CAIGG
CONSEJO DE AUDITORÍA INTERNA GENERAL DE GOBIERNO
Ministerio Secretaría General de la Presidencia

Guía de Auditoría, Seguridad de la Información y Ciberseguridad N°14

BUENAS PRÁCTICAS PARA LA PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES

ÍNDICE

Nota

PRESENTACIÓN

En cumplimiento con las instrucciones del Presidente de la República, Gabriel Boric Font, sobre fortalecimiento de la Política de Auditoría Interna de Gobierno; el Consejo de Auditoría Interna General de Gobierno, entidad asesora en materias de auditoría interna, control interno, probidad, gestión de riesgos y gobernanza del Supremo Gobierno, presenta a la Red de Auditoría Gubernamental, la GASIC N°14: Buenas Prácticas para la Protección y Tratamiento de Datos Personales.

Esta guía forma parte de una iniciativa del CAIGG orientada a fortalecer las competencias de la función de auditoría interna del sector público en materia de Seguridad de la Información y Ciberseguridad. Su propósito es proporcionar a los Auditores Internos y a los Servicios Públicos herramientas e instrumentos técnicos que les permitan analizar y evaluar los sistemas de información conforme a las mejores prácticas internacionales y a la legislación vigente.

Santiago, noviembre 2025.

Daniela Caldana Fulss
Auditora General de Gobierno

Capítulo 1

OBJETIVO Y ALCANCE DE LA GUÍA

Capítulo 1

OBJETIVO Y ALCANCE DE LA GUÍA

Objetivos:

01 Determinar si los tratamientos de datos personales realizados por la entidad se encuentran alineados con los principios, derechos y obligaciones definidos en la Ley 21719.

02 Verificar la existencia y a su vez la eficacia de los controles administrativos, técnicos y contractuales que sustenten la licitud, la seguridad y la transparencia en el ciclo de vida de los datos.

03 Identificar posibles brechas de control y riesgos residuales que afecten la confidencialidad, integridad o disponibilidad de la información personal.

04 Emitir recomendaciones pragmáticas para fortalecer el sistema de gestión de datos personales y apoyar la toma de decisiones de la alta dirección.

Alcance de la Guía

El programa cubre todos los procesos, sistemas, bases de datos y contratos que involucren tratamiento de datos personales dentro de la entidad auditada que incluye:

- **Políticas internas y registros de actividades de tratamiento.**
- **Mecanismos para la atención de derechos de acceso, rectificación, supresión, oposición, bloqueo y portabilidad.**
- **Controles de seguridad física, lógica y organizativa, así como los procedimientos de gestión y reporte de incidentes de seguridad.**
- **Evaluaciones de impacto en protección de datos y resultados de planes de acción asociados.**
- **Contratos con encargados de tratamiento y terceros, verificación de cláusulas y garantías.**
- **Operaciones de cesión y transferencias internacionales de datos, así como las garantías**

Se excluyen de la revisión los tratamientos de carácter personal o doméstico realizados por los propios funcionarios fuera del ámbito institucional.

Capítulo 2

DETALLE DEL PROGRAMA

2.1 ÁMBITO DE APLICACIÓN Y GOBERNANZA

Objetivo:
Confirmar que la organización ha identificado su rol (responsable y/o encargado) y comprende el alcance territorial y material de la ley.

Fuente del Requisito:
Art. 1 bis (ámbito territorial) - Art. 2 letras n) "responsable" y x) "encargado" - Art. 14 inc. final (medio de contacto para responsables sin domicilio) - Art. 14 letras a-e (obligaciones generales.)

Riesgos Críticos:

- **Responsable no designado:** La ausencia de un responsable formal impide la rendición de cuentas y conlleva multas graves.
- **Roles y funciones difusas:** La superposición o vacíos generan incumplimientos por falta de claridad operativa.
- **Tratamientos fuera del radar:** Procesos ocultos o no inventariados quedan sin controles y elevan la exposición a sanciones y filtraciones.

Objetivos de la Auditoría	*Preguntas Clave*	*Pruebas Analíticas y Sustantivas*	*Medios de Evidencia*
Confirmar que la organización ha identificado su rol (responsable y/o encargado) y comprende el alcance territorial y material de la ley.	1. ¿Existe un acto formal que designe al responsable de datos y a su representante legal? 2. ¿Se mantiene actualizado un organigrama que evidencie las funciones de gobierno de datos? 3. ¿La organización dirige bienes o servicios a titulares ubicados en Chile o monitoriza su comportamiento en el territorio chileno? 4. ¿Los encargados externos están identificados y cuentan con un contrato vigente? 5. ¿Se ha comunicado a la alta dirección el marco normativo y las sanciones aplicables?	•Cruce organigrama vs inventario de tratamientos. •Tendencia de n.º de bases de datos registradas por año. •Ratio responsables designados / unidades. •Inspección de actas de designación. •Confirmación con la alta dirección.	• Actas de directorio o resolución interna de designación. • Manual de funciones y organigrama. • Evidencia de presencia web (idioma, moneda, teléfono chileno). • Contratos y registros de encargados. • Minutas de comité de datos/personas clave.

2.2 BASE DE LICITUD Y CONSENTIMIENTO

Objetivo:
Verificar que cada tratamiento se ejecute sobre una base jurídica válida y que los consentimientos se obtengan y gestionen correctamente.

Fuente del Requisito:
Art. 12 regula los requisitos del consentimiento - Art. 13 describe otras fuentes delicitud como contrato o interés legitimo.

Riesgos Críticos:

- **Consentimientos inválidos:** El uso de casillas pre marcadas o cláusulas genéricas expone a nulidad de tratamientos y sanciones.
- **Interés legítimo mal fundamentado: La** ponderación deficiente puede ser impugnada por la agencia y los titulares.
- **Registro de consentimientos incompleto:** Imposibilidad de demostrar licitud ante auditorías o litigios.

Objetivos de la Auditoría	*Preguntas Clave*	*Pruebas Analíticas y Sustantivas*	*Medios de Evidencia*
Verificar que cada tratamiento se ejecute sobre una base jurídica válida y que los consentimientos se obtengan y gestionen correctamente.	1. ¿El Registro de Actividades de Tratamiento (RAT) indica la base legitimadora para cada finalidad? 2. ¿Qué mecanismos aseguran que el consentimiento sea libre, específico, informado e inequívoco (ej. casillas desmarcadas)? 3. ¿Se documenta fecha, versión de aviso de privacidad y medio de obtención? 4. ¿Existe proceso para retirar consentimiento y dejar constancia? 5. Cuando la base sea interés legítimo, ¿existe análisis de ponderación y se comunica al titular?	• Comparar % de tratamientos por base jurídica. • Análisis revocaciones vs total consentimientos. • Detección de consentimientos duplicados o inconsistentes. • Revisión de formularios y logs de captura. • Muestreo de X consentimientos y trazabilidad completa. • Re-ejecución test "opt-out" en sitio web / app.	• Formularios/ventanas de consentimiento. • Registros de back-end y bitácora de revocaciones. • Matrices de ponderación de interés legítimo. • Procedimientos de formación al personal que recolecta datos.

2.3 PRINCIPIOS DE TRATAMIENTO

Objetivo:
Corroborar respeto de licitud, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y transparencia.

Fuente del Requisito:
Art. 12 (requisitos del consentimiento) - Art. 13 letras a-e (otras bases de licitud) - Art. 2 (letra p) "consentimiento".

Riesgos Críticos:

- **Finalidad cambiante sin actualización:** Reutilizar datos para fines no declarados conlleva multas gravísimas.
- **Retención excesiva:** El almacenamiento indefinido incrementa la superficie de ataque y los costos de brecha.
- **Baja calidad de datos:** La inexactitud provoca decisiones erróneas y reclamos por daños.

Objetivos de la Auditoría	*Preguntas Clave*	*Pruebas Analíticas y Sustantivas*	*Medios de Evidencia*
Corroborar respeto de licitud, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y transparencia.	1. ¿Se limita la recolección a datos adecuados y pertinentes? 2. ¿Existen reglas de supresión/anonimización al expirar plazos? 3. ¿Se aplican controles de calidad de datos (exactitud, actualización)? 4. ¿El responsable puede demostrar trazabilidad de cada dato (fuente, fecha, transformación)? 5. ¿Se publica información clara y se fomenta cultura de confidencialidad?	• Ratio campos recolectados vs usados por proceso. • Edad media de registros almacenados. • Indicador de errores/1000 registros (calidad). • Revisión de scripts/policies de retención. • Observación de minimización en formularios. • Re-cálculo de reglas de validación y controles de calidad.	• Políticas de minimización y retención. • Cron-jobs o scripts de eliminación. • Dashboards de data-quality. • Logs de ETL y catálogos de metadatos. • NDAs/Acuerdos de confidencialidad.

2.4 POLÍTICA DE INFORMACIÓN Y TRANSPARENCIA

Objetivo:
Evaluar que la política de privacidad cumpla requisitos formales y sea accesible.

Fuente del Requisito:
Art. 14 ter lista la información mínima que debe estar permanentemente disponible, como la política vigente, medios de contacto y las medidas de seguridad adoptadas.

Riesgos Críticos:

- **Información insuficiente al titular:** Genera reclamos y medidas correctivas ordenadas por la Agencia.
- **Versiones obsoletas:** Divergencia entre prácticas reales y política publicada aumenta riesgo reputacional.
- **Accesibilidad limitada:** La falta de canales inclusivos expone a infracciones por discriminación.

Objetivos de la Auditoría	*Preguntas Clave*	*Pruebas Analíticas y Sustantivas*	*Medios de Evidencia*
Evaluar que la política de privacidad cumpla los requisitos formales y sea accesible.	1. ¿La política identifica responsable, domicilio y contacto? 2. ¿La organización detalla categorías de datos, finalidades, bases de licitud, destinatarios? 3. ¿Informa al titular sobre sus derechos y procedimientos? 4. ¿Especifica medidas de seguridad y plazos de conservación? 5. ¿Se mantiene historial de versiones?	• Análisis de versiones y fechas de cambios. • Conteo de secciones obligatorias faltantes. • Métricas de accesos (web analytics). • Inspección integral de la política publicada. • Verificación de control de versiones / gestor documental. • Prueba de accesibilidad (WCAG).	• Copia de la política (web y repositorio). • Registro de cambios y aprobaciones. • Capturas de pop-ups/avisos de privacidad. • Evidencia de accesibilidad (lectores de pantalla, etc.)

2.5 GESTIÓN DE DERECHOS DE TITULARES

Objetivo:
Comprobar procesos eficaces para responder solicitudes dentro de plazos.

Fuente del Requisito:
Art. 14 ter lista la información mínima que debe estar permanentemente disponible, como la política vigente, medios de contacto y las medidas de seguridad adoptadas.

Riesgos Críticos:

- **Plazos legales incumplidos:** La Ley impone sanciones progresivas por cada solicitud fuera de tiempo.
- **Verificación de identidad laxa:** Respuesta a impostores produce divulgación no autorizada.
- **Procesos manuales saturados:** Picos de solicitudes pueden colapsar y derivar en incumplimiento masivo.

Objetivos de la Auditoría	*Preguntas Clave*	*Pruebas Analíticas y Sustantivas*	*Medios de Evidencia*
Comprobar procesos eficaces para responder solicitudes dentro de plazos.	1. ¿Existe un canal único (portal, correo, oficina) para las solicitudes? 2. ¿Hay un procedimiento para verificar la identidad y este registra la fecha de ingreso y/o respuesta? 3. ¿Se cumplen los plazos legales (X días + prórroga)? 4. ¿Se comunica fundadamente la aceptación o rechazo? 5. ¿Se han realizado simulacros de alta demanda?	• Tendencia solicitudes vs mes. • Tiempo medio respuesta vs SLA. • Ratio solicitudes fuera de plazo. • Muestreo de expedientes cerrados. • Re-ejecución de solicitud ficticia e identificación. • Verificación documental de controles de identidad.	• Ticketing/Libro de registro. • Expedientes completos. • Resultados de pruebas internas (cliente incógnito). • KPIs de desempeño de servicio.

2.6 DECISIONES AUTOMATIZADAS Y PERFILES

Objetivo:
Comprobar procesos eficaces para responder solicitudes dentro de plazos.

Fuente del Requisito:
Art. 8 bis (derecho a no ser objeto de decisiones exclusivamente automatizadas) - Art.14 ter l) (obligación de informar lógica y consecuencias).

Riesgos Críticos:

- **Algoritmos opacos con sesgo:** Discriminación inadvertida genera sanciones y litigios por daños morales.
- **Falta de intervención humana:** Decisiones sin revisión violan derechos de los titulares.
- **Dataset de entrenamiento no documentado:** Imposibilidad de justificar lógica ante requerimientos regulatorios.

Objetivos de la Auditoría	*Preguntas Clave*	*Pruebas Analíticas y Sustantivas*	*Medios de Evidencia*
Comprobar procesos eficaces para responder solicitudes dentro de los plazos establecidos.	1. ¿Se identifican procesos con scoring, IA o ML de impacto jurídico o significativo? 2. ¿Se informa lógica aplicada al titular? 3. ¿Se ofrece intervención humana y derecho a impugnar? 4. ¿Existen evaluaciones de sesgo y auditorías de algoritmo? 5. ¿Los datasets de entrenamiento están documentados?	• Mapa de procesos con IA / scoring. • Análisis de tasas de rechazo por segmento. • Detección de variables sensibles en modelos. • Inspección de documentación y/o modelo. • Revisión dataset de entrenamiento y fairness testing. • Entrevistas con Data Science y verificación de controles.	• Inventario de algoritmos. • Avisos de privacidad y FAQ específicas. • Registros de apelaciones. • Informes de auditoría de IA.

2.7 PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

Objetivo:
Verificar aplicación de PbD en proyectos y sistemas.

Fuente del Requisito:
Art. 16 regla general y excepciones para datos sensibles - Art. 16 quater regula datos de menores con consentimiento de padres y principio de interés superior - Art. 14 quáter incisos 1-2 (medidas técnicas y organizativas desde el diseño y por defecto.)

Riesgos Críticos:

- **Nuevos proyectos sin evaluación de privacidad:** Lanzamientos apresurados generan brechas legales y de seguridad.
- **Configuraciones permisivas por defecto:** La exposición innecesaria de datos incrementa vectores de ataque.
- **Entornos de prueba con datos reales:** Posible filtración accidental mediante desarrolladores o terceros.

Objetivos de la Auditoría	*Preguntas Clave*	*Pruebas Analíticas y Sustantivas*	*Medios de Evidencia*
Verificar aplicación de PbD en proyectos y sistemas.	1. ¿Existe metodología formal PbD en ciclo de vida TI? 2. ¿Hay revisiones de privacidad en comité de arquitectura? 3. ¿Los entornos dev/test usan datos seudonimizados? 4. ¿La configuración por defecto restrictiva? 5. ¿Se documentan riesgos y mitigaciones?	• Nº proyectos con PbD aplicado / total. • Comparativa hitos PbD vs cronograma TI. • Revisión de plantillas PbD llenadas. • Observación de entorno dev/test. • Validación de parámetros privacy-by-default.	• Plantillas/Checklists PbD. • Actas comité de arquitectura. • Evidencia de seudonimización. • Capturas de configuración.

2.8 MEDIDAS DE SEGURIDAD

Objetivo:
Asegurar controles técnicos-organizativos que protejan confidencialidad, integridad y disponibilidad.

Fuente del Requisito:
Art. 14 quinquies literales a-d (seudonimización, cifrado, resiliencia, pruebas de eficacia de controles.)

Riesgos Críticos:

- **Cifrado inexistente o mal implementado:** Datos en texto claro comprometidos ante intrusiones.
- **Respaldo y recuperación ineficaces:** La pérdida de disponibilidad genera sanciones y daños operativos.
- **Gestión de vulnerabilidades reactiva:** Posible explotación de fallas conocidas antes de parches.

Objetivos de la Auditoría	*Preguntas Clave*	*Pruebas Analíticas y Sustantivas*	*Medios de Evidencia*
Asegurar controles técnicos y organizativos que protejan la confidencialidad, integridad y disponibilidad.	1. ¿Existe Seudonimización y cifrado implementados en reposo y tránsito? 2. ¿Se ha definido un Plan de continuidad con RTO/RPO definidos y probado? 3. ¿Hay evaluaciones de vulnerabilidad y pentest anuales? 4. ¿El Inventario de activos está actualizado y los datos están clasificados? 5. ¿Hay una revisión periódica de eficacia de controles?	• Tendencia hallazgos críticos (vuln scan). • Cobertura cifrado (discos/DB). • Análisis incidentes por tipo. • Inspección evidencias de cifrado. • Restore test de backup. • Muestreo informes pentest y cierres.	• Políticas y/o estándares de seguridad. • Reportes de restauración. • Escaneos de vulnerabilidad y planes de remediación. • Herramientas gestión de activos.

2.9 GESTIÓN DE INCIDENTES Y NOTIFICACIÓN

Objetivo:
Verificar que incidentes se gestionen y notifiquen conforme la ley.

Fuente del Requisito:
Art. 14 incisos 1-4 (obligación de reportar vulneraciones a la Agencia y, en casos sensibles, a los titulares; registro de incidentes.)

Riesgos Críticos:

- **Detección tardía de brechas:** Aumenta impacto y agrava sanciones por notificación extemporánea.
- **Criterios de severidad ambiguos:** Las discusiones internas retrasan el aviso obligatorio.
- **Comunicaciones incompletas:** Las omisiones en la notificación generan medidas sancionatorias adicionales.

Objetivos de la Auditoría	*Preguntas Clave*	*Pruebas Analíticas y Sustantivas*	*Medios de Evidencia*
Verificar que los incidentes se gestionen y notifiquen conforme la ley.	1. ¿Existe IRP con roles y severidad definidos? 2. ¿Se analiza el riesgo para los titulares antes de notificar? 3. ¿Las notificaciones a la Agencia se registran con detalle? 4. ¿Se notifica a los titulares en casos legales? 5. ¿Se realizan evaluaciones ex post y lecciones aprendidas?	• Tiempo de detección > contención. • Nº incidentes notificados / total. • Clasificación por severidad. • Inspección bitácora SIEM/IRP. • Simulacro de brecha. • Confirmación de las notificaciones a agencia y/o titulares.	• IRP aprobado. • Registro de incidentes. • Comunicaciones a agencia y titulares. • Informes post-mortem.

2.10 DIFERENCIACIÓN DE ESTÁNDARES

Objetivo:
Confirmar aplicación de estándares proporcionales al tamaño y naturaleza.

Fuente del Requisito:
Art. 14 incisos 1-4 (obligación de reportar vulneraciones a la Agencia y, en casos sensibles, a los titulares; registro de incidentes)

Riesgos Críticos:

- **Sobre-o sub-dimensionar controles:** El exceso encarece las operaciones; el defecto deja brechas legales.
- **Cambio de categoría sin ajuste:** El crecimiento empresarial sin actualizar medidas viola proporcionalidad.
- **Desconocimiento de instrucciones de la Agencia:** El incumplimiento directo de regulaciones específicas.

Objetivos de la Auditoría	*Preguntas Clave*	*Pruebas Analíticas y Sustantivas*	*Medios de Evidencia*
Confirmar la aplicación de estándares proporcionales al tamaño y la naturaleza.	1. ¿La entidad clasificó su categoría según la Ley 20.416? 2. ¿Los controles se ajustan a categoría? 3. ¿Se justifica controles simplificados/reforzados? 4. ¿Se revisan cambios de tamaño o datos? 5. ¿Se aplican instrucciones de la Agencia?	• Benchmark controles vs categoría. • Ratio inversión seguridad / ingreso. • Matriz controles simplificados. • Verificar matriz de controles. • Inspección de justificativos. • Entrevista del área de compliance.	• Certificados tamaño empresa. • Matriz proporción-controles. • Boletines Agencia. • Planes de mejora escalonados.

2.11 CESIÓN Y CONTRATACIÓN DE ENCARGADOS

Objetivo:
Evaluar que cesiones y contratos cumplan requisitos.

Fuente del Requisito:

Art. 15 (cesión de datos: consentimiento, contrato escrito, nulidad) - Art. 15 bis (encargado: objeto, duración, subcontratación, responsabilidad solidaria.)

Riesgos Críticos:

- **Contratos sin cláusulas clave:** La ausencia de confidencialidad y subcontratación controlada expone datos.
- **Auditoría insuficiente a proveedores:** Compromisos que son asumidos en el papel pero no se cumplen en la práctica.
- **Retención de datos tras término del servicio:** Fuga o uso ulterior no autorizado.

Objetivos de la Auditoría	*Preguntas Clave*	*Pruebas Analíticas y Sustantivas*	*Medios de Evidencia*
Evaluar que las cesiones y contratos cumplan los requisitos.	1. ¿Contratos de cesión identifican datos, finalidades, plazos? 2. ¿Se prohíbe uso para finalidades distintas? 3. ¿Se solicita la autorización de subcontratación por escrito? 4. ¿Existe un proceso de auditoría periódica a proveedores? 5. ¿Existe un proceso de supresión o devolución al término?	• Nº contratos con cláusulas faltantes. • Análisis SLA de proveedores. • Excepciones de sub-encargo. • Revisión de 25 contratos. • Confirmación SOC 2 / ISO 27001. • Verificación de destrucción/devolución.	• Contratos y anexos. • Declaración de subcontratos. • Informes de auditoría al proveedor. • Certificados de destrucción de datos.

2.12 EVALUACIÓN DE IMPACTO

Objetivo:
Comprobar EIPD para tratamientos de alto riesgo.

Fuente del Requisito:
Art. 15 ter incisos 1-5 (alto riesgo, supuestos a-d, lista orientativa, consulta a la Agencia.)

Riesgos Críticos:

- **Riesgos altos no identificados:** Los tratamientos inician sin las mitigaciones adecuadas.
- **EIPD cosmética:** Los documentos sin análisis técnico real exponen a sanciones si llega a ocurrir un incidente.
- **No actualización post-cambios:** Los nuevos escenarios dejan obsoleta la evaluación original.

Objetivos de la Auditoría	*Preguntas Clave*	*Pruebas Analíticas y Sustantivas*	*Medios de Evidencia*
Comprobar EIPD para tratamientos de alto riesgo.	1. ¿Existe una metodología formal para EIPD? 2. ¿Se elaboran antes de iniciar tratamiento? 3. ¿Consulta a la Agencia si el riesgo es alto? 4. ¿La evaluación de impacto es aprobada por la alta dirección? 5. ¿Se monitorean las mitigaciones?	• porcentaje de tratamientos de alto riesgo con EIPD. • Antigüedad promedio de EIPD. • Comparativa de riesgos residuales al año. • Revisión de EIPD completas. • Confirmación de la aprobación de la dirección. • Comprobación del seguimiento de las mitigaciones.	• Plantillas y guías EIPD. • Informes firmados. • Correspondencia con la agencia. • Actas de aprobación.

2.13 DATOS SENSIBLES Y MENORES

Objetivo:
Garantizar salvaguardas reforzadas.

Fuente del Requisito:
Art. 27 incisos 1-3 y literales a-c (país adecuado, garantías contractuales, modelos certificados) - Art. 27 inciso final literales a-h (supuestos excepcionales) - Art. 28 literales a-c (criterios de adecuación y control de la Agencia)

Riesgos Críticos:

- **Autorización vaga:** Consentimiento tácito o confuso para los datos sensibles genera una infracción gravísima.
- **Falta de controles parentales:** La recopilación de datos de menores sin verificación legal conlleva sanciones severas.
- **Accesos amplios a bases sensibles:** Aumenta la probabilidad de filtración y extorsión.

Objetivos de la Auditoría	*Preguntas Clave*	*Pruebas Analíticas y Sustantivas*	*Medios de Evidencia*
Garantizar salvaguardas bien reforzadas.	1. ¿El consentimiento es expreso y separado? 2. ¿Las excepciones legales están documentadas? 3. ¿Hay verificación de edad y control parental? 4. ¿Se aplica seudonimización reforzada? 5. ¿El acceso es restringido y auditado?	• Ratio de datos sensibles / totales. • Tendencia de accesos bases sensibles. • Alertas de fallos del control parental. • Muestreo de consentimientos explícitos. • Prueba RBAC y logs de acceso. • Verificación de procesos de verificación de edad.	• Formularios de consentimiento. • Logs acceso a bases. • Políticas RBAC. • Registros de verificación de edad.

2.14 TRANSFERENCIA INTERNACIONAL

Objetivo:
Asegurar transferencias transfronterizas válidas.

Fuente del Requisito:
Art. 2 (letra z) (definición del Registro) - Art. 33 incisos 3-6 (obligación de inscripción de modelos certificados y sanciones firmes.)

Riesgos Críticos:

- **Países sin nivel adecuado:** Exportar datos a jurisdicciones inseguras y sin garantías expone a multas y a unq prohibición temporal de flujos.
- **Cláusulas contractuales tipo ausentes:** Transferencias internamente autorizadas, pero legalmente inválidas.
- **Monitoreo post-transferencia inexistente:** Pérdida de control sobre datos fuera del país sin detección de incumplimientos.

Objetivos de la Auditoría	*Preguntas Clave*	*Pruebas Analíticas y Sustantivas*	*Medios de Evidencia*
Asegurar transferencias transfronterizas válidas.	1. ¿Se revisa el nivel adecuado del país destino? 2. ¿SCC/BCR firmadas cuando no hay adecuación? 3. ¿Registros de transferencias excepcionales? 4. ¿Monitoreo periódico de las garantías? 5. ¿Se le informa al titular sobre la transferencia?	• Volumen mensual de exportaciones por destino. • Porcentaje de flujos con SCC/BCR vigentes. • Tiempo de actualización de las garantías. • Revisión de registros de transferencia. • Inspección de cláusulas contractuales. • Confirmación del nivel adecuado del destino.	• Listado de países adecuados. • Contratos con SCC/BCR. • Logs de exportación. • Auditoría de destinatarios. • Comunicaciones al titular.

Capítulo 3

RESULTADOS OBTENIDOS

3.1 RESULTADOS

La aplicación de los procedimientos analíticos y sustantivos propuestos permitirá identificar tendencias, brechas y riesgos críticos en el cumplimiento de la Ley 21.719. Dado que esta ley regula la protección de los derechos de los titulares de datos personales y las obligaciones de los responsables del tratamiento, los hallazgos se orientan hacia la eficacia de las políticas, la existencia de mecanismos de respuesta y la coherencia entre lo declarado y lo ejecutado.

De los procedimientos aplicados, podrían surgir resultados como los siguientes:

- **Ausencia o desactualización de la política de protección de datos personales publicada en el sitio web institucional.**
- **Falta de identificación clara del responsable de tratamiento, domicilio de contacto u otros requisitos del Art. 14 ter.**
- **Uso de categorías de datos sin justificación documentada, o tratamiento de datos sensibles sin autorización válida.**
- **Incumplimiento en la entrega de respuestas a solicitudes de derechos de los titulares (acceso, rectificación, cancelación, oposición).**
- **Registro incompleto o inexistente de solicitudes de titulares y de medidas de atención implementadas.**
- **Deficiencias en la implementación de medidas de seguridad técnicas y organizativas frente a los estándares requeridos.**
- **Ausencia de mecanismos para acreditar consentimiento expreso cuando corresponde.**
- **Evidencia de que algunos procesos internos no cuentan con controles para limitar el acceso a los datos personales.**
- **Brechas en la trazabilidad de las transferencias de datos a terceros, incluidas autoridades y proveedores externos.**
- **Desajustes entre lo declarado en la política de privacidad y las prácticas reales observadas durante la auditoría.**

Capítulo 4

DOCUMENTACIÓN REQUERIDA

4.1 DOCUMENTACIÓN REQUERIDA

Para respaldar los hallazgos y conclusiones de la auditoría de cumplimiento, será necesario recabar la siguiente documentación de respaldo, que podrá ser solicitada al organismo o entidad auditada según los procedimientos establecidos.

- **Copia actualizada de la política de privacidad y protección de datos personales publicada en los medios oficiales.**
- **Documentación formal que individualice al responsable del tratamiento (Nombre, cargo, domicilio, medio de contacto).**
- **Registro de las categorías y tipos de datos tratados, así como sus bases legales de justificación.**
- **Evidencias de los mecanismos de consentimiento expreso o tácito según corresponda.**
- **Registro de solicitudes de titulares (Acceso, rectificación, cancelación, oposición) y respuestas emitidas, con fechas y responsables.**
- **Procedimientos internos para garantizar la seguridad de la información (Protocolos, manuales, matrices de riesgo).**
- **Evidencias de la implementación de medidas de seguridad: Respaldos, controles de acceso, encriptación, monitoreo.**
- **Copia de contratos y convenios con terceros que tengan acceso a datos personales, que incluyan cláusulas de protección de datos.**
- **Actas de comités, capacitaciones o actividades de sensibilización en torno a la protección de datos personales.**
- **Informes de incidentes de seguridad relacionados con datos personales, medidas correctivas y lecciones aprendidas.**

Capítulo 5

INDICADORES DE DESEMPEÑO

5. INDICADORES DE DESEMPEÑO

Con el fin de evaluar los resultados de las pruebas realizadas y establecer un sistema de control periódico respecto a la gestión de riesgos y el cumplimiento de las obligaciones legales en materia de protección de datos y ciberseguridad, se sugiere definir y evaluar **Indicadores Clave de Desempeño (KPI)** con periodicidad mensual, trimestral, semestral y/o anual. Los KPI permiten identificar tendencias, detectar alertas tempranas y evaluar el impacto institucional de las pruebas realizadas.

5.1 INDICADORES DE USO Y COMPORTAMIENTO

- **Porcentaje de sistemas evaluados con hallazgos de seguridad críticos o altos.**
- **Promedio de hallazgos por sistema o aplicación evaluada.**
- **Promedio de hallazgos corregidos por ciclo de revisión.**
- **Porcentaje de hallazgos reiterados en diferentes evaluaciones o pruebas.**
- **Porcentaje de titulares de datos informados respecto a brechas o incidentes, conforme a la normativa.**
- **Porcentaje de cumplimiento de los controles de ciberseguridad exigidos en la ley y normativas aplicables (Ejemplo: Art. 14 ter: política de seguridad, medidas técnicas, responsable designado).**

5.2 INDICADORES DE RIESGO O ALERTA

- **Porcentaje de hallazgos críticos sin plan de tratamiento aprobado en el plazo definido.**
- **Porcentaje de pruebas en las que no se presentó evidencia de medidas de seguridad. (Ej: cifrado, autenticación, registro de acceso).**
- **Porcentaje de controles de seguridad no implementados pese a estar declarados en la política de protección de datos.**
- **Número de incumplimientos a los derechos de los titulares detectados. (Ej: Falta de respuesta a solicitudes de acceso o rectificación).**
- **Cantidad de incidentes de ciberseguridad detectados durante las pruebas, que requirieron escalamiento a organismos externos. (CSIRT, reguladores).**

5.3 INDICADORES DE IMPACTO INSTITUCIONAL

- **Impacto estimado en horas/hombre destinadas a corregir hallazgos críticos derivados de las pruebas.**
- **Variación interanual en la cantidad de hallazgos graves detectados.**
- **Porcentaje de reducción de la pérdida anual esperada (ALE) tras la implementación de controles identificados en las pruebas.**
- **Efecto de las mejoras implementadas sobre el apetito y tolerancia al riesgo definidos por la organización.**
- **Impacto estimado en recursos financieros asociados a incidentes simulados o detectados. (Costo de remediación, sanciones potenciales, pérdida de confianza).**

Capítulo 6

DESCRIPCIÓN DE TÉCNICAS DE AUDITORÍA ÚTILES PARA EL TRABAJO

6.1 PROCEDIMIENTOS ANALÍTICOS APLICADOS A DATOS MASIVOS

Objetivo:
Detectar patrones de incumplimiento, omisiones y conductas inusuales en la aplicación de la Ley 21.719, a través del análisis sistemático de datos estructurados. (Políticas publicadas, solicitudes de derechos, registros de seguridad, etc.).

	Técnica / Procedimiento	*Descripción Aplicada*	*Ejemplo Práctico*
1	Análisis de Consistencia Documental.	Verificar si las políticas de privacidad incluyen todos los elementos exigidos. •Responsable. •Domicilio. •Categorías de datos. •Medidas de seguridad. •Derechos.	*La detección de una política publicada que no incluye domicilio ni medidas de seguridad.*
2	Detección de omisiones en respuestas a titulares.	Analizar bases de datos de solicitudes recibidas y respuestas entregadas para identificar tiempos de respuesta y omisiones.	*Se detecta que el 30% de las solicitudes de acceso superaron el plazo legal de respuesta.*
3	Análisis de clasificación de datos.	Revisar la categorización de datos tratados versus los datos declarados en la política publicada.	*La organización declara que no trata datos sensibles, pero sí mantiene registros de salud de empleados.*
4	Detección de patrones de incidentes.	Evaluar los registros de seguridad para identificar reincidencias en las fugas de datos o en los accesos indebidos.	*El mismo usuario interno aparece en tres reportes de acceso indebido a datos sensibles en un semestre.*
5	Evaluación de coherencia entre bases de datos.	Contrastar los datos declarados a la autoridad en contraposición con la información interna de la organización.	*El informe anual declara 20 solicitudes de rectificación, pero los registros internos muestran 45.*

6.2 TÉCNICAS DE AUDITORÍA SUSTANTIVA

Objetivo:
Obtener evidencia directa que confirme o refute los hallazgos detectados mediante los procedimientos analíticos.

	Técnica / Procedimiento	*Descripción Aplicada*	*Ejemplo Práctico*
1	Confirmación externa con titulares.	Verificar directamente con los titulares si recibieron una respuesta adecuada a sus solicitudes.	*Los titulares confirman que nunca recibieron una notificación sobre la eliminación de sus datos.*
2	Confirmación externa con la autoridad.	Revisar comunicaciones y requerimientos de la autoridad respecto a incumplimientos o sanciones.	*Se detecta oficio de la autoridad instruyendo correcciones no reflejadas en la práctica de la organización.*
3	Inspección de evidencias de seguridad.	Revisar registros de control de accesos, respaldos y planes de continuidad.	*No existen respaldos documentados que soporten la política de seguridad publicada.*
4	Revisión de canales de ejercicio de derechos.	Verificar que los mecanismos habilitados (web, correo, presencial) estén activos y disponibles.	*Un link en la web de la organización redirige a una página inexistente para ejercer derechos ARCO.*
5	Análisis cruzado de contratos y consentimientos.	Revisar contratos de terceros y registros de consentimientos para confirmar alineación con lo declarado en las políticas.	*El contrato con un proveedor de cloud no contempla cláusulas de confidencialidad de datos personales.*

6.3 TÉCNICAS DE VISUALIZACIÓN DE DATOS

Objetivo:
Comunicar hallazgos de auditoría de manera clara y comprensible, facilitando la detección de patrones de incumplimiento y riesgos.

	Técnica / Procedimiento	*Descripción Aplicada*	*Ejemplo Práctico*
1	Mapas de calor de los tiempos de respuesta.	Visualizar el cumplimiento de los plazos de respuesta a las solicitudes de los titulares.	*Una alta concentración de respuestas fuera de plazo durante los meses Enero y Julio.*
2	Diagramas de red de responsables y flujos de datos.	Representar relaciones entre responsables, encargados y flujos de datos dentro y fuera de la organización.	*La identificación de un proveedor externo como nodo central de transferencias no declaradas.*
3	Series temporales de incidentes.	Mostrar frecuencia y recurrencia de incidentes de seguridad en el tiempo.	*Picos de incidentes reportados en los trimestres en que hubo cambios tecnológicos.*
4	Gráficos de barras comparativas.	Comparar el cumplimiento de los requisitos legales entre las distintas unidades o servicios.	*La unidad A cumple con el 90% de los requisitos en políticas, mientras que la unidad B solo cumple con un 60%.*
5	Semáforo de criticidad. (Alertas visuales)	Codificar las áreas o los requisitos según el nivel de riesgo: •Rojo (Alto). •Naranja (Medio). •Verde (Bajo).	*El requisito de derecho de supresión aparece en rojo por no encontrarse operativo.*

Anexo

TABLA DE CORRESPONDENCIA

7. ANEXO: TABLA DE CORRESPONDENCIA

	Derecho / Requisito Detallado (Art.)	*Punto*
1	**Derechos del titular (Título I)**	
	• Derecho de Acceso (Art. 5 a–f) Datos tratados, finalidad,destinatarios, plazo, intereses legítimos, lógica automatizada.	*5*
	• Derecho de Rectificación (Art. 6) – Corrección datos inexactos/desactualizados, comunicación a terceros.	*5*
	• Derecho de Supresión (Art. 7 a–f, excepciones i–vi)	*5*
	• Derecho de Oposición (Art. 8 a–c)	*5*
	• Derecho de Portabilidad (Art. 4 / definiciones + Art. 8 bis)	*5*
	• Derecho de Bloqueo (Art. 4, 5)	*5*
2	**Principios de Tratamiento (Art. 3)** **Licitud y lealtad, finalidad,proporcionalidad, calidad, responsabilidad, seguridad, transparencia, confidencialidad.**	*3*
3	**Bases de Licitud (Art. 12–13)** **Consentimiento; contrato; obligación legal; interés legítimo; defensa de derechos, interés vital, función pública.**	*2*
4	**Consentimiento Válido (Art. 12) Libre, específico, informado,inequívoco; Retiro sin afectar licitud previa.**	*2*
5	**Obligaciones Generales del Responsable (Art. 14 a–e)**	*1,2,3*
	• a) Acreditar Licitud del Tratamiento	*3*
	• b) Fuentes Lícitas y Finalidad Específica	*3*
	• c) Comunicar Datos Exactos/Actuales	*3*
	• d) Suprimir/Anonimizar Tras Medidas Precontractuales	*3*
	• e) Cumplir Principios y Deberes de la Ley	*3*
6	**Deber de Secreto/Confidencialidad (Art. 14 bis)**	*3-8*
7	**Deber de Información y Transparencia (Art. 14 ter) – Detalle Literal: A–L**	*4*
	• a) Política de Tratamiento, Versión y Fecha	*4*
	• b) Individualización Responsable y Representante; Encargado de Prevención	*4*
	• c) Domicilio Postal, Correo, Formulario de Contacto	*4*

7. ANEXO: TABLA DE CORRESPONDENCIA

	Derecho / Requisito Detallado (Art.)	*Punto*
7	• d) Derecho de Acceso (Art. 5 a–f) Datos tratados, finalidad,destinatarios, plazo, intereses legítimos, lógica automatizada.	*4*
	• e) Política y Medidas de Seguridad Adoptadas	*4,8*
	• f) Derecho del Titular a Solicitar ARSOPB (Acceso-rectificación-supresión-oposición-portabilidad-bloqueo)	*4,5*
	• g) Derecho a Reclamar Ante la Agencia	*4*
	• h) Transferencia Internacional, Nivel Adecuado o Garantías	*4,14*
	• i) Plazo de Conservación de Datos	*3,4*
	• j) Fuente de los Datos y Procedencia de Acceso Público	*4*
	• k) Derecho a Retirar Consentimiento	*2,4*
	• l) Existencia de Decisiones Automatizadas y Lógica	*6,4*
8	**Privacy by Design y por Defecto (Art. 14 quáter)**	*7*
9	**Medidas de Seguridad (Art. 14 quinquies a–d) Seudonimización, cifrado, resiliencia, test de eficacia**	*8*
10	**Notificación de Vulneraciones (Art. 14 sexies) Agencia y titulares sensibles/menores/etc.**	*9*
11	**Diferenciación de Estándares (Art. 14 septies) Tamaño empresa, tipo de datos**	*10*
12	**Cesión de Datos Personales (Art. 15)** **Consentimiento, contrato por escrito, identificación datos, finalidad, nulidad si falta**	*11*
13	**Contrato con Encargado (Art. 15 bis) Objeto, duración, categorías, subcontratación, responsabilidad solidaria**	*11*
14	**Evaluación de Impacto en Protección de Datos (Art. 15 ter)** **Requisitos a-d, lista de la Agencia, consulta, orientaciones mínimas**	*12*
15	**Reglas Especiales Datos Sensibles (Art. 16) Consentimiento expreso, excepciones a-f**	*13*
16	**Protección de Datos de Menores (Art. 16 quater)** **Consentimiento parental, interés superior (cuando procede)**	*13*
17	**Transferencia internacional (Título V – arts. 27-28)**	*14*
	• a) Regla General de Autorización (27 a–c) País adecuado, garantías, modelo cumplimiento	*14*
	• b) Transferencia Específica en Ausencia de Adecuación/Garantías	*14*

7. ANEXO: TABLA DE CORRESPONDENCIA

	Derecho / Requisito Detallado (Art.)	*Punto*
17	• c) Criterios para Determinar País Adecuado y Control Agencia (Art. 28 a-c)	*14*
18	**Registro Nacional de Sanciones y Modelos Certificados (Art. 2 literal z + art. 33)**	*14*
19	**Obligación de Designar Medio de Contacto si Responsable sin Domicilio en Chile (Art. 14 último inciso)**	*4,1*
20	**Derecho a no ser Discriminado por Ejercicio de Derechos (Arts. 4-8)**	*Parcial - 5*
21	**Obligación de Conservar el Historial de Notificaciones de Incidentes (14 sexies)**	*9*
22	**Garantizar Medidas Reforzadas para Menores de 14 años (Arts. 16-17)**	*13*
23	**Obligación de Conservar el Historial de Notificaciones de Incidentes (14 sexies)**	*6*