

CHECKLIST PARA GERENCIAS DE PERSONAS

Datos de trabajadores: 12 puntos que revisar antes de diciembre

Ley N° 21.719 de protección de datos personales. Lo que conviene tener ordenado en un área de personas antes del 1 de diciembre de 2026.

POR QUÉ ESTO LLEGA PRIMERO A PERSONAS

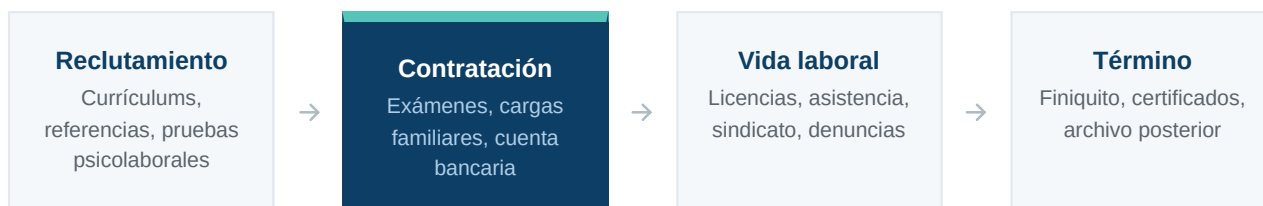
El mayor volumen de datos sensibles de tu empresa está en la carpeta de personal

Nombre, RUT, domicilio, cuenta bancaria, licencias médicas, exámenes preocupacionales, huella digital, grabaciones de cámaras, denuncias internas. Casi nada de eso está inventariado.

LA REGLA QUE CAMBIA EL PUNTO DE PARTIDA

La carga de la prueba está sobre la empresa. El artículo 13 cierra señalando que el responsable deberá acreditar la licitud del tratamiento, y el artículo 12 agrega que también le corresponde probar que contó con el consentimiento. Lo que no está documentado no es demostrable.

DÓNDE SE ACUMULAN LOS DATOS EN UN ÁREA DE PERSONAS



En cada etapa hay un proveedor externo involucrado: plataforma de reclutamiento, laboratorio, mutual, software de asistencia, empresa de remuneraciones. Todos ellos son encargados y necesitan contrato (artículo 15 bis).

DATO SENSIBLE POR DEFINICIÓN LEGAL

El artículo 2° letra g) califica como sensibles, entre otros, los datos de salud, los datos biométricos, la situación socioeconómica y la afiliación sindical o gremial. Es decir, buena parte de lo que un área de personas maneja todos los días.

Lo que hay que revisar en el ciclo de vida del trabajador

Cada punto incluye la norma que lo respalda, para que puedas llevarlo a una reunión sin tener que buscarla.

1. Inventario de datos de personas

Artículos 12 y 13

☐


Qué datos existen, en qué sistema o carpeta, con qué finalidad se recogieron, por cuánto tiempo se conservan y quién tiene acceso. Sin este mapa no se puede redactar una política de privacidad correcta ni responder a un trabajador dentro de plazo.

2. Bases de postulantes no contratados

Artículo 14 letra d)

☐


Es la brecha más frecuente y la más fácil de acreditar en una fiscalización. La ley obliga a suprimir o anonimizar los datos obtenidos para la ejecución de medidas precontractuales. Un proceso de selección cerrado sin contratación es exactamente eso. Guardar currículums por si acaso, de forma indefinida, no tiene respaldo.

3. Plazos de conservación por tipo de dato

Artículo 3° letra a)

☐


El principio de finalidad exige que los datos se traten solo mientras sirvan al fin para el que se recogieron. Conviene fijar por escrito cuánto se conserva cada categoría y qué ocurre al vencer el plazo, distinguiendo lo que obliga a guardar la legislación laboral y tributaria de lo que se guarda por costumbre.

4. Control de asistencia con huella o rostro

Artículos 16 y 16 ter

☐


La huella y los rasgos faciales son datos biométricos y la ley los trata como sensibles. Antes de seguir usándolos hay que informar al trabajador cuatro cosas concretas: qué sistema biométrico se usa, para qué exactamente, durante cuánto tiempo se usarán esos datos y cómo puede ejercer sus derechos. Conviene además documentar por qué se eligió biometría y no otro sistema de registro.

5. Cámaras en locales, faenas y bodegas

Artículos 3° letra c), 14 ter y 15 ter

☐


Exigen proporcionalidad y deber de información. Revisa qué se graba, cuánto se conserva la grabación, quién la puede ver y si el trabajador fue informado. Si además hay monitoreo sistemático de una zona de acceso público, la evaluación de impacto es previa al tratamiento y obligatoria, no un trámite posterior.

6. Datos de salud y exámenes preocupacionales

Artículos 2° letra g), 14 bis y 16

☐


Son datos sensibles con régimen reforzado. El problema habitual no es la obtención, es el almacenamiento: copias en carpetas de red compartidas, en el correo de la jefatura directa o en planillas sin control de acceso. El deber de secreto subsiste incluso después de terminada la relación laboral.

ANTES DE PASAR A LA PÁGINA SIGUIENTE

Los seis puntos anteriores dependen casi todos de decisiones internas: qué se recoge, dónde se guarda y por cuánto tiempo. No requieren presupuesto de tecnología ni esperar las instrucciones que dicte la Agencia. Los seis que siguen involucran a terceros y por eso suelen tomar más tiempo.

Proveedores, derechos e incidentes

Esta segunda mitad es la que más rápido aparece cuando un cliente corporativo audita o cuando un trabajador reclama.

7. Proveedores que acceden a datos de tu gente

Artículo 15 bis

☐

Remuneraciones, mutual, software de asistencia, plataformas de reclutamiento, beneficios, capacitación. Cada uno es un encargado que trata datos por cuenta de tu empresa. Necesita contrato que fije qué puede hacer, prohibición de subcontratar sin autorización escrita y qué ocurre con los datos al terminar el servicio.

8. Envío de datos a la casa matriz o al extranjero

Artículos 27 y 28

☐

Si el destino está fuera de Chile hay transferencia internacional, y eso incluye el servidor donde está alojado el sistema de recursos humanos. Se exige país con nivel adecuado de protección o cláusulas con garantías acreditables ante la Agencia. Revisa dónde están alojados tus sistemas antes de asumir que el tema no aplica.

9. Canal de denuncias e investigaciones internas

Artículo 14 bis y Ley N° 21.643

☐

Concentra datos de la persona denunciante y de la denunciada, muchas veces sensibles. Define quién accede al expediente, dónde se guarda, por cuánto tiempo y qué pasa con los antecedentes cuando la investigación termina. El deber de confidencialidad subsiste después de cerrado el procedimiento.

10. Procedimiento de solicitudes de trabajadores

Artículos 5° a 9° y 11

☐

Cualquier persona puede pedir acceso, rectificación, supresión, oposición o portabilidad de sus datos. El plazo de respuesta es de treinta días corridos, prorrogable una vez. Define hoy quién recibe la solicitud, quién la responde, con qué formato y dónde queda el registro de esa respuesta.

11. Protocolo ante una filtración de datos

Artículo 14 sexies

☐

La ley no da un plazo de 72 horas, contra lo que suele leerse. Exige reportar a la Agencia por los medios más expeditos posibles y sin dilaciones indebidas. Eso obliga a tener resuelto de antemano quién decide, quién comunica y qué se informa. Si la filtración afecta datos sensibles, también hay que avisar a las personas afectadas.

12. Evidencia que acredite el cumplimiento

Artículos 12, 13 y 14 quinquies

☐

Registro de consentimientos cuando corresponda, versionado de políticas, bitácora de accesos y constancia de las capacitaciones al equipo. Sin evidencia, el cumplimiento existe pero no se puede demostrar, que para estos efectos es equivalente a no existir.

SOBRE LA EVENTUAL POSTERGACIÓN

Aunque se postergue, este trabajo no cambia

A agosto de 2026 no hay norma publicada que mueva la fecha, y la vigencia sigue fijada para el 1 de diciembre de 2026. Existe una discusión abierta porque el Consejo Directivo de la Agencia todavía no se nombra. Una postergación alcanzaría a la institucionalidad y a la fiscalización, no al contenido de estas obligaciones ni a la responsabilidad civil frente a los trabajadores. Los doce puntos de este checklist se pueden cerrar hoy.

Qué hacer con lo que acabas de marcar

De 0 a 4 puntos

Es el punto de partida más habitual y no es mala noticia. Casi todo lo que falta es trabajo de orden y de contratos, no de tecnología. Parte por el inventario, porque de ahí cuelga todo lo demás.

De 5 a 9 puntos

Hay una base parcial. Lo típico en este tramo es que la práctica sea razonable pero no esté documentada. El foco debería estar en dejar por escrito lo que ya se hace y en cerrar los contratos con proveedores.

De 10 a 12 puntos

Buena posición. Lo que queda suele ser lo más específico: plazos de conservación, protocolo de incidentes y evidencia. Vale la pena una revisión externa antes de que lo audite un cliente.

PLAN REALISTA

Tres bloques de trabajo, en este orden

PRIMERO

Saber qué tienes

- ☐ Inventario de datos de trabajadores y postulantes
- ☐ Lista de proveedores con acceso y país de alojamiento
- ☐ Depuración de bases de postulantes de procesos cerrados
- ☐ Revisión de dónde se guardan los datos de salud

DESPUÉS

Ordenar lo contractual

- ☐ Cláusulas de tratamiento con cada proveedor
- ☐ Plazos de conservación definidos por escrito
- ☐ Información al trabajador sobre biometría y cámaras
- ☐ Actualización del reglamento interno

POR ÚLTIMO

Operar y demostrar

- ☐ Procedimiento de solicitudes con responsables y plazos
- ☐ Protocolo de incidentes de seguridad
- ☐ Capacitación al equipo, con registro
- ☐ Evidencia que permita acreditar el cumplimiento

Una precisión sobre el período de amonestación. Durante los primeros doce meses de vigencia, la Agencia puede aplicar una amonestación escrita en lugar de la multa a empresas calificadas como de menor tamaño según la Ley N° 20.416 (artículo sexto transitorio). Es una atenuación de la sanción administrativa, no una suspensión de las obligaciones. La amonestación queda registrada, no cubre la responsabilidad civil y no protege frente a un cliente que exija cumplimiento para contratar.

¿Revisamos cómo está tu empresa?

Ofrecemos una conversación inicial de 45 minutos, sin costo, para gerencias de personas que quieran entender qué cambia en su operación y por dónde conviene partir.

Francys Foix Fuentealba, abogada

ffox@sfabogados.cl

+56 9 8391 8969

sfabogados.cl