Webinar · Chile

Cómo los equipos TI deben prepararse para Ley 21.719

Preguntas frecuentes del **webinar** para equipos de TI y sus asesores legales.

Prey · Julio 2026

El 1 de diciembre de 2026 entra en vigencia la **Ley 21.719**, y con ella un cambio de fondo: proteger datos personales deja de ser una buena práctica y pasa a ser una obligación exigible, con una agencia que fiscaliza y multas que pueden llegar al 4% de los ingresos anuales.

Durante el webinar quedó claro que prepararse para la 21.719 no es un proyecto de Legal que TI ejecuta al final. Es trabajo compartido desde el día uno. Por eso las preguntas mezclaron consentimiento con BYOD, DPO, transferencias internacionales con borrado seguro de equipos: temas legales y técnicos que en la práctica son el mismo problema visto desde dos sillas. Y casi todos, tarde o temprano, terminan sobre la mesa del equipo de TI.

Esta guía reúne esas preguntas frecuentes y las responde, sin relleno. Están ordenadas por tema para que vayas a lo que te interesa: primero el contexto (qué es la agencia, a quién aplica la ley) y después lo operativo, que es donde TI se juega la preparación: dispositivos, inventario, derechos de los titulares, proveedores y personas.

Disclaimer: esto es un resumen de lo conversado en el webinar y un punto de partida para ordenar tu programa de cumplimiento. No reemplaza asesoría legal formal para tu caso específico.

Preguntas

La Agencia y la fiscalización

Cómo funciona la APDP, quién vigila y qué tan efectivas van a ser las multas.

¿Cuál es esa agencia? ¿De quién depende?

La Agencia de Protección de Datos Personales (APDP) es un órgano autónomo descentralizado con patrimonio propio. No depende administrativamente del Ejecutivo, pero se relaciona con el Presidente de la República a través del Ministerio de Economía, Fomento y Turismo. Su dirección recae en un Consejo Directivo independiente.

¿Quién va a fiscalizar?

La Agencia de Protección de Datos Personales (APDP) es la entidad encargada. Va a poder fiscalizar de oficio o por denuncia, requerir información y documentación, hacer visitas inspectivas, ordenar medidas correctivas, iniciar procedimientos sancionatorios y aplicar multas. También lleva el Registro Nacional de Cumplimiento y aprueba modelos de prevención. En paralelo, cada empresa mantiene su responsabilidad interna y, cuando corresponda, la de su DPO.

Se ha sabido que las personas que quieren integrar esta agencia están con conflicto de intereses. ¿Crees que esto afectará el inicio en diciembre de esta ley?

La ley entra en vigencia el 1 de diciembre de 2026 independientemente de cómo se resuelvan los nombramientos del Consejo Directivo. Los cuestionamientos por conflicto de interés son un riesgo real: pueden retrasar la operatividad plena de la APDP, la aprobación de reglamentos y la capacidad fiscalizadora efectiva en los primeros meses. Pero eso no cambia la obligación de cumplir. Nuestra recomendación es no esperar a ver cómo se resuelve la agencia: las obligaciones sustantivas de la ley aplican desde el día uno y la responsabilidad civil frente al titular del dato existe con o sin fiscalizador operativo.

¿Existe dentro de la ley el perfil de los fiscalizadores, dado que deben ser altamente capacitados?

La ley entra en vigencia el 1 de diciembre de 2026 independientemente de cómo se resuelvan los nombramientos del Consejo Directivo. Los cuestionamientos por conflicto de interés son un riesgo real: pueden retrasar la operatividad plena de la APDP, la aprobación de reglamentos y la capacidad fiscalizadora efectiva en los primeros meses. Pero eso no cambia la obligación de cumplir. Nuestra recomendación es no esperar a ver cómo se resuelve la agencia: las obligaciones sustantivas de la ley aplican desde el día uno y la responsabilidad civil frente al titular del dato existe con o sin fiscalizador operativo.

Pero si no se cobran las multas por colusiones, ¿cuál será la herramienta para que las multas sí sean efectivas con esta ley?

Es una preocupación válida y compartida en el sector. Los factores que juegan a favor de la efectividad son: la APDP tiene facultades propias de cobro y ejecución, las multas son porcentuales sobre ingresos (más disuasivas que un monto fijo), se contempla registro público de sanciones (efecto reputacional), y existe responsabilidad civil paralela del titular contra la empresa. El talón de Aquiles es el mismo que en otros ámbitos: capacidad operativa del fiscalizador y voluntad política de sostener sanciones grandes. La expectativa razonable es que los primeros años se prioricen casos emblemáticos —empresas grandes, brechas visibles— para instalar el precedente, y después baje la escala.

Alcance de la ley y cruce con otras normas

A quién aplica y cómo se conecta con la Ley Marco de Ciberseguridad y con la ISO 27001.

Las alrededor de 1700 empresas que están en el listado de la Ley 21.663 (Marco de ciberseguridad) ¿están en el alcance de la ley de Protección de datos que entra en vigencia desde el 01 de diciembre?

Sí, están en el alcance —pero por vías distintas. La Ley 21.719 aplica a cualquier organización que trate datos personales de personas en Chile, sin importar si es OIV, servicio esencial o no. Que estén en el listado de la 21.663 significa que además tienen obligaciones específicas de ciberseguridad, gobernanza de incidentes y reporte a la ANCI. En la práctica los dos regímenes se cruzan: los controles técnicos que exige la ley marco de ciberseguridad ayudan a cumplir el deber de seguridad de la ley de datos, y los incidentes que comprometan datos personales van a gatillar reporte a la APDP y a la ANCI en paralelo. Nuestra recomendación es armar un solo programa de cumplimiento que responda a las dos.

¿La ISO 27001 me ayuda para estar alineado con esta ley?

Sí, la ISO 27001 es una excelente base porque instala un **Sistema de Gestión de Seguridad de la Información** con controles técnicos y organizativos que se alinean con varios requisitos de la ley: gestión de riesgos, control de accesos, cifrado, gestión de incidentes y auditorías. Pero no es suficiente por sí sola: la ley 21.719 exige obligaciones específicas de protección de datos —consentimiento, derechos ARSOP, DPO, notificación de brechas al usuario y a la agencia, evaluaciones de impacto— que la ISO 27001 no cubre por completo. La usamos como piso técnico y sumamos un programa específico de protección de datos encima.

¿Las multas en dinero también son para los servicios públicos? Y en los procesos formales de trámites como obtención de licencia de conducir o emisión de permiso de circulación, ¿se debe pedir consentimiento al usuario?

Los organismos públicos están sujetos a la ley 21.719 con reglas particulares: enfrentan responsabilidad administrativa y sanciones, aunque no siempre en el mismo régimen de multas económicas que el sector privado —para servicios públicos aplican amonestaciones, medidas correctivas y responsabilidad del funcionario. Sobre trámites como licencia de conducir o permiso de circulación: no requieren consentimiento del titular porque la base de licitud es el cumplimiento de una obligación legal y el ejercicio de potestades públicas, no el consentimiento. Sí deben cumplir con información al titular, finalidad, minimización de datos, seguridad y plazos de retención. El consentimiento solo aplica cuando no hay otra base de licitud.

No veo que se hable de que los datos deban estar almacenados dentro del territorio nacional chileno. ¿Entiendo que no hay problema en que se utilice cualquier nube con datacenter en cualquier parte del mundo?

La ley 21.719 no impone data residency general en Chile, así que en principio se puede usar nube global. Pero regula las transferencias internacionales: si el país destino no ofrece nivel de protección adecuado, hay que asegurar el traslado con instrumentos específicos —cláusulas contractuales tipo, reglas corporativas vinculantes, consentimiento explícito del titular, o alguna excepción legal—. Los grandes (AWS, Azure, GCP) ya ofrecen mecanismos para cubrir eso. Excepciones a tener en cuenta: ciertos datos sensibles o de sectores regulados (salud, sector público, financiero) pueden tener reglas específicas más estrictas. La respuesta corta: nube global sí, pero con transferencia internacional formalmente documentada.

Multas: precedentes y cómo mover a la organización

Qué muestra la experiencia europea y cómo llevar el riesgo legal al directorio.

¿Tienen evidencia de que en Europa efectivamente multaron a pymes?

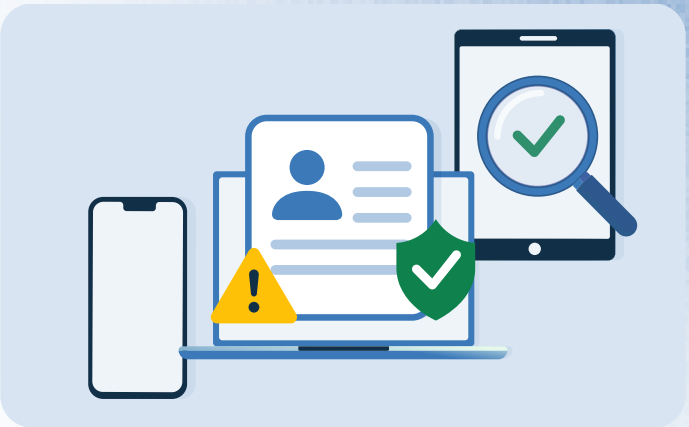
Sí, hay miles de casos registrados desde que el GDPR entró en vigencia en 2018. Las multas a pymes van desde algunos miles hasta cientos de miles de euros por prácticas comunes: falta de consentimiento en cookies, videovigilancia sin señalización, no responder solicitudes de titulares, envío de email marketing sin base legal, brechas no notificadas. La lectura importante es que las autoridades europeas han sancionado sistemáticamente a pequeñas y medianas empresas, no solo a las grandes tecnológicas. En Chile esperamos un patrón similar en los primeros años de la APDP.

¿Cómo podemos, siendo asesores legales, concientizar de manera más fuerte sobre lo crítico que es el área de TI?

El puente que mejor funciona es traducir riesgo legal a riesgo operativo con cifras. Presenta al comité o al directorio el mapa de multas (hasta 4% de ingresos anuales para infracciones gravísimas), sumado a los casos reales de GDPR contra pymes en Europa y el costo promedio de una brecha. Después baja eso a acciones concretas de TI: cifrado, control de accesos, gestión de dispositivos, borrado remoto, respuesta a incidentes. Cuando TI ve que un control técnico ausente se traduce en una multa concreta y en responsabilidad personal del directorio, la conversación cambia. Nuestra sugerencia: una matriz simple de dos columnas —obligación legal / control técnico que la satisface— firmada por Legal y por TI.

Dispositivos y endpoints: BYOD, escritorio remoto y borrado

El corazón operativo: qué hacer con cada equipo que toca datos.



¿Qué pasa cuando la empresa no tiene dispositivos sino que los trabajadores usan sus equipos personales?

El escenario BYOD no exime de responsabilidad: la empresa sigue siendo responsable del tratamiento de los datos aunque el hardware sea personal. Lo que hay que hacer es acotar el problema con reglas claras: una política BYOD firmada, separación lógica entre el perfil corporativo y el personal (perfiles de trabajo en Android, contenedores gestionados en iOS, MDM que solo toca lo laboral), cifrado obligatorio, control de accesos, borrado remoto del perfil corporativo sin tocar los datos personales del trabajador, y bloqueo de acceso a datos sensibles fuera de canales controlados. Sin ese marco, la empresa asume el riesgo entero del comportamiento del trabajador.

Según entendí, hay que proteger los datos en los servidores y también en los dispositivos. Dado eso, ¿sería una solución trabajar con equipos vacíos con toda la data en la nube (M365, por ejemplo)?

Es una estrategia razonable y bastante usada para reducir superficie de ataque, pero no elimina la obligación de proteger el dispositivo. Aunque la data viva en M365, el endpoint sigue teniendo credenciales, cachés, tokens de sesión, cookies, descargas temporales y correos locales. Un notebook perdido con acceso persistente a M365 es una brecha aunque técnicamente no guarde archivos. La regla es: cloud-first sí, pero con MDM que fuerce cifrado, MFA, bloqueo automático, borrado remoto y control de sesión. Vacío no es lo mismo que seguro.

¿Qué pasa si se pierde un dispositivo, pero que no tiene datos relacionados a la ley de datos personales?

Primero: hay que verificar de verdad que no hay datos personales, y ese ejercicio es más difícil de lo que parece. Un notebook corporativo casi siempre tiene correo, contactos, cachés, cookies, tokens que dan acceso a sistemas donde sí hay datos personales. Si después de la verificación es efectivamente un equipo sin datos y sin credenciales activas, no hay obligación de notificar por ley 21.719, pero el evento se debe registrar internamente como parte del inventario y de la gestión de incidentes. Nuestra recomendación: incluso ahí, aplicar borrado remoto por precaución y documentar la evaluación —eso protege ante una fiscalización posterior.

Si los usuarios se conectan vía escritorio remoto al dispositivo de trabajo, ¿el dispositivo desde el que se conectan también debe contar con la protección?

Sí. Aunque en teoría los datos vivan en el equipo remoto, el dispositivo desde el que se conecta genera capturas de pantalla, memoria, cachés, tokens de sesión, credenciales guardadas y descargas locales. Un keylogger o un screen recorder en el equipo cliente compromete todo el escritorio remoto. La regla es: cualquier dispositivo que sea puerta de entrada a datos personales de la empresa entra en el alcance de las obligaciones de seguridad, cifrado, control de accesos y respuesta a incidentes. Eso vale también para BYOD conectado por RDP.

¿Qué se debe cumplir con los dispositivos que no contienen data sensible pero trabajan vía RDP (Escritorio Remoto) sobre dispositivos que sí tienen data sensible?

Aunque el dispositivo no almacene la data, es el eslabón que abre la puerta al sistema donde sí está —y ese acceso es lo que hay que proteger. Los mínimos: MFA fuerte para el acceso remoto, cifrado del canal (RDP sobre VPN o gateway con TLS), políticas de sesión con timeout y bloqueo automático, prohibición de guardar credenciales localmente, deshabilitar el redireccionamiento de dispositivos y portapapeles cuando no sea imprescindible, monitoreo y logging del acceso remoto, y control del dispositivo cliente (parche, antimalware, cifrado de disco). Un cliente con acceso RDP a un servidor con datos sensibles es una brecha lista para ocurrir.

¿Cómo se puede demostrar el borrado de un equipo, incluso de manera local como un simple formateo? ¿Cómo se certifica eso?

Un formateo simple no es evidencia suficiente ni cumple estándar. Lo que se pide es borrado seguro y certificable: uso de herramientas que ejecuten sobrescritura conforme a estándares (NIST SP 800-88, DoD 5220.22-M), o destrucción física del medio para datos sensibles. La evidencia se materializa en un certificado de borrado con: identificador del equipo (número de serie), fecha, método usado, operador responsable, resultado y firma. Las plataformas de MDM/ gestión de dispositivos generan este certificado automáticamente al ejecutar un wipe remoto. Ese certificado es lo que se muestra en una fiscalización o ante un titular que ejerce derecho de supresión.

Inventario, logs y trazabilidad

Cómo saber qué tienes, dónde está y quién lo tocó.

Cuando hablas de inventario vivo, ¿a qué te refieres exactamente? ¿Un sistema que controle otro sistema?

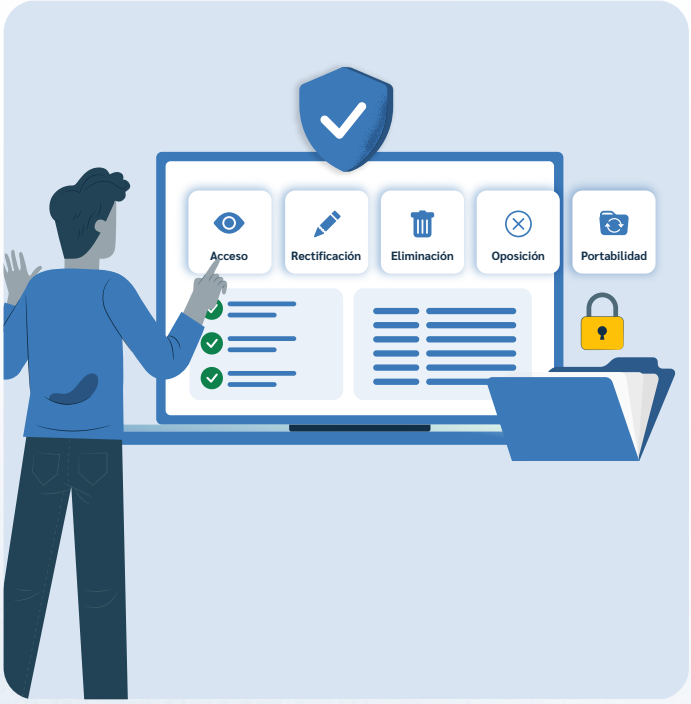
Inventario vivo es un registro actualizado en tiempo real de qué activos tienes, dónde están, quién los usa y qué datos personales manejan. No es una planilla estática de Excel actualizada una vez al año —eso muere el primer día. Es un sistema que se sincroniza automáticamente con las fuentes de verdad: MDM para dispositivos, IAM para identidades, la nube para servicios, HR para bajas. Cuando alguien recibe un notebook, se instala software o se da de baja a un colaborador, el inventario se actualiza solo. Es la única forma de responder a la APDP en un plazo razonable qué datos tenías, dónde y quién los accedió cuando pasa algo.

¿Tienen evidencia de que en Europa efectivamente multaron a pymes?

La ley 21.719 no fija un plazo específico para logs, pero sí exige demostrar cumplimiento del principio de responsabilidad proactiva y del deber de seguridad. En la práctica, la retención debe ser suficiente para: investigar incidentes, atender solicitudes ARSOP, responder a fiscalizaciones y demostrar trazabilidad de accesos y borrados. La referencia que estamos usando en el mercado es entre 1 y 2 años para logs de acceso y actividad, y hasta 5 años para registros vinculados a decisiones automatizadas o consentimiento. Importante: cuidado con retener logs que a su vez contengan datos personales sin base de licitud —eso también hay que declararlo y proteger.

Derechos de los titulares (ARSOP) y consentimiento

Cómo recibir y responder solicitudes, y qué pasa con los datos ya publicados.



Para cumplir las solicitudes ARSOP+, ¿debemos implementar algún sistema para recibir y gestionar estas solicitudes?

Sí. La ley obliga a habilitar canales claros, gratuitos y accesibles para que los titulares ejerzan sus derechos, y a responder en plazos definidos (generalmente 30 días, extensible con justificación). Con volumen bajo se puede empezar con un formulario web + casilla dedicada + workflow interno documentado. A partir de cierto volumen es imprescindible un sistema que registre solicitud, verifique identidad, orqueste la búsqueda en todos los sistemas donde vive el dato, ejecute la acción (acceso, rectificación, supresión, oposición, portabilidad), guarde evidencia y mida SLA. Ese registro es también la prueba de cumplimiento ante fiscalización.

Me parece que la implementación para TI implica muchas cosas más, como implementación de cookies, proceso de solicitudes ARCO automatizadas, etc.

Exacto, y esa es una de las conclusiones más importantes: la ley no se resuelve con un contrato ni con una política publicada. Es un programa transversal que toca cookies y consent management en frontend, orquestación automatizada de solicitudes ARSOP en backend, inventario de tratamientos, DPO, gestión de proveedores con DPA, evaluaciones de impacto, notificación de brechas, capacitación, y todo el aparato técnico de seguridad. Nuestra sugerencia es armar un roadmap por olas: primero base legal + inventario + canal ARSOP + seguridad mínima, después automatización de consent y ARSOP, después el análisis de cumplimiento y una auditoría continua.

¿Qué pasa con los datos que existen en internet? Porque uno puede buscar el RUT de las personas y sale el nombre y dirección.

Esos datos filtrados no dejan de ser datos personales por estar publicados: la ley 21.719 sigue aplicando. Cualquier sitio, servicio o base que los recopile y los siga tratando necesita una base de licitud —consentimiento del titular o alguna de las excepciones legales— y el titular puede ejercer sus derechos ARSOP para pedir eliminación, oposición o rectificación. La APDP va a poder ordenar el borrado a esos operadores. El hecho de que hoy circulen libremente no es una autorización tácita, y ese va a ser justamente uno de los focos de fiscalización más visibles en el arranque.

Proveedores, encargados y el rol de Prey

Qué exige la ley a tu cadena de proveedores, y dónde encaja una plataforma como Prey.

¿Qué ocurre cuando se utilizan plataformas internacionales de operaciones, pero están en representación de la empresa? ¿Quién debe encargarse de eliminar esa información?

La responsabilidad frente al titular es siempre del responsable del tratamiento —la empresa que decide qué datos se recolectan y para qué—, sin importar si la operación técnica se hace en una plataforma internacional. Esa plataforma opera como encargado (procesador), y su relación tiene que estar regulada por un contrato de tratamiento de datos (DPA) que la obligue a atender solicitudes de eliminación, aplicar medidas de seguridad y notificar incidentes. Cuando llega un ARSOP, la empresa responde al titular y en paralelo instruye al proveedor para ejecutar el borrado. Si el proveedor no lo hace, la empresa igual responde: por eso el DPA y la auditoría de proveedores son críticos.

Importante contar con un DAP con terceros que procesan nuestros datos.

Exacto. El contrato de tratamiento de datos —**DPA o DAP**— es una obligación explícita cuando compartes datos con encargados (proveedores que procesan por cuenta tuya). Los mínimos que tiene que fijar son: objeto y finalidad del tratamiento, categorías de datos y titulares, duración, medidas de seguridad, subprocesadores autorizados, obligación de asistencia en solicitudes ARSOP, notificación de incidentes con plazo definido, cooperación en auditorías, y devolución o eliminación de datos al terminar el contrato. Sin DPA, si el proveedor tiene una brecha, la empresa asume la responsabilidad íntegra. Nuestra recomendación: inventario de todos los proveedores que tocan datos y verificación de que cada uno tiene DPA firmado y vigente.

Para gestionar a los proveedores externos, ¿debe ser por contrato con ellos y que ellos demuestren cumplimiento?

Sí, y es una obligación exigible. La gestión de proveedores tiene tres capas: contractual (**DPA** con los mínimos que exige la ley), documental (que el proveedor demuestre cumplimiento —certificaciones ISO 27001, SOC 2, políticas de seguridad, resultados de auditoría, prueba de que tiene DPO si aplica) y operativa (derecho de auditoría, revisión periódica de subprocesadores, evaluación de riesgos en la contratación y en cada renovación). Los proveedores críticos —los que tocan volúmenes grandes o datos sensibles— requieren evaluación de impacto en privacidad antes de contratar. La cadena es tan fuerte como su eslabón más débil: si el proveedor falla, respondes tú.

¿Qué sucede con los datos que son respaldados para casos de pruebas de DRP, además algunos son almacenados fuera de la empresa, en nubes privadas?

Los respaldos DRP son tratamiento de datos personales y aplican todas las obligaciones de la ley: base de licitud, finalidad clara (continuidad operacional), plazo de retención definido, cifrado en reposo y en tránsito, control de accesos, registro en el inventario de tratamientos y —si están en nube externa— DPA con el proveedor. Si el datacenter está fuera de Chile, sumas la obligación de transferencia internacional. Un punto delicado: si un titular ejerce el derecho de supresión, la empresa debe garantizar que el borrado alcanza también los respaldos, aunque sea con un ciclo diferido. Ese detalle hay que dejarlo escrito en la política.

¿Lo que Prey sugiere en la presentación es un MDM?

Prey es una plataforma de gestión y seguridad de dispositivos que cubre buena parte de lo que se espera de un **MDM tradicional** —inventario, geolocalización, bloqueo y borrado remoto, control de accesos, alertas de movimiento— con foco especial en protección de datos y respuesta ante pérdida o robo. Dependiendo del stack de la empresa, funciona como MDM completo o como capa complementaria a un MDM existente (Intune, Jamf) que suma capacidades específicas de protección de datos y trazabilidad. Para cumplir la 21.719 lo importante no es la etiqueta sino que estén cubiertas las funciones: control, visibilidad, borrado y evidencia.

¿Qué pasa si contrato Prey y en una fiscalización Prey tiene un error?

Frente a la APDP y al titular del dato, la responsable sigue siendo la empresa que contrató el servicio —el responsable del tratamiento— porque es quien decide para qué se usan los datos. Prey opera como encargado del tratamiento y tiene sus propias obligaciones legales y contractuales: seguridad, notificación de incidentes, cumplimiento del DPA, auditorías. Si el error es atribuible a Prey, la empresa puede repetir contra nosotros por vía civil y contractual, y el DPA fija responsabilidades y coberturas. Nosotros trabajamos con controles certificados, auditorías externas y cláusulas de responsabilidad explícitas justamente para dar respaldo formal a nuestros clientes en ese escenario.

Si contratan sus servicios para que protejan los datos de mi empresa, ¿quién protege mis datos de ustedes?

Buena pregunta y es la que hay que hacerle a todo proveedor. Nuestro compromiso es concreto: encriptación en tránsito y en reposo, controles de acceso mínimos y auditados, separación estricta entre datos de clientes, cumplimiento con estándares internacionales de seguridad, ubicación de infraestructura documentada, y un DPA que fija con claridad qué hacemos con la información, por cuánto tiempo, y bajo qué condiciones se elimina. Recibimos auditorías de nuestros clientes y publicamos nuestra postura de seguridad y privacidad. En corto: los datos de tu empresa son de tu empresa —nosotros somos custodios técnicos con obligaciones contractuales y legales exigibles.

Personas: offboarding, roles y cultura

El factor humano: desvinculaciones, quién responde y cómo sostenerlo en el tiempo.

¿Qué pasa si el trabajador, al ser desvinculado, antes de entregar, borra datos de la empresa?

Es un escenario que hay que anticipar con controles, no reaccionar después. Los datos de la empresa deberían estar respaldados en la nube o en repositorios centrales, no vivir solo en el equipo. El proceso de desvinculación debe cortar accesos primero, bloquear el dispositivo remotamente si es necesario, y recién después coordinar la entrega. Si aún así el trabajador logró borrar información, hay dos frentes: laboral (incumplimiento contractual, eventual acción civil o penal por daño patrimonial) y de datos (si borró datos personales de clientes, la empresa sigue siendo responsable frente a los titulares por no haber tenido respaldo). La lección: la política de offboarding es un control clave para 21.719.

Si el usuario, al ser desvinculado, borra información de la empresa, ¿cómo lo toma la ley?

Desde el ángulo estricto de la ley 21.719, la empresa sigue siendo responsable del tratamiento frente a los titulares cuyos datos se perdieron: si por ese borrado la empresa ya no puede atender un ARSOP, cumplir una obligación de conservación, o responder por un incidente, la responsabilidad es de la empresa, no del ex-trabajador. Frente al titular no vale como excusa que fue un tercero. En paralelo, contra el trabajador queda la vía laboral, civil (daño patrimonial) y eventualmente penal según el tipo y volumen de datos. La ley empuja a las empresas a tener respaldos y controles de offboarding para que este borrado sea imposible o rápidamente reversible.

¿El responsable debe ser TI local o estar en Chile? ¿Qué pasa con las empresas transnacionales que tienen su oficial de seguridad en casa matriz global?

La ley aplica al tratamiento de datos de personas en Chile, sin importar dónde esté físicamente el responsable. Para empresas transnacionales sin establecimiento en Chile la ley exige designar un representante local, que es el punto de contacto formal con la APDP y con los titulares. El DPO (Delegado de Protección de Datos) puede estar en casa matriz siempre que sea accesible en horario razonable para Chile, hable español o cuente con canal en español, y tenga autonomía real de decisión. Nuestra recomendación práctica para multinacionales: DPO global + oficial de cumplimiento local, con roles y matriz de escalamiento documentados.

Siempre va a haber equipos personales nuevos que no alcanzan a estar monitoreados. Importante capacitar y modificar el reglamento interno de la organización.

Totalmente de acuerdo. Ningún control técnico funciona sin marco normativo interno y sin cultura. Las tres piezas clave son: reglamento interno actualizado que incluya deberes de protección de datos, uso aceptable de dispositivos, BYOD y consecuencias del incumplimiento; capacitación obligatoria y recurrente con evidencia de asistencia y comprensión (no basta un correo); y un onboarding técnico que en el mismo momento de la incorporación instale controles mínimos —MDM, cifrado, MFA— antes de dar acceso a datos. Sin eso, siempre va a existir la ventana que mencionas, y esa ventana es donde ocurren los incidentes.

La ley llega en diciembre. Empieza desde ya.

Si algo quedó del webinar, es esto: la Ley 21.719 no se resuelve con un contrato firmado ni con una política publicada en la intranet. Es un programa transversal que toca el frontend (cookies, consentimiento), el backend (solicitudes ARSOP, inventario de tratamientos), la infraestructura (cifrado, control de accesos, borrado certificable) y a las personas (DPO, capacitación, offboarding).

La buena noticia es que no hay que hacerlo todo el 1 de diciembre. Se ordena por olas: primero la base legal, el inventario de datos, el canal de solicitudes y la seguridad mínima; después la automatización del consentimiento y de ARSOP; y encima, la auditoría continua.

Y un consejo que repetimos toda la sesión: no esperes a ver cómo resuelve la agencia. Las obligaciones aplican desde el día uno y la responsabilidad frente al titular del dato existe con o sin fiscalizador operativo. Los que empiezan hoy llegan con margen; los que esperan, llegan corriendo.

En Prey ayudamos con la protección y visibilidad de tu flota de dispositivos, control de accesos, borrado remoto certificable y evidencia para cuando toque demostrar cumplimiento. Si quieres ver cómo se ve eso sobre tu propia flota, conversémoslo.

¿Te quedaron dudas sobre tu caso puntual?

Habla con nuestra especialista en el tema Camila Burgos, quien lideró el webinar. Te ayudaremos a ordenar por dónde partir con la preparación de tu equipo.

Conversemos | **camila@preyproject.com** | **+56 9 92321671**

Sobre Prey

Nacimos en 2009 con una misión clara: devolverle a las personas el control sobre su tecnología. Hoy, Prey ha evolucionado en una **plataforma integral de gestión y seguridad para flotas globales**. Más allá del rastreo, empoderamos a las empresas con herramientas avanzadas para el manejo de software, cumplimiento de políticas y protección de datos.

Somos el aliado estratégico que ayuda a administrar y proteger entornos de trabajo remoto, facilitando el cumplimiento normativo. Un equipo comprometido con la continuidad de tu operación.

Prey para: **Personas** | **Organizaciones** | **Escuelas y Universidades**