GA ABOGADOS

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

Ley 21.719

Legislación específica sobre protección de datos personales que regula el tratamiento de información en todos los ámbitos, incluido el laboral.

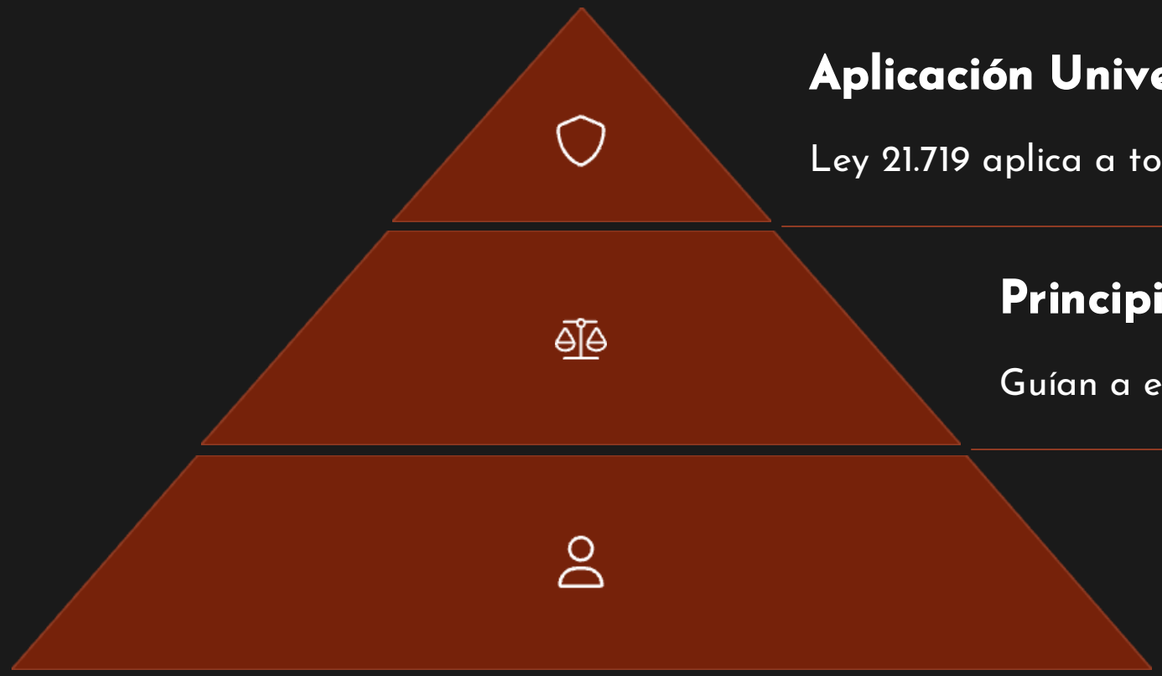
Código del Trabajo

Artículos 153 y siguientes establecen el marco para la regulación de las relaciones laborales, incluyendo aspectos relacionados con la privacidad.

Documentación Interna

Obligación de incorporar en contratos o reglamentos internos las políticas de protección de datos adoptadas por la empresa.

Contexto Legal de la Protección de Datos



Aplicación Universal

Ley 21.719 aplica a todo tratamiento de datos

Principios Rectores

Guían a empleadores y terceros relacionados

Alcance Completo

Cubre relaciones actuales y procesos de selección

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

Es importante destacar que la ley no excluye al sector laboral de su ámbito de aplicación, abarcando tanto las relaciones laborales ya establecidas como los procesos de selección y reclutamiento.

GA·ABOGADOS

Fases del Ciclo Laboral y Tratamiento de Datos

Etapa de Contratación

Tratamiento de antecedentes laborales, académicos, referencias y datos de salud. Requiere consentimiento o base de licitud. Obligación de suprimir datos si no se concreta la contratación.

Evaluaciones y Desempeño

Las evaluaciones automatizadas o perfilamientos requieren evaluación de impacto si generan efectos jurídicos significativos. Debe existir transparencia en los criterios utilizados.

Historial del Colaborador

Tratamiento de datos en el marco del cumplimiento del contrato laboral. Debe limitarse al tiempo necesario y garantizar medidas de seguridad adecuadas.

GA·ABOGADOS

Consentimiento en el Ámbito Laboral

¿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, etc.).

El consentimiento debe ser libre, informado, específico e inequívoco.

Límites del consentimiento

No puede ser forzado por desequilibrio en la relación laboral. Debe evitarse usarlo como "paraguas" para todo tipo de tratamientos.

El retiro del consentimiento debe ser tan fácil como otorgarlo, sin consecuencias negativas para el trabajador.

Alternativas al consentimiento

Ejecución del contrato laboral, cumplimiento de obligaciones legales, interés legítimo del empleador (siempre que no prevalezcan los derechos del trabajador).

Estas bases deben evaluarse caso a caso según el tipo de datos y finalidad.

GA·ABOGADOS

Finalidad del Tratamiento de Datos

Exigencias Legales

Fines determinados, explícitos y legítimos

Compatibilidad

Prohibido uso posterior para fines incompatibles

Finalidades Legítimas

Evaluación de competencias, obligaciones contractuales

Finalidades Ilegítimas

Monitoreo injustificado, uso indebido de datos de salud

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.

Proporcionalidad y Minimización de Datos

Principio de proporcionalidad

Solo tratar datos estrictamente necesarios

Prohibiciones derivadas

No recopilar datos "por si acaso"

Buenas prácticas

Limitar acceso a datos sensibles

El principio de proporcionalidad exige que solo se traten los datos estrictamente necesarios para cumplir la finalidad establecida. Esto requiere un juicio de adecuación, necesidad y pertinencia en cada caso.

De este principio se derivan prohibiciones importantes, como la recopilación de datos "por si acaso" o el almacenamiento indefinido de información personal. Las empresas deben implementar buenas prácticas como evitar la recopilación de datos de familiares si no son estrictamente necesarios y limitar el acceso a datos sensibles al mínimo indispensable.

Ejemplos Prácticos de Tratamiento de Datos

Situación	¿Consentimiento?	¿Finalidad válida?	¿Proporcionalidad?
Examen preocupacional	Solo si incluye datos de salud	✅ Evaluar aptitud laboral	✅ Sí, si está acotado
Monitoreo GPS en celulares	⚠️ Sí, salvo necesidad por función	Depende del caso	⚠️ Solo con justificación
Recolección de redes sociales	❌ No procede sin consentimiento	❌ No es finalidad legítima	❌ Desproporcionado

Esta tabla muestra ejemplos concretos de situaciones comunes en el ámbito laboral y cómo aplicar los principios de consentimiento, finalidad y proporcionalidad. Es fundamental evaluar cada caso particular considerando el contexto específico y la naturaleza de los datos tratados.

Principios Clave a Cumplir

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.

Transparencia e información

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

Proporcionalidad y minimización

Solo deben tratarse los datos estrictamente necesarios para la finalidad perseguida, evitando excesos en la recopilación.

Seguridad

Implementación de medidas técnicas y organizativas que eviten accesos no autorizados y garanticen la integridad de los datos.

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. Estas medidas deben considerar la naturaleza de los datos, la finalidad del tratamiento y los riesgos para los derechos del titular.

Objetivos de Seguridad

- Confidencialidad: garantizar que solo personal autorizado accede a los datos
- Integridad: evitar alteraciones indebidas de la información
- Disponibilidad: asegurar el acceso oportuno por quienes deban tratarlos
- Resiliencia: mantener capacidad de recuperación ante incidentes

Tipos de Medidas de Seguridad Recomendadas

Organizativas

Políticas internas, clasificación de datos, capacitaciones, control de accesos

Técnicas

Encriptación, autenticación múltiple, monitoreo, antivirus, copias de seguridad

Respuesta a Incidentes

Protocolos de detección, contención y notificación

Auditorías

Evaluaciones periódicas y actualización de controles

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

Respuesta ante Incidentes de Seguridad

Detección y Contención

Identificar rápidamente el incidente y tomar medidas inmediatas para limitar su impacto. Esto puede incluir el aislamiento de sistemas afectados, bloqueo de accesos comprometidos o desconexión temporal de servicios vulnerables.

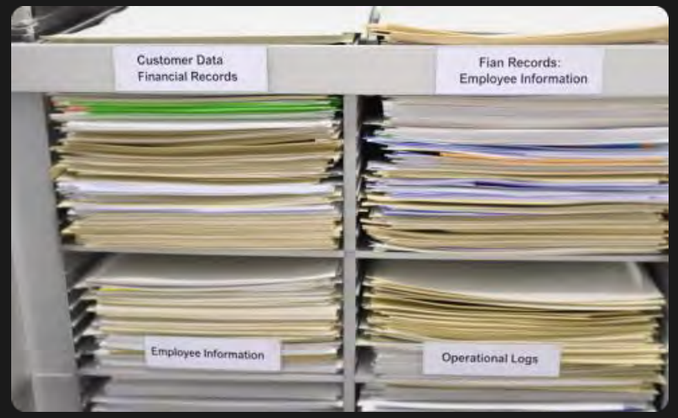
Notificación

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 la información requerida sobre la naturaleza y alcance del incidente.

Registro y Seguimiento

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

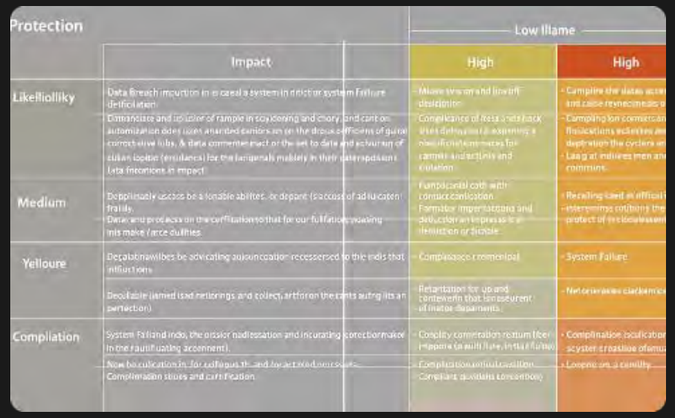


Registro de Actividades

Buena práctica para responsables y encargados que traten datos sistemáticamente. Debe reflejar las medidas de seguridad adoptadas y los protocolos de revisión continua.

Auditorías Periódicas

Se recomienda realizar evaluaciones regulares para verificar el cumplimiento de las medidas de seguridad implementadas. Estas auditorías deben adaptarse a los cambios tecnológicos, nuevas amenazas y modificaciones en los procesos internos.



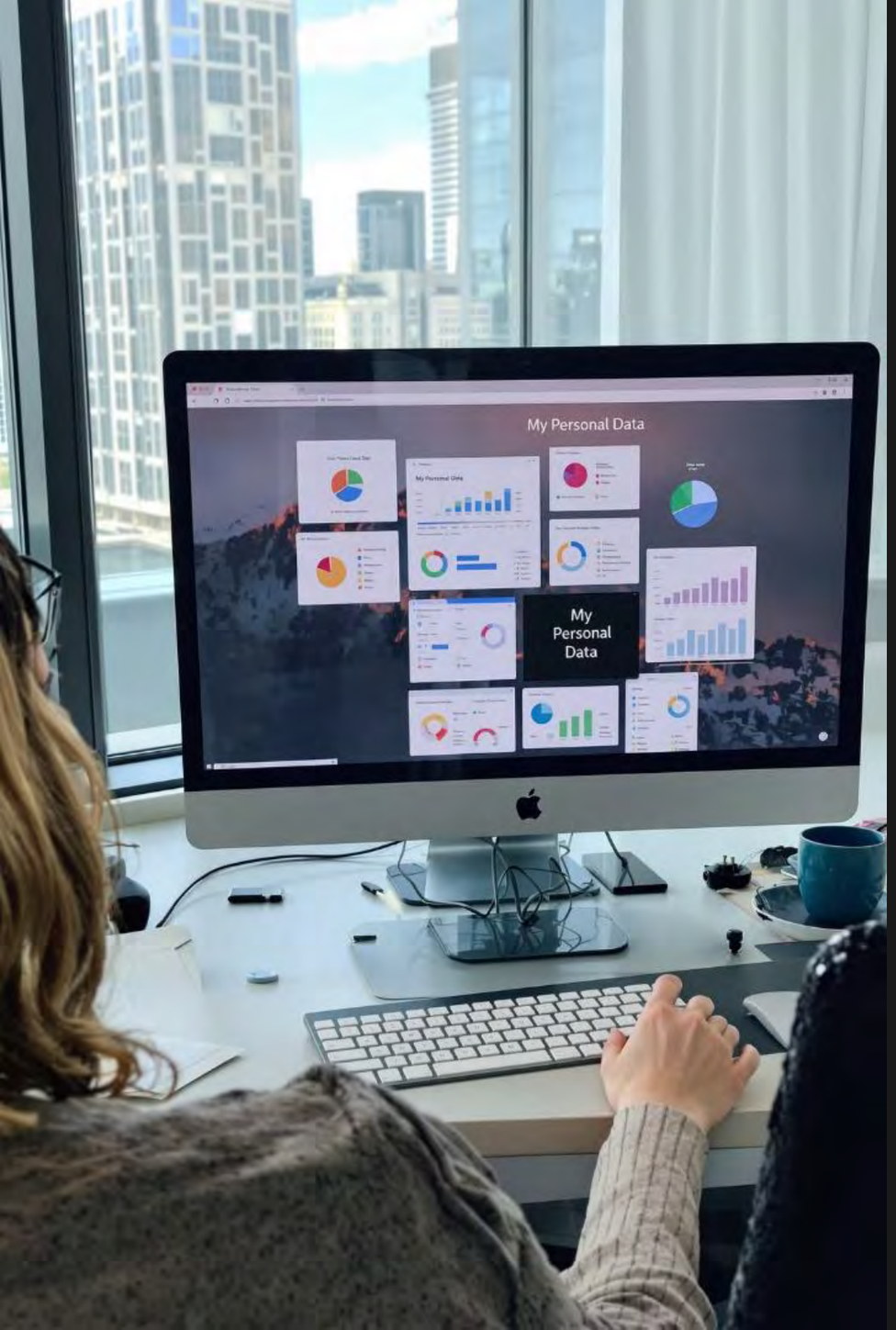
Evaluación de Riesgos

Análisis sistemático de las vulnerabilidades y amenazas potenciales para los datos personales de los colaboradores, con el fin de implementar controles proporcionales a los riesgos identificados.

Buenas Prácticas Complementarias

Implementar buenas prácticas complementarias fortalece la protección de datos personales en el ámbito laboral. Estas incluyen la redacción de cláusulas de confidencialidad en contratos de trabajo, el control del acceso físico a archivos o servidores, la anonimización de datos cuando no se requiera identificar al colaborador y la revisión de contratos con proveedores tecnológicos.

Estas medidas, junto con el nombramiento de un Delegado de Protección de Datos cuando corresponda, contribuyen a crear un sistema integral de gestión de la privacidad en la organización.



GA ABOGADOS

Derechos ARCO: Fundamentos

4

Derechos Fundamentales

Los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) constituyen el núcleo de la protección de datos personales.

30

Días Hábiles

Plazo máximo legal para resolver solicitudes relacionadas con estos derechos.

3

Obligaciones Básicas

El empleador debe habilitar canales de recepción, garantizar la identidad del solicitante e informar claramente del procedimiento.

Los derechos ARCO están regulados detalladamente en los artículos 19 a 23 de la Ley 21.719, estableciendo garantías esenciales para que los colaboradores puedan ejercer control sobre sus datos personales en el entorno laboral.

¿Qué son los Derechos ARCO?

Acceso

Derecho a saber si sus datos están siendo tratados, con qué fines y por quién. Incluye la posibilidad de obtener copia de los datos personales objeto de tratamiento.

Rectificación

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

Cancelación

Derecho a solicitar la eliminación de los datos cuando ya no sean necesarios para la finalidad original o cuando se estén tratando sin justificación legal válida.

Oposición

Derecho a negarse al tratamiento cuando no exista base legal válida o cuando existan motivos legítimos relacionados con su situación particular.

GA·ABOGADOS

Procedimiento Interno Recomendado

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.

Evaluación

Analizar si la solicitud es válida y completa, si se refiere a datos efectivamente tratados por la empresa y determinar si procede la rectificación, cancelación o si corresponde aplicar alguna limitación legal.

Respuesta

Emitir una resolución formal dentro del plazo legal de 30 días hábiles, prorrogable por 30 días adicionales con justificación. Informar claramente si la solicitud se acoge, rechaza o se limita parcialmente, fundamentando la decisión.

Registro y Seguimiento

Mantener un registro actualizado de todas las solicitudes recibidas, identificando las unidades que participaron en su gestión y reportando periódicamente al Delegado de Protección de Datos, cuando corresponda.

Casos Especiales en el Ejercicio de Derechos ARCO

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 o cumplimiento de obligaciones tributarias.

Anonimización

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

Indicadores de Gestión y Recomendaciones

Indicadores de Gestión Interna

- Porcentaje de solicitudes respondidas dentro del plazo legal
- Tiempo promedio de respuesta a solicitudes ARCO
- Número de solicitudes clasificadas por tipo (acceso, rectificación, etc.)
- Incidentes relacionados con la gestión de derechos ARCO

Recomendaciones Clave

- Capacitar a RRHH y personal administrativo sobre los derechos ARCO
- Integrar el procedimiento a las políticas de privacidad laboral
- Documentar todas las solicitudes y respuestas emitidas
- Revisar y actualizar periódicamente el procedimiento interno
- Establecer canales claros y accesibles para el ejercicio de derechos

GA·ABOGADOS

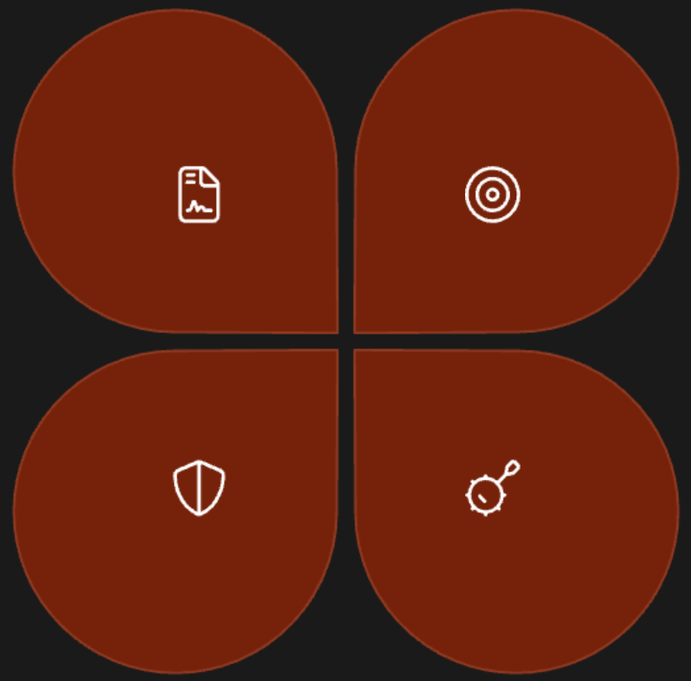
Subcontratación del Tratamiento: Fundamentos

Contrato por Escrito

Obligación legal de formalizar la relación con el encargado mediante un contrato escrito que establezca claramente las condiciones del tratamiento.

Seguridad Equivalente

Obligación de implementar medidas de seguridad equivalentes a las que mantendría el responsable del tratamiento.



Finalidades Limitadas

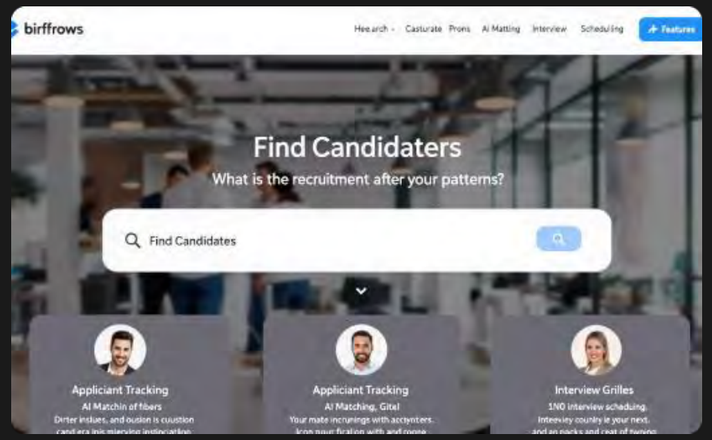
El encargado solo puede tratar los datos para las finalidades específicamente establecidas en el contrato, sin desviaciones.

Prohibición de Uso Propio

No pueden utilizarse los datos para fines propios ni cederlos a terceros sin autorización expresa del responsable.

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.

¿Qué es la Subcontratación 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.

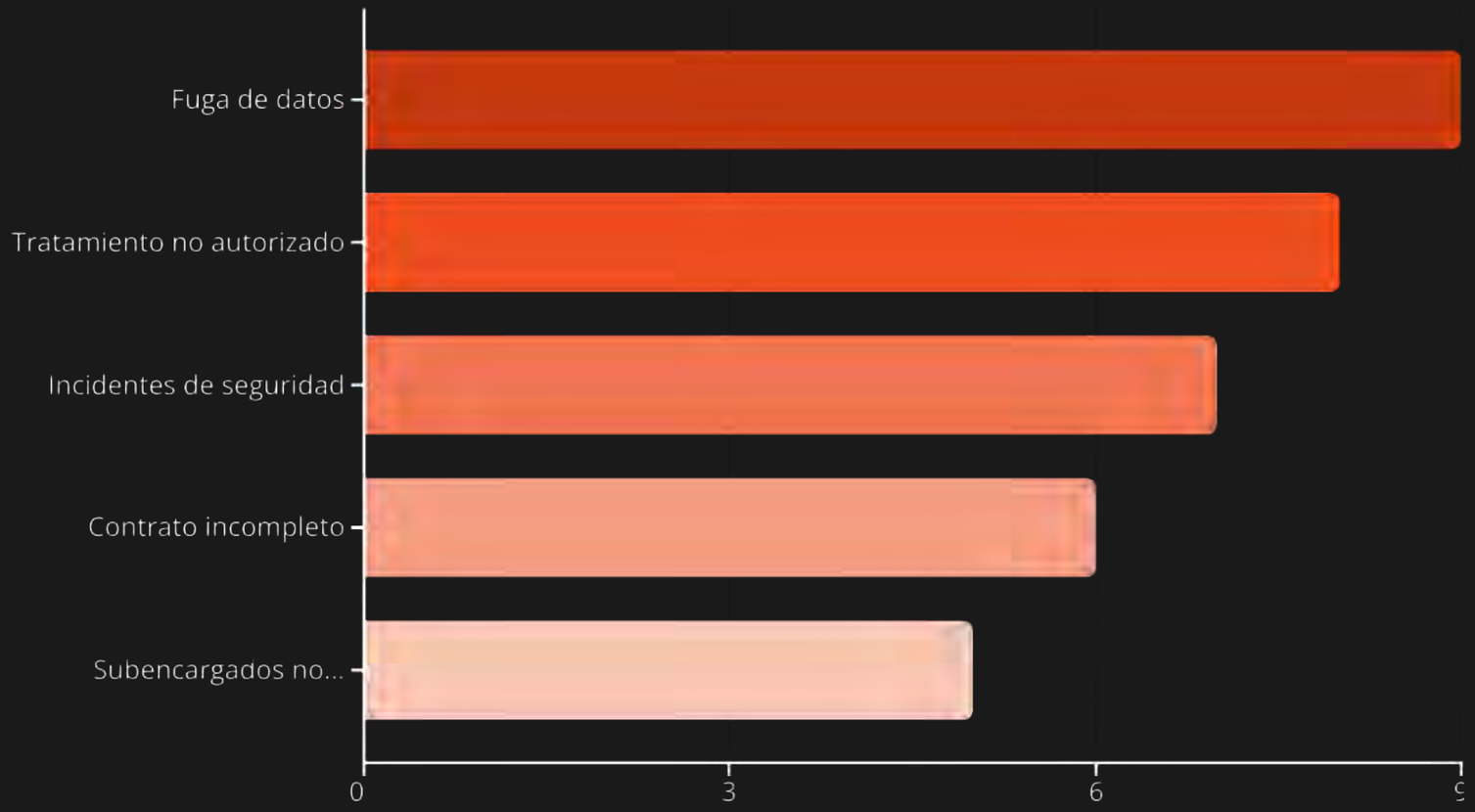
Software de Gestión de Personal

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

Servicios de Remuneraciones

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

Riesgos Asociados a la Subcontratación



La subcontratación del tratamiento de datos personales conlleva diversos riesgos que deben ser evaluados y gestionados adecuadamente. El acceso indebido a bases de datos sensibles, el uso de información para fines no autorizados y las posibles filtraciones por fallas técnicas son algunos de los riesgos más significativos.

La falta de cláusulas adecuadas en los contratos y la posibilidad de que el proveedor subcontrate a su vez sin autorización también representan vulnerabilidades importantes que deben ser abordadas mediante controles específicos.

GA·ABOGADOS

Evaluación de Riesgos en la Subcontratación

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 y seguridad de la información.

Cumplimiento Normativo

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

Contrato de Encargo

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

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.

GA·ABOGADOS

Auditoría y Supervisión: Fundamentos

Responsabilidad Proactiva

La Ley 21.719 exige al responsable del tratamiento cumplir con el principio de responsabilidad proactiva, implementando medidas eficaces para garantizar y demostrar el cumplimiento normativo. Esto incluye la realización de auditorías periódicas como parte del modelo de cumplimiento.

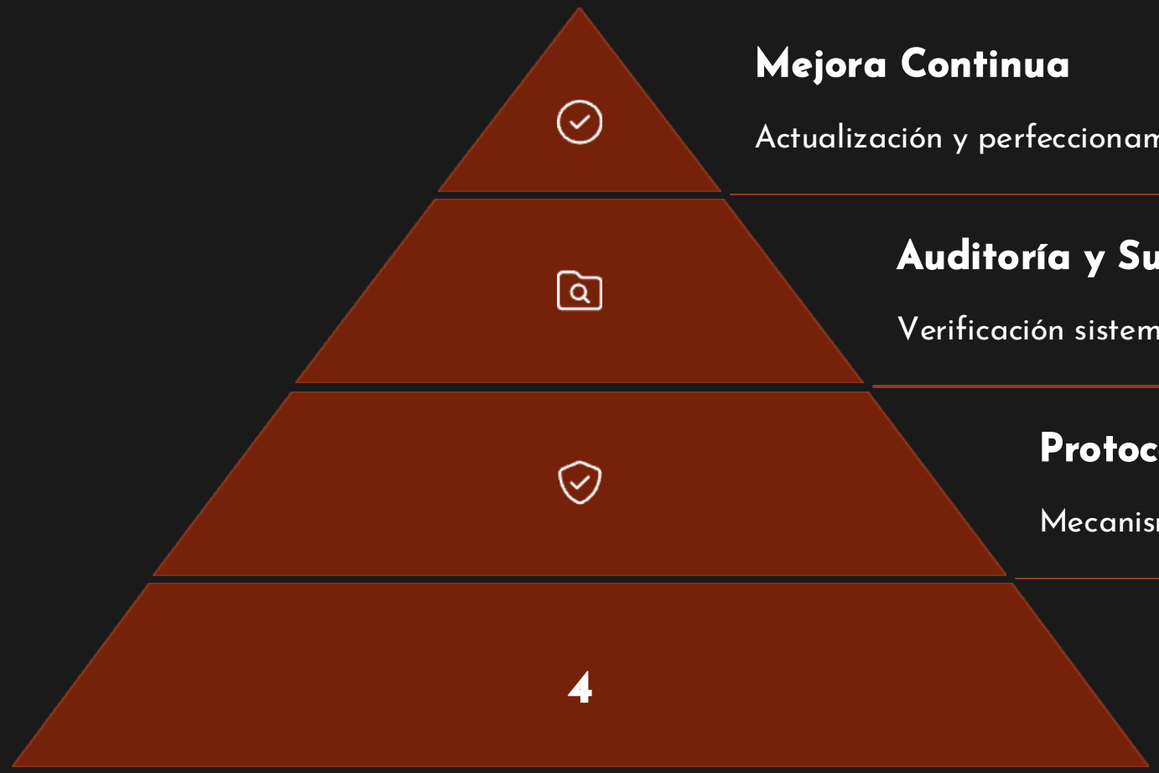
Objetivos de la Auditoría

Las auditorías en materia de protección de datos tienen como finalidad identificar brechas de cumplimiento normativo, prevenir sanciones administrativas o judiciales, detectar malas prácticas internas o de terceros y generar evidencia documental ante posibles fiscalizaciones.

Ámbitos de Supervisión

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

Modelo de Prevención y Mejora Continua



Mejora Continua

Actualización y perfeccionamiento constante

Auditoría y Supervisión

Verificación sistemática del cumplimiento

Protocolos de Control

Mecanismos para prevenir y detectar incumplimientos

Evaluación de Riesgos

Identificación de vulnerabilidades y amenazas

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

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

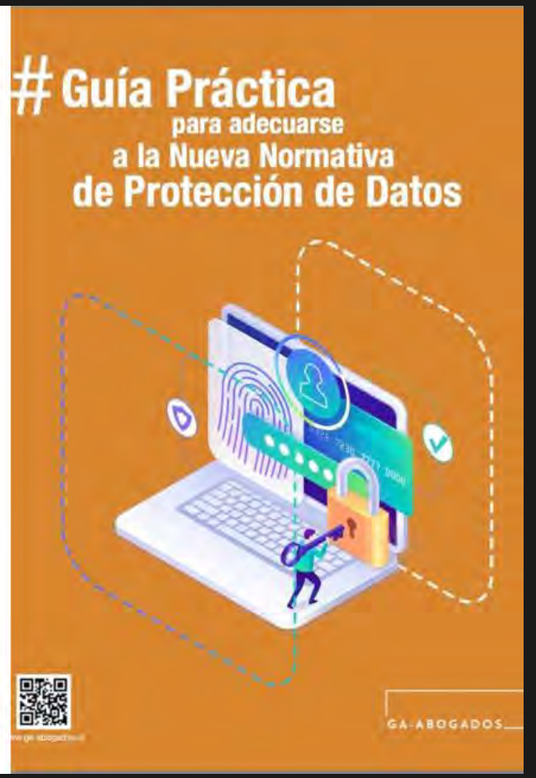
Raúl Arrieta Cortés

raul.arrieta@ga-abogados.cl

+56 2 2638 1527

www.ga-abogados.cl

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



GA-ABOGADOS