discriminación grave o vulnerar la dignidad de la persona. La ley los llama datos sensibles y establece exigencias más estrictas para su tratamiento.

Son datos sensibles:

- Datos de salud y médicos (incluye diagnósticos, tratamientos, incapacidades)
- Origen racial o étnico
- Opiniones políticas y convicciones religiosas o filosóficas
- Vida sexual y orientación sexual
- Datos biométricos y datos relativos al perfil biológico humano, como los datos genéticos, proteómicos o metabólicos, conforme a las categorías reguladas por la Ley 21.719.

En el ISL, los datos de salud presentes en documentos como la Resolución de Calificación (RECA), Licencia Médica, REIP, Ficha clínica y plataforma como SPM o SGLME, SBE son siempre datos sensibles. El acceso a estos datos debe estar asociado a una función institucional, una tarea autorizada y una necesidad concreta. El acceso injustificado puede constituir un tratamiento indebido y generar responsabilidades.

[Para conocer más detalle sobre que datos sensibles existen en ISL diríjase al Anexo de Procesos y Datos Sensibles](#)

2. PRINCIPIOS QUE RIGEN EL TRATAMIENTO DE DATOS

Proteger datos personales no es solo evitar filtraciones: es tratar la información de manera que respete a la persona que está detrás de cada registro. La ley establece principios que funcionan como reglas de conducta para todos quienes tratan datos.

Principio	Qué significa en la práctica del ISL
Licitud y lealtad	Los datos personales sólo pueden tratarse de manera legal, transparente y respetuosa. Antes de utilizarlos, debe existir una función institucional o fundamento jurídico que lo permita.
Finalidad	Los datos recolectados para administrar el Seguro de la Ley 16.744 no pueden usarse para otro propósito. No puedes consultar el historial médico de un trabajador por curiosidad o para un fin ajeno a su caso.
Proporcionalidad	Solo recolectar y tratar los datos estrictamente necesarios. Si para resolver una consulta basta con el RUT, no pidas ni registres datos adicionales.

Principio	Qué significa en la práctica del ISL
Calidad	Los datos deben ser exactos y estar actualizados. Un error en un diagnóstico o en una fecha de accidente puede afectar derechos del trabajador.
Responsabilidad proactiva	No esperar a que ocurra un incidente. El ISL debe anticipar riesgos, implementar controles y capacitar a su personal. Este principio se refuerza significativamente con la Ley 21.719.
Seguridad	Adoptar medidas técnicas y organizacionales para proteger los datos de accesos no autorizados, pérdida o destrucción.
Transparencia e información	Las personas tienen derecho a saber qué datos tiene el ISL sobre ellas, con qué finalidad se tratan, quién es responsable del tratamiento y cómo pueden ejercer sus derechos.
Confidencialidad	Quienes acceden a datos personales deben mantenerlos bajo reserva y utilizarlos únicamente para cumplir sus funciones. No puedes comentar, divulgar ni compartir información de trabajadores o beneficiarios con personas que no estén autorizadas, incluso después de dejar de desempeñar esas funciones.

3. LICITUD DEL TRATAMIENTO: POR QUÉ EL ISL PUEDE TRATAR DATOS PERSONALES

Una pregunta clave antes de cualquier tratamiento de datos es: ¿tenemos autorización legal para hacer esto? A esa autorización se le llama **base de habilitación o base legal**. Sin una base válida, el tratamiento es ilícito, aunque sea técnicamente posible.

3.1 Bases de habilitación aplicables al ISL

Base de habilitación	Explicación para el ISL
Cumplimiento de funciones legales	El ISL puede tratar datos personales cuando dicho tratamiento sea necesario para el cumplimiento de las funciones que le asigna la Ley N.º 16.744 y demás normativa vigente, siempre que actúe dentro del ámbito de sus competencias.
Autorización legal específica	Determinadas normas pueden autorizar o exigir tratamientos concretos, especialmente respecto de datos sensibles o comunicaciones de información.

Base de habilitación	Explicación para el ISL
Consentimiento	Puede utilizarse cuando corresponda legalmente, pero no sustituye la habilitación legal necesaria para ejercer funciones públicas ni debe solicitarse cuando el tratamiento sea obligatorio.
Fines históricos, estadísticos, científicos o de investigación	La Ley 21.719 contempla condiciones especiales cuando estos tratamientos atienden fines de interés público y cumplen las medidas de seguridad y protección exigidas.

Regla práctica

Antes de iniciar un tratamiento nuevo, verifica: ¿qué función institucional lo justifica?, ¿se encuentra dentro de las competencias del ISL?, ¿qué norma sustenta esa función?, ¿los datos solicitados son necesarios y proporcionales? Si estas preguntas no tienen una respuesta clara, consulta a la oficina de datos antes de proceder.

3.2 La pregunta esencial: ¿para qué se tratan estos datos?

La **finalidad del tratamiento** es la piedra angular del sistema. Toda la arquitectura normativa gira en torno a ella: define qué datos son necesarios, quiénes pueden acceder y durante cuánto tiempo deben conservarse.

Ejemplo ISL

Un trabajador sufre un accidente y se genera una calificación de dicho accidente (RECA) con su diagnóstico y antecedentes médicos asociados. Esos datos pueden tratarse para gestionar la prestación médica, calcular incapacidades y coordinar la rehabilitación.

- No deben utilizarse para finalidades incompatibles con aquellas que justificaron su recopilación.
- Los resultados estadísticos que se publiquen deben adoptar medidas que impidan identificar a las personas.
- La comunicación de datos al empleador debe limitarse a la información que corresponda entregar de acuerdo con la normativa aplicable y las funciones institucionales.

4. ACCESO Y COMUNICACIÓN DE DATOS PERSONALES

El acceso a datos personales no es libre dentro de una institución. Solo deben acceder a ellos quienes lo necesiten para cumplir su función específica. Este principio se llama limitación de acceso o principio de necesidad de conocer.

4.1 Criterios para autorizar acceso

Pregunta a hacerse	Criterio de decisión
¿Sus funciones institucionales justifican el acceso al caso o a la información solicitada?	El acceso puede autorizarse cuando sea necesario para cumplir una función institucional formalmente asignada.
¿El acceso es necesario para cumplir su tarea específica?	Si puede cumplir la tarea sin ese dato, no debe acceder.
¿Hay una norma o instrucción interna que autorice ese acceso?	El acceso debe estar respaldado por una norma, una resolución que establezca los perfiles de acceso, un procedimiento, un perfil institucional formalmente definido u otra autorización expresa. Si no existe claridad sobre dicho respaldo, la solicitud debe revisarse antes de conceder el acceso.
¿El acceso queda registrado (log)?	Como medida de seguridad y control, el ISL debe procurar que los accesos a plataformas que contienen datos sensibles sean individualizados, autorizados y trazables. Si no hay registro, hay riesgo.

4.2 Acceso a las plataformas institucionales SPM, SGLME, u otras donde se contengan datos como en la Resolución de Calificación y la Licencia Médica

Estas plataformas contienen datos sensibles relativos a la salud. El acceso debe limitarse a quienes lo necesiten para cumplir una función institucional autorizada. La posibilidad técnica de consultar información no constituye, por sí sola, una autorización para acceder a ella.

Criterios para acceder a elementos como la RECA, fundamentos de calificación, REIP, antecedentes clínicos y LM en los sistemas que corresponda

El acceso debe determinarse considerando conjuntamente:

- *las funciones asignadas a la persona;*
- *el proceso, expediente o actividad institucional en que participa;*
- *el perfil de acceso formalmente autorizado;*
- *la necesidad y proporcionalidad de los datos consultados;*
- *las obligaciones de reserva y confidencialidad;*
- *la trazabilidad de las operaciones realizadas.*

No corresponde acceder cuando no existe una tarea institucional concreta que lo justifique, aunque el perfil tecnológico permita realizar la consulta.

4.3 Comunicación de datos a terceros y otras instituciones

Comunicar datos a otra persona, organismo o empresa es también tratamiento de datos. Requiere la misma base de habilitación que cualquier otro tratamiento, y en algunos casos exige formalidades adicionales.

- Solicitudes de otras instituciones públicas (Seremi de Salud, Dirección del Trabajo, COMPIN, COMERE, etc.): deben recibirse por canales institucionales que permitan verificar la identidad del organismo solicitante, su competencia, la finalidad de la solicitud, los datos requeridos y la trazabilidad de la entrega. Cuando corresponda, deberá exigirse oficio u otro acto formal. Una solicitud verbal o recibida por un canal no institucional no debe responderse sin validación previa.
- Proveedores y empresas externas que acceden a datos ISL: cuando un proveedor trate datos personales por cuenta del ISL, debe existir un contrato o instrumento formal que regule el objeto, duración y finalidad del tratamiento; los datos involucrados; las medidas de seguridad y confidencialidad; la gestión de incidentes; y la devolución, supresión o disposición de los datos al finalizar el servicio.

- Empleadores que consultan sobre sus trabajadores: solo pueden recibir la información que la ley permite comunicarles. La relación laboral no habilita acceso irrestricto a datos de salud o información clínica.

5. BUENAS PRÁCTICAS PARA PROTEGER DATOS PERSONALES EN TU ÁREA

Proteger datos personales es responsabilidad de todas y todos los funcionarios, no solo del área jurídica o de tecnología. Aquí están las acciones concretas que puedes tomar desde hoy.

5.1 Lista de verificación para funcionarias y funcionarios

Buena práctica	Por qué importa
Accedo solo a los datos que necesito	No consultes expedientes, plataformas o bases de datos si no tienes una tarea concreta que lo justifique.
No comparto claves de acceso	Las credenciales de acceso a sistemas son personales e intransferibles. Compartir las es una infracción.
Cierro sesión al alejarme de mi equipo	Un equipo desbloqueado y desatendido es una puerta abierta a acceso indebido.
No descargo, copio ni traslado datos personales fuera de los sistemas o repositorios autorizados	Salvo que sea necesario para una tarea institucional y cuente con la autorización y las medidas de seguridad correspondientes.
Reporto incidentes aunque no esté seguro	Ante cualquier sospecha de acceso indebido, pérdida, envío erróneo o filtración de datos, informa inmediatamente a tu jefatura y a la Oficina de Datos, mediante el canal institucional definido. No elimines evidencias ni intentes resolver el incidente por cuenta propia.
No uso correo personal para enviar datos de trabajo	El correo personal no tiene los estándares de seguridad del correo institucional.

5.2 Ante una solicitud de datos: qué preguntar antes de responder

1. ¿Quién solicita los datos? (identidad verificada)
2. ¿Con qué propósito específico?
3. ¿Qué competencia, función o fundamento jurídico justifica la solicitud y la entrega?
4. ¿La solicitud está formalizada (oficio, correo institucional)?
5. ¿Los datos pedidos son proporcionales a ese propósito?

6. ¿Es posible entregar menos datos, anonimizar la información o utilizar otro mecanismo que reduzca el riesgo?

Si no puedes responder estas preguntas...

No entregues los datos de inmediato. Consulta a tu jefatura o a la Oficina de Datos a través del correo **oficina_datos@isl.gob.cl**.

6. LEY 19.628 Y LEY 21.719: QUÉ CAMBIA Y CUÁNDO

Chile está en proceso de modernización de su normativa de protección de datos. La Ley 19.628, vigente desde 1999, sobre almacenamiento, uso y cuidado de datos personales, fue modificada sustancialmente por la Ley 21.719 sobre protección y tratamiento de datos personales. Estas modificaciones entrarán en vigencia el 1 de diciembre de 2026. El ISL debe prepararse desde ahora.

6.1 Cuadro comparativo de cambios relevantes

Aspecto	Ley 19.628 (vigente hoy)	Ley 21.719 (desde dic. 2026)
Autoridad de control	Sin una autoridad general especializada. El Consejo para la Transparencia posee atribuciones relacionadas con el cumplimiento de la Ley 19.628 por los órganos de la Administración del Estado, en el marco de la Ley de Transparencia.	Nueva Agencia de Protección de Datos Personales
Base habilitación pública	Función pública + ley habilitante	Tratamiento lícito para cumplir funciones legales, dentro del ámbito de las competencias del órgano público.
Responsable del tratamiento	Concepto implícito, poco desarrollado	Definición expresa con deberes claros
Consentimiento	Estándar menos riguroso	Libre, informado, específico e inequívoco
EIPD	No exigida formalmente	Obligatoria para tratamientos de alto riesgo
Notificación de brechas	Sin obligación explícita	Reporte a la Agencia sin dilaciones indebidas cuando

Aspecto	Ley 19.628 (vigente hoy)	Ley 21.719 (desde dic. 2026)
		la vulneración genere un riesgo razonable para los derechos y libertades de los titulares.
Derechos del titular	ARCO básico	Acceso, rectificación, supresión, oposición, portabilidad y bloqueo temporal, además de garantías frente a decisiones automatizadas.
Sanciones	Alcance limitado	Régimen especial de responsabilidad y sanciones aplicable a los órganos públicos, sus jefaturas superiores y los funcionarios responsables.

Nota sobre la transición

Hasta el 30 de noviembre de 2026, la Ley 19.628 seguirá vigente sin las modificaciones introducidas por la Ley 21.719. Estas comenzarán a regir el 1 de diciembre de 2026. Sin embargo, prepararse ahora para los estándares de la Ley 21.719 es una decisión estratégica: los cambios en procedimientos, contratos y sistemas toman tiempo. El ISL no debe esperar hasta el último momento.

7. DERECHOS DE LAS PERSONAS TITULARES DE DATOS

Las personas cuyos datos personales son tratados por el ISL tienen derechos que la institución debe respetar y garantizar. Cuando un trabajador, empleador o beneficiario ejerce uno de estos derechos, la respuesta institucional debe ser oportuna y fundada.

Derecho	Qué implica para el titular
Acceso	Solicitar confirmación sobre el tratamiento de sus datos y conocer qué datos mantiene el ISL, su procedencia, finalidad, destinatarios y demás información legalmente exigible.
Rectificación	Solicitar la corrección o complemento de datos inexactos, desactualizados o incompletos.

Derecho	Qué implica para el titular
Supresión	Solicitar la eliminación de datos cuando concurra alguna de las causales establecidas por la ley.
Oposición	Solicitar que no se realice un tratamiento determinado, en los casos previstos por la ley.
Bloqueo temporal (desde diciembre de 2026)	Solicitar la suspensión temporal del tratamiento mientras se resuelve una solicitud de rectificación, supresión u oposición.
Portabilidad (desde diciembre de 2026)	Solicitar una copia de determinados datos en un formato electrónico estructurado y transferible, cuando se cumplan las condiciones legales.
Garantías frente a decisiones automatizadas (desde diciembre de 2026)	Oponerse, en los casos previstos por la ley, a decisiones automatizadas que produzcan efectos jurídicos o afecten significativamente a la persona, y solicitar explicación, intervención humana y revisión.

Los derechos de supresión, oposición, bloqueo y portabilidad no son absolutos. En los organismos públicos pueden existir limitaciones cuando su ejercicio impida o entorpezca determinadas funciones legales o afecte información declarada secreta por ley.

Si una persona ejerce estos derechos

El ISL tiene plazos legales para responder. Si recibes una solicitud relacionada con estos derechos, remítela inmediatamente a la Oficina de Datos (oficina_datos@isl.gob.cl) mediante el canal institucional definido. No la ignores ni respondas sin coordinación previa.

8. SITUACIONES DE ALERTA: CUÁNDO DETENERSE Y CONSULTAR

Existen situaciones concretas en que el riesgo de tratamiento indebido es alto. Ante cualquiera de las siguientes, detente y consulta a tu jefatura o a la Oficina de Datos, de acuerdo con los canales institucionales definidos antes de actuar.

- Alguien te solicita acceso a **SPM, SGLME u otro sistema o registro con datos personales o sensibles**, sin explicar la función o finalidad que justifica dicho acceso.
- Una institución externa, como **Seremi, Dirección del Trabajo, Fiscalía o un empleador**, solicita datos de trabajadores de manera informal o sin que esté clara la competencia, finalidad o fundamento de la solicitud.
- Se proyecta un tratamiento nuevo que, por su **naturaleza, alcance, contexto, tecnología o finalidad**, podría generar un alto riesgo para los derechos de las personas, y no se ha evaluado la necesidad de realizar una **Evaluación de Impacto en Protección de Datos (EIPD)**.
- Se contrata a un proveedor que tendrá acceso a bases de datos personales sin que se hayan establecido las **condiciones, responsabilidades y cláusulas necesarias para la protección de esos datos**.
- Detectas que una persona accedió a información sensible de un caso sin que exista una función o necesidad institucional que justifique dicho acceso.
- Se te solicita enviar una lista de personas o datos a un correo externo, compartir una carpeta o utilizar otro medio, **sin un canal institucional autorizado o sin verificar la identidad, competencia y finalidad del destinatario**.
- Se te solicita compartir o utilizar **antecedentes de salud**, como diagnósticos, fichas clínicas, exámenes, tratamientos, licencias médicas, evaluaciones médicas o antecedentes de incapacidad, y no está claro que todos esos datos sean necesarios para la finalidad solicitada.
- Recibes o debes utilizar información relativa a la **situación socioeconómica, origen étnico o pueblo originario, afiliación sindical o gremial u otros datos sensibles**, y no tienes claridad sobre la necesidad de tratarlos para la función que estás realizando.

Ante la duda, no actúes: consulta.

Es mejor retrasar una acción y hacerla bien, que actuar rápido y cometer una infracción.

9. GLOSARIO ESENCIAL

Los siguientes términos aparecen frecuentemente en materia de protección de datos. Conocerlos te ayuda a entender las instrucciones internas y a comunicarte correctamente con las áreas técnicas y jurídicas.

Término	Definición
Dato personal	Cualquier información que permita identificar o hacer identificable a una persona natural.
Dato sensible	Categoría especial de datos cuyo tratamiento requiere mayor protección: salud, origen étnico, religión, orientación sexual, biometría, entre otros.
Titular	La persona natural a quien corresponden los datos.
Responsable del tratamiento	Persona natural o jurídica, pública o privada, que decide acerca de los fines y medios del tratamiento. El ISL actúa como responsable respecto de los tratamientos que realiza para cumplir sus funciones legales.
Tratamiento	Cualquier operación sobre datos personales: recolección, almacenamiento, uso, comunicación o eliminación.
Base de habilitación	Fundamento legal que autoriza el tratamiento. Sin ella, el tratamiento es ilícito.
EIPD	Evaluación de Impacto en la Protección de Datos. Análisis previo de riesgos para tratamientos que puedan producir un alto riesgo para los derechos de las personas.
CPLT	Consejo para la Transparencia. Órgano encargado de fiscalizar el cumplimiento de la Ley de Transparencia y que posee atribuciones relacionadas con el debido cumplimiento de la Ley 19.628 por parte de los órganos de la Administración del Estado.
Agencia de Protección de Datos Personales	Institución creada por la Ley 21.719 que ejercerá las funciones de regulación, fiscalización y sanción en materia de protección de datos personales desde el 1 de diciembre de 2026.
Vulneración de seguridad	Incidente que ocasiona destrucción, pérdida, alteración, filtración, comunicación o acceso no autorizado a datos personales. Desde el 1 de diciembre de 2026, deberá reportarse a la Agencia cuando genere un riesgo razonable para los derechos y libertades de las personas.
Principio de finalidad	Los datos solo pueden usarse para el propósito que justificó su recolección.

Término	Definición
Principio de proporcionalidad	Solo recolectar y tratar los datos estrictamente necesarios para el fin declarado.
Anonimización	Procedimiento mediante el cual los datos personales son modificados de forma irreversible para que la persona a la que se refieren no pueda ser identificada ni resultar identificable.
Seudonimización	Tratamiento que impide atribuir los datos a una persona sin utilizar información adicional, la cual debe conservarse por separado y estar protegida mediante medidas técnicas y organizativas.
Tercero mandatario o encargado	Persona natural o jurídica que trata datos personales por cuenta y siguiendo las instrucciones del responsable del tratamiento.
Comunicación de datos	Acción mediante la cual el responsable da a conocer datos personales a una persona distinta de su titular, sin llegar a cederlos o transferirlos.
Cesión de datos	Transferencia de datos personales desde un responsable del tratamiento a otro responsable.
Bloqueo temporal	Suspensión temporal de las operaciones de tratamiento mientras se resuelve una solicitud de rectificación, supresión u oposición, en los casos establecidos por la ley.

10. PREGUNTAS FRECUENTES

1. ¿Puedo compartir datos de un trabajador con su empleador si me lo pide?

Depende. La normativa regula qué información puede comunicarse al empleador y en qué circunstancias. Los datos relativos a la salud tienen una protección reforzada y no pueden entregarse libremente. Ante una solicitud de esta naturaleza, consulta a tu jefatura o a la Oficina de Datos antes de responder.

2. ¿Puedo revisar el expediente de un familiar, una persona conocida o un compañero de trabajo?

No. La relación familiar, personal o laboral no autoriza el acceso a un expediente. Solo puedes consultar información cuando sea necesario para cumplir una función institucional formalmente asignada. Si participas en la tramitación de un caso que involucra a una persona cercana, informa a tu jefatura para que evalúe una posible reasignación y prevenga conflictos de interés.

3. ¿Puedo compartir una planilla completa si solo me solicitan algunos antecedentes?

No necesariamente. Antes de entregar una planilla, revisa si contiene columnas, hojas ocultas, comentarios, metadatos o datos de otras personas que no sean necesarios para responder la solicitud. Comparte únicamente la información estrictamente necesaria y evalúa si es posible eliminar, ocultar o anonimizar los datos restantes.

4. ¿Qué hago si recibo más datos personales de los que necesito?

No utilices esos datos para otras finalidades ni los compartas. Informa al remitente y consulta si corresponde devolverlos, restringir su acceso o eliminarlos mediante un procedimiento autorizado. Si la recepción fue improcedente o incluye datos sensibles, informa a tu jefatura o a la Oficina de Datos.

5. ¿Puedo enviar antecedentes por WhatsApp?

Solo si se utiliza un canal institucional expresamente autorizado y se cumplen los procedimientos y medidas de seguridad definidos por el ISL. No envíes datos personales, documentos ni fotografías mediante cuentas personales de WhatsApp. Si recibes información por este medio o tienes dudas sobre el canal adecuado, consulta antes de reenviar, descargar o almacenarla.

6. ¿Puedo guardar documentos del ISL en mi computador, correo o nube personal?

No. Los datos y documentos institucionales deben almacenarse únicamente en sistemas, equipos y repositorios autorizados por el ISL. No utilices correos personales, servicios personales de almacenamiento en la nube, dispositivos USB no autorizados u otros medios externos para guardar o trasladar información institucional.

7. ¿Puedo ingresar datos personales en ChatGPT u otras herramientas de inteligencia artificial?

No ingreses datos personales, datos sensibles ni antecedentes institucionales en herramientas de inteligencia artificial que no hayan sido expresamente autorizadas por el ISL. Antes de utilizar estas plataformas para una tarea institucional, verifica las instrucciones vigentes y, ante dudas, consulta a tu jefatura o a la Oficina de Datos. La herramienta IA autorizada por el departamento de Tecnologías de la Información es Copilot Chat.

8. ¿Puedo tomar fotografías de documentos o pantallas con mi teléfono?

No utilices un teléfono personal para fotografiar expedientes, documentos o pantallas que contengan datos personales. Si una tarea requiere capturar o digitalizar información, utiliza exclusivamente los equipos, aplicaciones y procedimientos autorizados por el ISL.

9. ¿Qué debo revisar antes de enviar un correo con datos personales?

Verifica que los destinatarios y los archivos adjuntos correspondan al caso correcto. Revisa si es necesario utilizar copia o copia oculta y evita incluir datos personales en el asunto. Comparte únicamente la información necesaria y utiliza las medidas de seguridad institucionales disponibles.

10. ¿Qué hago si envío datos personales a una persona equivocada o entrego información que no correspondía?

Reporta inmediatamente la situación a tu jefatura y a la Oficina de Datos. Informa qué datos fueron enviados, a quién, por qué medio y cuándo ocurrió. No intentes ocultar el error, eliminar evidencias ni resolverlo por tu cuenta. El incidente debe gestionarse y documentarse conforme a los procedimientos institucionales.

11. ¿Puedo conversar sobre un caso en espacios comunes o durante una videollamada?

Solo cuando sea necesario para cumplir tus funciones y adoptando medidas para impedir que personas no autorizadas escuchen o vean la información. Evita comentar casos en pasillos, ascensores, cafeterías, transporte público u otros espacios compartidos. En una videollamada, verifica quiénes participan antes de mostrar documentos o compartir la pantalla.

12. ¿Qué hago si recibo un correo sospechoso con datos de personas que no corresponde que yo tenga?

No reenvíes, utilices ni elimines esos datos. Reporta inmediatamente la situación a tu jefatura y a la Oficina de Datos mediante el canal institucional definido. Conserva el mensaje y sus archivos hasta recibir instrucciones, porque pueden ser necesarios para analizar y documentar el incidente.

13. ¿Qué hago si encuentro un documento con datos personales en una impresora?

No lo dejes expuesto, no lo fotografíes, no lo copies ni revises más información de la necesaria. Retíralo de la impresora y mantenlo temporalmente en un lugar seguro. Si puedes identificar a la persona responsable sin divulgar su contenido, entrégaselo directamente; de lo contrario, informa a tu jefatura o a la Oficina de Datos. Si contiene datos sensibles o permaneció expuesto, reporta la situación para evaluar si corresponde registrarla como un incidente de seguridad.

14. ¿El ISL puede usar los datos del Seguro de la Ley 16.744 para hacer estadísticas?

Sí, cuando exista un fundamento jurídico y se adopten las medidas de calidad, seguridad y protección correspondientes. Cuando se publiquen resultados o análisis, los datos deben anonimizarse previamente para impedir la identificación de las personas.

15. ¿La nueva ley me obliga a algo?

Las modificaciones introducidas por la Ley 21.719 entrarán en vigencia el 1 de diciembre de 2026. Hasta el 30 de noviembre de 2026 continuará rigiendo la Ley 19.628 sin dichas modificaciones. Sin perjuicio de ello, el ISL debe prepararse anticipadamente y puede aplicar desde ahora las buenas prácticas descritas en esta guía.

INSTITUTO DE SEGURIDAD LABORAL

Oficina de Datos

Proteger datos personales es parte de nuestro trabajo.

Las y los trabajadores y beneficiarios del ISL nos confían su información más sensible.

Tratarla con responsabilidad es una obligación legal y un compromiso ético.

Ante consultas o situaciones no contempladas en esta guía, dirígete a la Oficina de Datos del ISL (oficina_datos@isl.gob.cl).

ANEXO 1 - DATOS SENSIBLES TRATADOS EN ISL

Macroproceso	Datos sensibles tratados
Gestión de la Atención y Contacto Ciudadano	Situación socioeconómica: ingresos, principal fuente de sustentación y dependencia económica.
Admisión y Calificación de la Denuncia	Origen étnico: pueblo originario. Salud: enfermedad o síntomas, condición de salud, ficha y antecedentes clínicos, diagnósticos o patologías, resultados de exámenes y evaluaciones psicológicas.
Gestión de Prestaciones Médicas	Salud: diagnósticos, problemas de salud o afecciones; síntomas y secuelas; ficha clínica y antecedentes médicos y ocupacionales; atenciones, tratamientos, hospitalización, medicamentos y exámenes; licencias u órdenes de reposo; salud mental y rehabilitación física o psíquica; condición médica o funcional; incapacidad temporal o permanente, grado de incapacidad, invalidez y gran invalidez; prótesis, aparatos ortopédicos y antecedentes de reeducación profesional.
Gestión de Prestaciones Económicas	Salud: grado de incapacidad o invalidez, secuelas, licencia médica u orden de reposo, afección e incapacidad laboral. En Asignación Familiar, cuando corresponda, datos sensibles de niños, niñas y adolescentes causantes: discapacidad o invalidez, diagnóstico, antecedentes médicos, resolución COMPIN y grado o porcentaje de incapacidad. Situación socioeconómica: remuneración o renta, ingresos y dependencia económica.
Gestión de Programas de Vigilancia	Salud: antecedentes médicos, evaluaciones médicas, exámenes de vigilancia, resultados, alteraciones de salud, diagnósticos o hallazgos asociados a exposición ocupacional.
Operaciones Preventivas	Salud: encuesta o declaración de salud, lesión o condición de salud, gravedad, incapacidad, fallecimiento, evaluaciones médicas, exámenes, resultados, diagnósticos o hallazgos, interconsultas y alteraciones de salud.

Gestión de la Red de Prestadores de Salud	Salud: atención médica, hospitalización, exámenes, tratamientos, medicamentos, rehabilitación y otras prestaciones de salud otorgadas.
Gestión de Recaudaciones	Salud: incapacidades temporales y permanentes, días perdidos, grado de invalidez y fallecimiento. Afiliación sindical/gremial: condición de dirigente sindical. Situación socioeconómica: remuneración o renta imponible.
Gestión del Ciclo de Vida Laboral	Salud: licencia médica, afección o condición de salud y período de reposo o incapacidad laboral. Situación socioeconómica: remuneraciones, rentas, asignaciones u otros antecedentes económicos asociados a la persona funcionaria, cuando permitan conocer su situación socioeconómica.