GA-ABOGADOS

CAMARA DE COMERCIO DE SANTIAGO

Protección de Datos Personales en el Ámbito Laboral

Seminario Protección de Datos en la Empresa

Cámara de Comercio de Santiago

Raúl Arrieta Cortés

Marco Normativo Aplicable

La protección de datos personales en Chile se rige por un marco normativo integral que combina legislación específica, regulaciones laborales y documentación interna. Comprender este ecosistema legal es fundamental para garantizar el cumplimiento normativo en el ámbito laboral.

Ley 21.719

Legislación específica sobre protección de datos personales que regula el tratamiento de información en todos los ámbitos, incluido el laboral. Establece principios rectores, derechos de los titulares y obligaciones para responsables y encargados del tratamiento.

Código del Trabajo

Los artículos 153 y siguientes establecen el marco para la regulación de las relaciones laborales, incluyendo aspectos relacionados con la privacidad del trabajador, limitaciones al poder de fiscalización del empleador y protección de la dignidad personal.

Documentación Interna

Obligación legal de incorporar en contratos individuales o reglamentos internos de trabajo las políticas de protección de datos adoptadas por la empresa, asegurando que los colaboradores conozcan sus derechos y las prácticas de tratamiento aplicables.

Contexto Legal de la Protección de Datos

La Ley 21.719 establece un marco integral que se aplica a todos los tratamientos de datos personales realizados en el contexto laboral, sin excepciones ni exclusiones para este sector. Los principios rectores definidos en esta normativa deben ser observados rigurosamente por empleadores, encargados del tratamiento y cualquier tercero que participe en el procesamiento de información personal.

Es importante destacar que la ley no solo regula las relaciones laborales ya establecidas, sino que también abarca los procesos de selección y reclutamiento de personal. Esto significa que desde el momento en que una empresa solicita información a un candidato, ya está sujeta a las obligaciones de protección de datos establecidas en la normativa vigente.

Aplicación Universal

Ley 21.719 aplica a todo tratamiento de datos en el ámbito laboral

Principios Rectores

Guían a empleadores y terceros relacionados en el procesamiento de información

Alcance Completo

Cubre relaciones actuales y procesos de selección de personal

Fases del Ciclo Laboral y Tratamiento de Datos

El tratamiento de datos personales en el ámbito laboral debe ajustarse a cada etapa del ciclo de vida del colaborador, desde la selección hasta la finalización de la relación laboral. Cada fase tiene requisitos específicos y consideraciones legales particulares que deben ser observadas.

Etapa de Contratación

Tratamiento de antecedentes laborales, académicos, referencias personales y datos de salud preocupacional. Requiere consentimiento o base de licitud claramente establecida. Obligación de suprimir datos si no se concreta la contratación, salvo que exista otra base legal para su conservación.

Evaluaciones y Desempeño

Las evaluaciones automatizadas o perfilamientos que generen efectos jurídicos significativos requieren evaluación de impacto previa. Debe existir transparencia absoluta en los criterios utilizados, permitiendo al colaborador conocer cómo se toman las decisiones que afectan su carrera profesional.

Historial del Colaborador

Tratamiento de datos en el marco del cumplimiento del contrato laboral, incluyendo asistencia, remuneraciones, capacitaciones y registros disciplinarios. Debe limitarse al tiempo estrictamente necesario y garantizar medidas de seguridad adecuadas para proteger la confidencialidad de la información.

Consentimiento en el Ámbito Laboral

El consentimiento es una de las bases legales más conocidas para el tratamiento de datos personales, pero su aplicación en el contexto laboral requiere especial cuidado debido al desequilibrio inherente en la relación empleador-trabajador. Es fundamental comprender cuándo es necesario, cuándo no es apropiado y qué alternativas existen.

¿Cuándo es necesario?

No siempre es obligatorio, pero sí es una base legal válida cuando no existe otra base legal aplicable (como obligación legal o ejecución de contrato) o cuando se tratan datos sensibles (salud, datos biométricos, afiliación sindical, etc.). El consentimiento debe ser **libre, informado, específico e inequívoco**.

Límites del consentimiento

No puede ser forzado por el desequilibrio en la relación laboral. Debe evitarse usarlo como "paraguas" para todo tipo de tratamientos sin evaluar si existe otra base más apropiada. El retiro del consentimiento debe ser tan fácil como otorgarlo, **sin consecuencias negativas para el trabajador**.

Alternativas al consentimiento

- **Ejecución del contrato laboral:** para datos necesarios para cumplir obligaciones contractuales
- **Cumplimiento de obligaciones legales:** cuando la ley exige el tratamiento de ciertos datos
- **Interés legítimo del empleador:** siempre que no prevalezcan los derechos fundamentales del trabajador

Estas bases deben evaluarse caso a caso según el tipo de datos y la finalidad perseguida, privilegiando siempre la alternativa más apropiada y menos invasiva.

Finalidad del Tratamiento de Datos

La ley exige que todo tratamiento de datos personales tenga una **finalidad clara y justificada**. En el ámbito laboral, esto significa que cada vez que se recopilan o procesan datos de los trabajadores, debe existir un propósito específico y legítimo que respalde dicha actividad.

Las finalidades deben ser **determinadas, explícitas y legítimas** desde el inicio del tratamiento. No se puede recopilar información "por si acaso" o con finalidades vagas como "mejorar la gestión". Cada tratamiento debe responder a una necesidad concreta y estar claramente comunicado al titular de los datos.

Finalidades Legítimas

Evaluación de competencias, cumplimiento de obligaciones contractuales, gestión de nóminas, control de asistencia

Finalidades Ilegítimas

Monitoreo injustificado, uso indebido de datos de salud, vigilancia excesiva sin justificación

Proporcionalidad y Minimización de Datos

El principio de proporcionalidad exige que solo se traten los datos **estrictamente necesarios** para cumplir la finalidad establecida. Esto requiere un juicio riguroso de adecuación, necesidad y pertinencia en cada caso, evaluando si los datos solicitados son realmente indispensables para el propósito declarado.

De este principio se derivan prohibiciones importantes, como la recopilación de datos "por si acaso", el almacenamiento indefinido de información personal sin justificación o la solicitud de datos que exceden lo razonable para la función desempeñada.

Principio de proporcionalidad

Solo tratar datos estrictamente necesarios para la finalidad específica

Prohibiciones derivadas

No recopilar datos "por si acaso" ni almacenar indefinidamente

Buenas prácticas

Limitar acceso a datos sensibles al mínimo indispensable de personal

Las empresas deben implementar buenas prácticas como evitar la recopilación de datos de familiares si no son estrictamente necesarios, no solicitar información sobre antecedentes no relacionados con el cargo y limitar el acceso a datos sensibles al mínimo personal indispensable.

Ejemplos Prácticos de Tratamiento de Datos

Analizar casos concretos ayuda a comprender cómo aplicar los principios de consentimiento, finalidad y proporcionalidad en situaciones reales del ámbito laboral. Esta tabla muestra ejemplos comunes y cómo evaluarlos correctamente.

Caso	¿Requiere consentimiento?	Finalidad	¿Es proporcional?
Examen preocupacional	Solo si incluye datos de salud	✅ Evaluar aptitud laboral	✅ Sí, si está acotado al cargo
Monitoreo GPS en celulares corporativos	⚠ Sí, salvo necesidad por función	⚠ Depende del caso específico	⚠ Solo con justificación clara
Recolección de datos de redes sociales	❌ No procede sin consentimiento	❌ No es finalidad legítima	❌ Desproporcionado e invasivo
Control biométrico de asistencia	⚠ Puede requerir consentimiento	✅ Control de jornada laboral	⚠ Evaluar alternativas menos invasivas

Es fundamental evaluar cada caso particular considerando el contexto específico, la naturaleza de los datos tratados, el tipo de relación laboral y las alternativas disponibles menos invasivas de la privacidad del trabajador.

Principios Clave a Cumplir

El tratamiento de datos personales en el ámbito laboral debe guiarse por principios fundamentales que garantizan el respeto a los derechos de los colaboradores y el cumplimiento normativo. Estos principios constituyen el pilar del sistema de protección de datos y deben estar presentes en cada decisión relacionada con el procesamiento de información personal.

Licitud y finalidad específica

Todo tratamiento debe tener una base legal válida y un propósito claramente definido y comunicado a los titulares de los datos. No se pueden utilizar datos para fines distintos a los declarados originalmente.

Transparencia e información

Los colaboradores deben ser informados de manera clara, comprensible y accesible sobre el tratamiento de sus datos personales, sus derechos y cómo ejercerlos.

Proporcionalidad y minimización

Solo deben tratarse los datos estrictamente necesarios para la finalidad perseguida, evitando excesos en la recopilación y conservación de información personal.

Seguridad

Implementación de medidas técnicas y organizativas adecuadas que eviten accesos no autorizados, pérdida de datos y garanticen la integridad de la información personal.

Medidas de Seguridad: Fundamento y Objetivos

Fundamento Legal

La Ley 21.719 exige que el responsable del tratamiento adopte **medidas técnicas y organizativas adecuadas** para proteger los datos personales contra accesos no autorizados, pérdida, destrucción o alteración indebida. Estas medidas deben considerar la naturaleza de los datos tratados, la finalidad del tratamiento, los riesgos identificados y el estado de la tecnología disponible.

El nivel de seguridad debe ser proporcional al riesgo: datos más sensibles requieren controles más estrictos. Las medidas no son estáticas; deben revisarse y actualizarse periódicamente para mantener su efectividad ante nuevas amenazas.

Confidencialidad

Garantizar que solo personal autorizado y debidamente capacitado accede a los datos personales

Integridad

Evitar alteraciones indebidas, pérdida o destrucción no autorizada de la información

Disponibilidad

Asegurar el acceso oportuno a los datos por quienes deban tratarlos legítimamente

Resiliencia

Mantener capacidad de recuperación rápida y efectiva ante incidentes de seguridad

Tipos de Medidas de Seguridad Recomendadas

La implementación de medidas de seguridad debe ser **integral y estratificada**, combinando aspectos organizativos y técnicos. Las medidas organizativas establecen las políticas, procedimientos y controles administrativos que guían el tratamiento seguro de los datos, mientras que las técnicas proporcionan las herramientas y mecanismos tecnológicos necesarios para proteger la información en la práctica.

Medidas Organizativas

Políticas internas documentadas, clasificación de datos según sensibilidad, programas de capacitación continua para colaboradores, control de accesos basado en roles y necesidad de conocer, procedimientos de ingreso y salida de personal

Medidas Técnicas

Encriptación de datos en tránsito y reposo, autenticación múltiple (MFA), monitoreo continuo de sistemas, antivirus y antimalware actualizados, firewalls configurados, copias de seguridad periódicas y seguras, segregación de redes

Respuesta a Incidentes

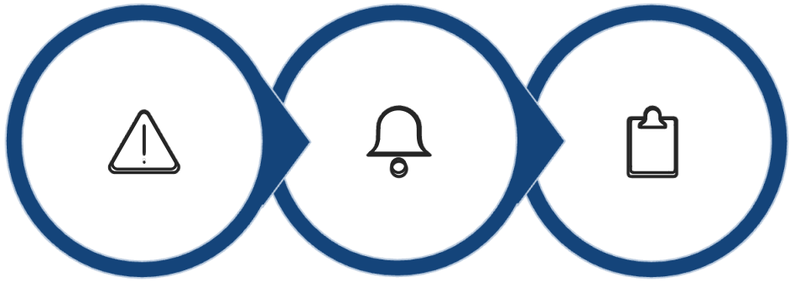
Protocolos documentados de detección temprana de amenazas, procedimientos de contención y mitigación, canales de notificación interna y externa, equipos de respuesta designados y entrenados

Auditorías y Revisión

Evaluaciones periódicas de controles de seguridad, pruebas de penetración, revisión de logs y registros de acceso, actualización continua de controles según nuevas amenazas y tecnologías

Respuesta ante Incidentes de Seguridad

Un incidente de seguridad es cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de los datos personales. Contar con un protocolo de respuesta efectivo es fundamental para minimizar el impacto y cumplir con las obligaciones legales de notificación.



Detección Notificación Registro

La respuesta debe ser rápida, coordinada y documentada. El tiempo es crítico: mientras más pronto se detecte y contenga un incidente, menor será su impacto.

Detección y Contención

Identificar rápidamente el incidente mediante sistemas de monitoreo y alertas. Tomar medidas inmediatas para limitar su impacto: aislamiento de sistemas afectados, bloqueo de accesos comprometidos, desconexión temporal de servicios vulnerables.

Notificación Oportuna

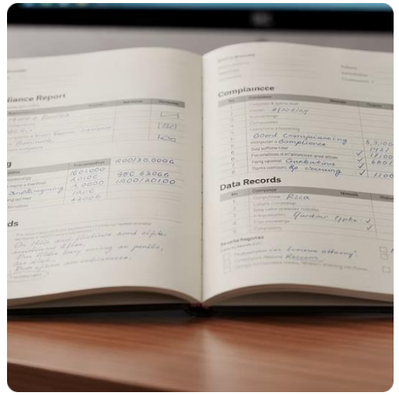
Comunicar el incidente a la Agencia de Protección de Datos cuando sea aplicable según la normativa. La notificación debe realizarse dentro de los plazos establecidos y contener información sobre naturaleza, alcance, consecuencias y medidas adoptadas.

Registro y Lecciones

Documentar detalladamente el incidente, las acciones correctivas implementadas y las lecciones aprendidas. Este registro debe conservarse por al menos 5 años como parte de las obligaciones de cumplimiento normativo.

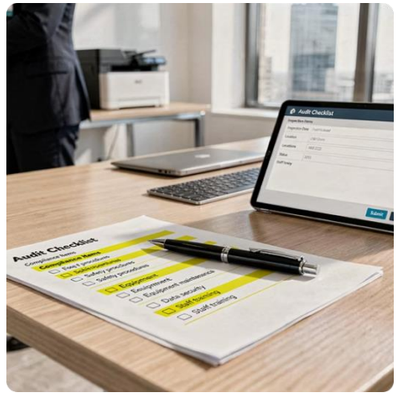
Registro de Actividades y Evaluaciones de Seguridad

La documentación adecuada y la evaluación continua son pilares fundamentales de un programa robusto de protección de datos. Estos elementos permiten demostrar cumplimiento normativo, identificar áreas de mejora y responder efectivamente ante fiscalizaciones o incidentes.



Registro de Actividades

Buena práctica para responsables y encargados que traten datos sistemáticamente. Debe reflejar las operaciones de tratamiento, finalidades, categorías de datos, destinatarios, plazos de conservación, medidas de seguridad adoptadas y los protocolos de revisión continua implementados.



Auditorías Periódicas

Se recomienda realizar evaluaciones regulares (al menos anuales) para verificar el cumplimiento de las medidas de seguridad implementadas. Estas auditorías deben adaptarse a los cambios tecnológicos, nuevas amenazas emergentes y modificaciones en los procesos internos de la organización.

Evaluación de Riesgos

Análisis sistemático de las vulnerabilidades y amenazas potenciales para los datos personales de los colaboradores. Permite implementar controles proporcionales a los riesgos identificados y priorizar inversiones en seguridad según el nivel de exposición real.

Buenas Prácticas Complementarias

Implementar buenas prácticas complementarias fortalece significativamente la protección de datos personales en el ámbito laboral. Estas medidas adicionales, aunque no siempre obligatorias, demuestran un compromiso genuino con la privacidad de los colaboradores y reducen riesgos operacionales y legales.

Cláusulas de confidencialidad en contratos

Incorporar obligaciones específicas de confidencialidad en contratos de trabajo y acuerdos con terceros

Control de acceso físico

Restringir el acceso físico a archivos, servidores y áreas donde se procesan datos sensibles

Anonimización cuando sea posible

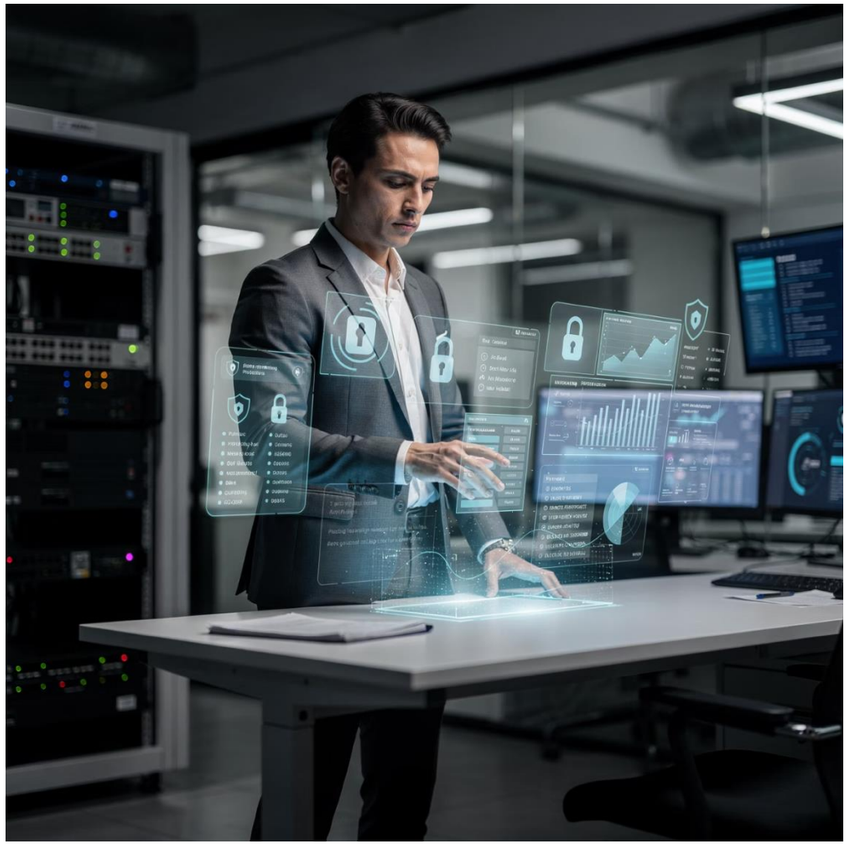
Aplicar técnicas de anonimización cuando no se requiera identificar al colaborador específico

Revisión de contratos con proveedores

Evaluar cláusulas de protección de datos en contratos con proveedores tecnológicos y de servicios

Delegado de Protección de Datos

Nombrar un DPO cuando corresponda según el volumen y naturaleza del tratamiento



Derechos ARCO: Fundamentos

Los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) constituyen el núcleo esencial de la protección de datos personales. Estos derechos están regulados detalladamente en los artículos 19 a 23 de la Ley 21.719, estableciendo garantías fundamentales para que los colaboradores puedan ejercer control efectivo sobre sus datos personales en el entorno laboral.

1

Derechos Fundamentales

Acceso, Rectificación, Cancelación y Oposición son los pilares del control individual sobre datos personales

2

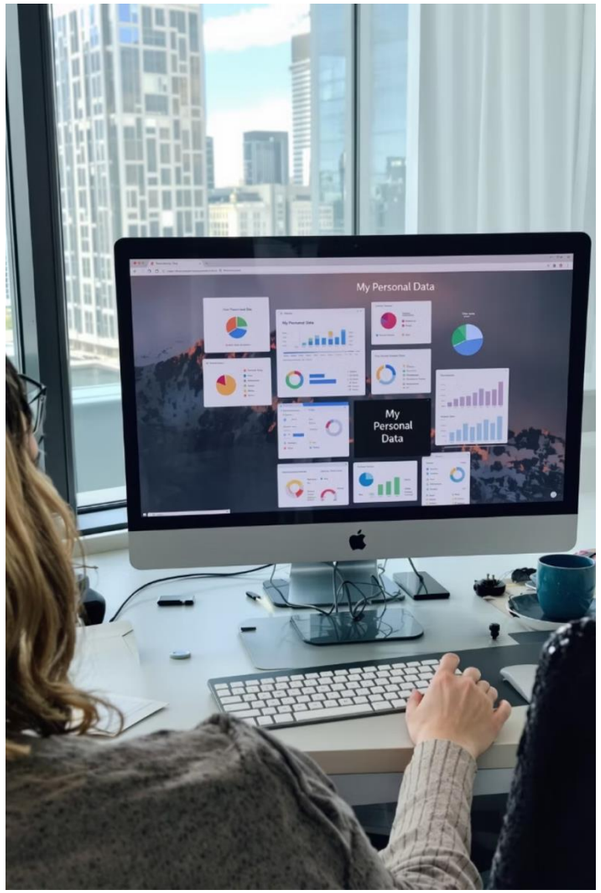
Días Hábiles

Plazo máximo legal para resolver solicitudes relacionadas con estos derechos, prorrogable excepcionalmente

3

Obligaciones Básicas

Habilitar canales, garantizar identidad del solicitante e informar claramente del procedimiento de ejercicio



El empleador tiene la responsabilidad de facilitar el ejercicio de estos derechos mediante canales accesibles, procedimientos claros y plazos razonables de respuesta. El incumplimiento puede generar sanciones administrativas y acciones legales por parte de los colaboradores afectados.

¿Qué son los Derechos ARCO?

Acceso

Derecho a saber si sus datos están siendo tratados, con qué fines, por quién y durante cuánto tiempo. Incluye la posibilidad de obtener copia gratuita de los datos personales objeto de tratamiento, en formato comprensible y estructurado.

Rectificación

Derecho a corregir datos inexactos, desactualizados o incompletos. Garantiza la calidad y precisión de la información personal almacenada por el empleador, permitiendo actualizar información que haya cambiado.

Cancelación

Derecho a solicitar la eliminación definitiva de los datos cuando ya no sean necesarios para la finalidad original, cuando se estén tratando sin justificación legal válida o cuando el titular retire su consentimiento y no exista otra base legal.

Oposición

Derecho a negarse al tratamiento cuando no exista base legal válida, cuando existan motivos legítimos relacionados con su situación particular o cuando los datos se utilicen para fines de marketing o decisiones automatizadas.

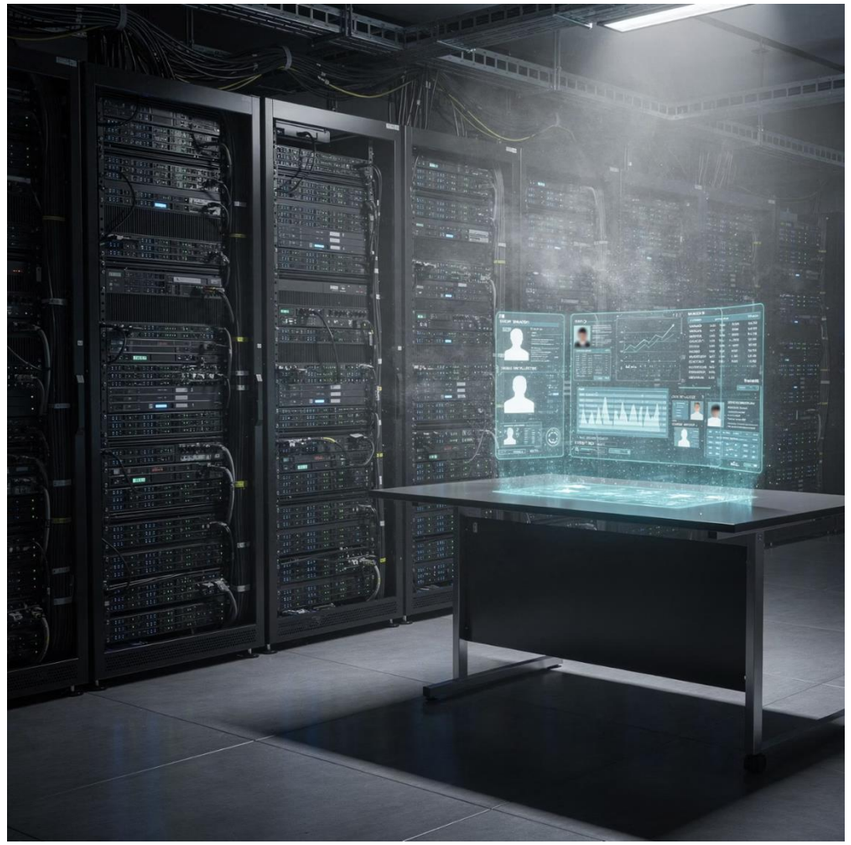
Procedimiento Interno Recomendado

Establecer un procedimiento claro y eficiente para gestionar las solicitudes de ejercicio de derechos ARCO es fundamental para el cumplimiento normativo y la satisfacción de los colaboradores. Un buen procedimiento reduce tiempos de respuesta, minimiza errores y genera confianza.

Este procedimiento debe estar documentado, comunicado internamente y revisado periódicamente para asegurar su efectividad.

1. **Recepción**
   Establecer un canal único (correo electrónico, portal interno o formulario físico) para recibir solicitudes. Confirmar recepción en un plazo máximo de 3 días hábiles y verificar la identidad del colaborador mediante mecanismos seguros para prevenir fraude o suplantación.
2. **Evaluación**
   Analizar si la solicitud es válida y completa, si se refiere a datos efectivamente tratados por la empresa, determinar si procede la rectificación o cancelación solicitada y evaluar si corresponde aplicar alguna limitación o excepción legal justificada.
3. **Respuesta**
   Emitir una resolución formal dentro del plazo legal de 30 días hábiles, prorrogable excepcionalmente por 30 días adicionales con justificación clara. Informar de manera transparente si la solicitud se acoge totalmente, se rechaza o se limita parcialmente, fundamentando adecuadamente la decisión.
4. **Registro y Seguimiento**
   Mantener un registro actualizado y completo de todas las solicitudes recibidas, las unidades que participaron en su gestión, los plazos de respuesta y las decisiones adoptadas. Reportar periódicamente al Delegado de Protección de Datos cuando corresponda.

Casos Especiales en el Ejercicio de Derechos ARCO



Algunas situaciones requieren consideraciones especiales al procesar solicitudes de derechos ARCO. Es fundamental comprender estas particularidades para gestionar adecuadamente casos complejos sin incumplir la normativa.

Datos Sensibles

La información sobre salud, afiliación sindical u otros datos sensibles debe tratarse con estricta confidencialidad. Al recibir solicitudes relacionadas con estos datos, es necesario evaluar cuidadosamente el impacto que su rectificación o cancelación podría tener en las obligaciones legales o laborales existentes.

Término del Contrato

La cancelación de datos tras la finalización de la relación laboral procede únicamente cuando no existe una obligación legal de conservación, como podría ser el caso de información necesaria para causas judiciales en curso, cumplimiento de obligaciones tributarias o laborales pendientes.

Anonimización

Cuando no sea posible eliminar completamente los datos personales debido a obligaciones legales de conservación, se recomienda implementar técnicas de anonimización o seudonimización que impidan la identificación directa del titular, manteniendo solo la información estadística o agregada necesaria.

Indicadores de Gestión y Recomendaciones

Medir y monitorear la gestión de derechos ARCO permite identificar áreas de mejora, demostrar cumplimiento y optimizar procesos internos. Los indicadores también son útiles para reportar a la alta dirección y tomar decisiones informadas sobre recursos y capacitación.

Indicadores de Gestión Interna

- **Porcentaje de solicitudes respondidas dentro del plazo legal:** objetivo mínimo 95%
- **Tiempo promedio de respuesta a solicitudes ARCO:** benchmark recomendado: 15-20 días hábiles
- **Número de solicitudes clasificadas por tipo:** acceso, rectificación, cancelación u oposición
- **Tasa de solicitudes acogidas vs. rechazadas:** para identificar patrones y problemas recurrentes
- **Incidentes relacionados con la gestión de derechos ARCO:** quejas, reclamos o escalamientos
- **Capacitación del personal:** porcentaje de colaboradores clave capacitados anualmente

Recomendaciones Clave

- Capacitar periódicamente a RRHH y personal administrativo sobre los derechos ARCO y su correcta gestión
- Integrar el procedimiento de derechos ARCO a las políticas de privacidad laboral y manuales internos
- Documentar exhaustivamente todas las solicitudes recibidas y las respuestas emitidas
- Revisar y actualizar periódicamente el procedimiento interno según lecciones aprendidas
- Establecer canales claros, accesibles y bien publicitados para facilitar el ejercicio de derechos
- Designar un responsable interno para coordinar y supervisar la gestión de solicitudes

Subcontratación del Tratamiento: Fundamentos

La Ley 21.719 permite la subcontratación del tratamiento de datos personales, pero establece un marco estricto de obligaciones para garantizar que esta delegación no disminuya el nivel de protección de los datos de los colaboradores. El responsable del tratamiento mantiene la responsabilidad final ante los titulares y las autoridades.

Contrato por Escrito

Obligación legal de formalizar la relación con el encargado mediante un contrato escrito que establezca claramente las condiciones, alcance, finalidades, plazos y medidas de seguridad del tratamiento.

Finalidades Limitadas

El encargado solo puede tratar los datos para las finalidades específicamente establecidas en el contrato, sin desviaciones ni usos adicionales no autorizados expresamente.

Seguridad Equivalente

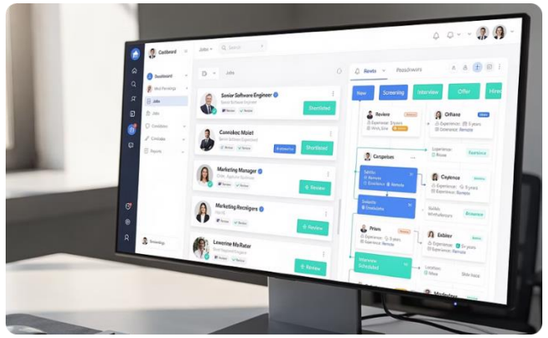
Obligación de implementar medidas de seguridad técnicas y organizativas equivalentes o superiores a las que mantendría el responsable del tratamiento.

Prohibición de Uso Propio

Los datos no pueden utilizarse para fines propios del encargado ni cederlos a terceros sin autorización expresa y documentada del responsable.

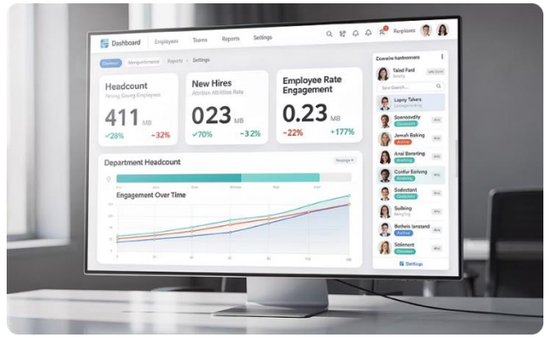
¿Qué es la Subcontratación del Tratamiento?

La subcontratación del tratamiento ocurre cuando una empresa (responsable) delega total o parcialmente el procesamiento de datos personales de sus colaboradores a un tercero (encargado). Este tercero actúa bajo las instrucciones y por cuenta del responsable, sin tomar decisiones autónomas sobre los fines y medios del tratamiento.



Plataformas de Reclutamiento

Servicios externos que gestionan bases de datos de candidatos, procesan currículums y facilitan los procesos de selección. Estas plataformas actúan como encargados del tratamiento al procesar información personal de potenciales colaboradores por cuenta de la empresa contratante.



Software de Gestión de Personal

Soluciones de RRHH en la nube que almacenan y procesan datos de los empleados, como información personal, registros de asistencia, evaluaciones de desempeño, gestión de vacaciones y otros aspectos relacionados con la administración del talento humano.

Servicios de Remuneraciones

Proveedores externos especializados que procesan datos financieros y personales de los colaboradores para la gestión de nóminas, cálculo de impuestos y retenciones, administración de beneficios y otras obligaciones relacionadas con la compensación laboral.

Riesgos Asociados a la Subcontratación

Principales Riesgos Identificados

- **Acceso indebido a bases de datos sensibles** por personal no autorizado del proveedor o terceros
- **Uso de información para fines no autorizados** como marketing propio, estudios o cesión a otros clientes
- **Filtraciones por fallas técnicas** como vulnerabilidades en sistemas, configuraciones incorrectas o ataques cibernéticos
- **Falta de cláusulas adecuadas en contratos** que dejen vacíos sobre responsabilidades, plazos o medidas de seguridad
- **Subcontratación en cadena no autorizada** donde el encargado delega a su vez a otros proveedores sin conocimiento del responsable
- **Transferencia internacional de datos** a países sin protección adecuada y sin las salvaguardas requeridas
- **Retención indebida de datos** tras la finalización del contrato o incumplimiento en la devolución/destrucción

Estos riesgos deben ser evaluados y gestionados adecuadamente mediante controles contractuales, técnicos y organizativos específicos que protejan los datos de los colaboradores sin comprometer su confidencialidad o integridad.

Evaluación de Riesgos en la Subcontratación

Antes de contratar a un encargado del tratamiento, es fundamental realizar una evaluación exhaustiva de sus capacidades, políticas y controles de seguridad. Esta debida diligencia previa reduce significativamente los riesgos y permite seleccionar proveedores confiables.

Seguridad Técnica y Organizativa

Evaluar si el proveedor cumple con estándares adecuados de cifrado, backup y control de accesos. Verificar su historial de incidentes de seguridad y las certificaciones que posee en materia de protección de datos (ISO 27001, SOC 2, etc.).

Contrato de Encargo

Revisar que el contrato contenga todos los elementos mínimos exigidos por la ley: finalidad, duración, tipos de datos, medidas de seguridad, procedimientos ante incidentes y regulación del uso de subencargados.

Cumplimiento Normativo

Comprobar el conocimiento y aplicación de la Ley 21.719 por parte del proveedor. Verificar si cuenta con procedimientos documentados para facilitar el ejercicio de los derechos ARCO por parte de los titulares de los datos.

Auditorías y Supervisión

Confirmar la existencia de cláusulas que permitan la fiscalización o el derecho a auditar al proveedor. Establecer mecanismos para la revisión periódica de sus protocolos y controles de seguridad.

Auditoría y Supervisión: Fundamentos

La Ley 21.719 exige al responsable del tratamiento cumplir con el **principio de responsabilidad proactiva**, lo que significa implementar medidas eficaces para garantizar y demostrar el cumplimiento normativo de manera continua. Esto incluye la realización de auditorías periódicas como parte esencial del modelo de cumplimiento.

Ámbitos de Supervisión

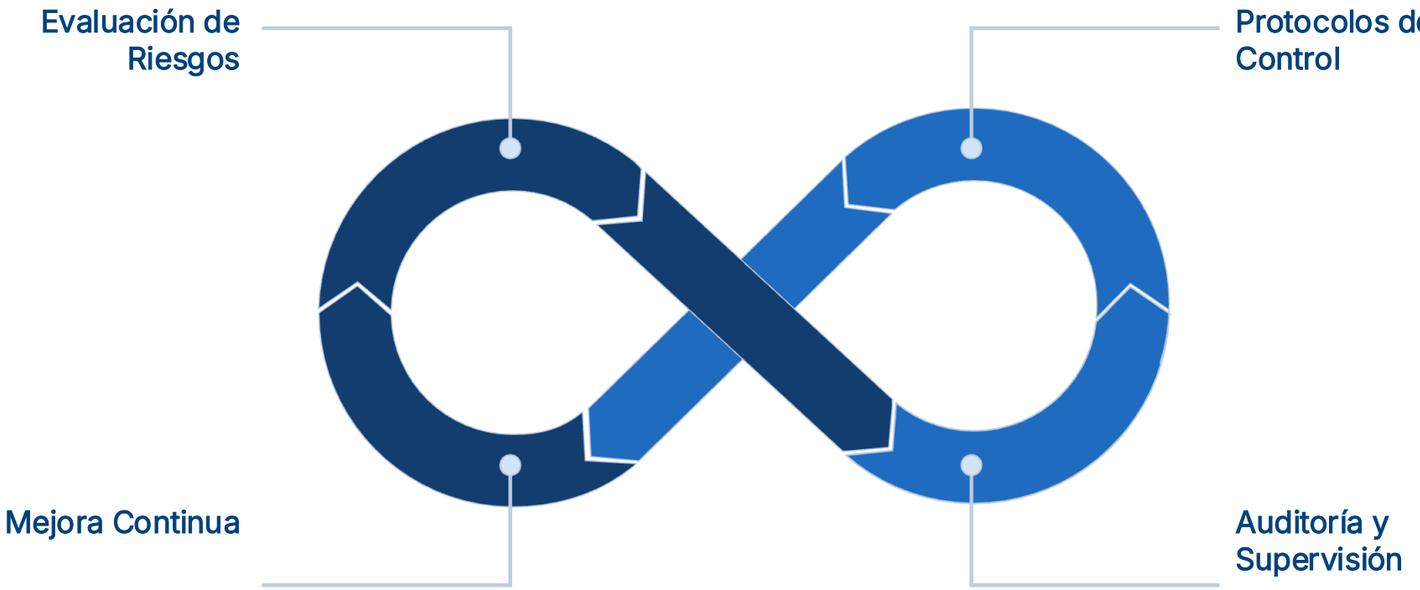
La supervisión debe abarcar aspectos clave como la validez de la base legal del tratamiento, la adecuación de las políticas internas, la efectividad de las medidas de seguridad implementadas, la correcta gestión de derechos ARCO, la relación con encargados del tratamiento y la realización de evaluaciones de impacto cuando corresponda.

Objetivos de la Auditoría

- Identificar brechas de cumplimiento normativo antes de que generen problemas
- Prevenir sanciones administrativas, judiciales o reputacionales
- Detectar malas prácticas internas o de terceros contratados
- Generar evidencia documental sólida ante posibles fiscalizaciones
- Mejorar continuamente los procesos de protección de datos

Modelo de Prevención y Mejora Continua

Toda organización debe implementar un **modelo integral de prevención de infracciones** en materia de protección de datos personales. Este modelo debe partir de un diagnóstico completo y una evaluación de riesgos que permita identificar las áreas más vulnerables y los tratamientos de mayor impacto potencial.



Sobre esta base, se deben establecer protocolos internos de control y auditoría claramente documentados, así como mecanismos efectivos para prevenir, detectar y corregir posibles incumplimientos de manera oportuna. El sistema debe estar en constante evolución, adaptándose proactivamente a los cambios normativos, tecnológicos y organizacionales.

Evaluación de Riesgos

Identificación sistemática de vulnerabilidades, amenazas y puntos críticos en el tratamiento de datos personales

Protocolos de Control

Mecanismos documentados para prevenir y detectar incumplimientos antes de que se materialicen

Auditoría y Supervisión

Verificación sistemática y periódica del cumplimiento efectivo de políticas y controles implementados

Mejora Continua

Actualización y perfeccionamiento constante basado en resultados de auditorías y lecciones aprendidas

GA-ABOGADOS

CAMARA DE COMERCIO DE SANTIAGO

Descarga nuestra Guía Práctica para adecuarse a la Nueva Normativa de Protección de Datos

Guía Práctica y Contacto

Para profundizar en la implementación de programas de cumplimiento en protección de datos, evaluaciones de impacto, diseño de políticas internas o asesoría en gobernanza de datos personales, le invitamos a:

Descargar Nuestra Guía Práctica

Escanee el código QR en la imagen de la izquierda para obtener acceso inmediato a nuestra Guía Práctica para adecuarse a la Nueva Normativa de Protección de Datos.

Contactanos en

contacto@ga-abogados.cl

+56 2 2638 1527

www.ga-abogados.cl

La protección de datos personales es un compromiso con la dignidad, la privacidad y los derechos fundamentales de las personas en la era digital, que debe coexistir con la necesidad de que las empresas traten datos personales de manera lícita, responsable y segura para desarrollar sus actividades, innovar y generar valor.