SOVOS

Ley de Protección de Datos en Chile: las claves del nuevo marco regulatorio

Una guía para comprender los principales cambios de la Ley 21.719 y su impacto en gobernanza de datos, ciberseguridad, IA y confianza digital.

Resumen ejecutivo

- La nueva **Ley de Protección de Datos N° 21.719** moderniza el marco regulatorio chileno y lo acerca a estándares internacionales como el GDPR.
- La normativa fortalece los derechos de las personas y establece mayores obligaciones de transparencia, seguridad y responsabilidad para las organizaciones.
- La creación de una autoridad fiscalizadora transforma el cumplimiento en una exigencia concreta, respaldada por mecanismos de supervisión y sanción.
- La ley impulsa un nuevo modelo de confianza digital basado en gobernanza, trazabilidad y uso responsable de los datos.

El nuevo valor de los datos en la economía digital

En la economía digital, los datos personales se han convertido en uno de los activos más valiosos para las organizaciones. Desde la personalización de servicios hasta la toma de decisiones basada en analítica, su uso está en el centro de prácticamente todas las industrias.

Este crecimiento también ha expuesto riesgos cada vez más visibles. Casos de fraude, filtraciones de información y uso indebido de datos han evidenciado una brecha crítica: las personas muchas veces desconocen quién tiene su información, cómo la obtuvo o para qué la utiliza.

En Chile, la normativa vigente desde 1999 —Ley 19.628 sobre protección de la vida privada—
quedó rezagada frente a un entorno digital más complejo y dinámico. En ese contexto surge la nueva Ley de Protección de Datos, con el objetivo de fortalecer los derechos de las personas y establecer reglas más claras para el tratamiento de la información.

¿Qué es la Ley de Protección de Datos en Chile?

La nueva Ley de Protección de Datos N° 21.719 reforma la normativa anterior introduciendo un marco actualizado para responder a los desafíos de la economía digital. En concreto, busca regular cómo las organizaciones recopilan, utilizan, almacenan y protegen los datos personales, estableciendo derechos para las personas y obligaciones para quienes los tratan.

Alcance de la normativa

La ley regula todo el ciclo de vida de los datos personales, desde su recolección, uso, almacenamiento y transferencia, hasta su eliminación. Asimismo, establece las condiciones bajo las cuales estas actividades son lícitas y las responsabilidades que deben asumir las organizaciones que realizan el tratamiento.

¿A quién aplica la ley?

La normativa tiene un alcance amplio y aplica tanto a empresas privadas como a organismos públicos, proveedores y terceros que procesan datos personales. En la práctica, cualquier organización que trate datos personales en Chile deberá evaluar sus procesos y adecuarse a las nuevas exigencias.

¿Qué es un dato personal?

Un dato personal es cualquier información que permite identificar directa o indirectamente a una persona, incluyendo el nombre, DNI o RUT, correo electrónico, datos biométricos e identificadores digitales, entre otros.

Del dato como activo al dato como derecho

Uno de los cambios más relevantes es que los datos personales dejan de ser vistos únicamente como un activo para las organizaciones y pasan a reconocerse como un derecho de las personas.

Esto implica que las empresas deben justificar la recolección de datos, limitar su uso a finalidades específicas, proteger la información adecuadamente y facilitar el ejercicio de los derechos de los titulares. En este nuevo marco, el tratamiento de datos debe ser legítimo, transparente y proporcional.

¿Por qué era necesaria una nueva ley?

Durante más de dos décadas, Chile operó con una normativa que fue pionera en su momento, pero que quedó rezagada frente a la digitalización, el crecimiento del comercio electrónico y el uso masivo de datos personales. La Ley N° 21.719 busca responder a esos desafíos mediante un marco regulatorio alineado con la realidad digital actual.

Al mismo tiempo aumentaron riesgos como el fraude digital, las filtraciones de información y el uso poco transparente de datos, en un escenario en el que las personas podían ejercer un control muy limitado sobre su información.

A ello se sumaba la necesidad de acercar el marco regulatorio chileno a estándares internacionales de protección de datos y fortalecer los mecanismos de supervisión y cumplimiento.

> **La nueva ley busca sentar las bases para un entorno digital más transparente, seguro y confiable, donde la protección de los datos personales sea parte integral de la relación entre organizaciones y ciudadanos.**

Roberto Guerrero
Counsel LATAM Commercial, Sovos.

¿Qué cambia con la nueva Ley de Protección de Datos?

La nueva Ley de Protección de Datos en Chile introduce un cambio estructural en la forma en que se gestionan los datos personales. Entre los cambios más relevantes destacan los siguientes:

De normativa declarativa a exigible: uno de los cambios más relevantes es el paso desde un marco principalmente declarativo a uno con mecanismos efectivos de supervisión y cumplimiento. La nueva normativa incorpora una autoridad especializada, procedimientos administrativos y sanciones concretas frente a incumplimientos.

De la acumulación de datos al uso justificado: la ley abandona la lógica de recolectar información de manera indiscriminada y exige que el tratamiento responda a finalidades específicas y legítimas. Esto incorpora principios como minimización, proporcionalidad y eliminación de datos cuando dejan de ser necesarios.

De la opacidad a la transparencia: las organizaciones deberán informar de forma clara qué datos recopilan, con qué propósito los utilizan, cuánto tiempo los conservan y cómo pueden las personas ejercer sus derechos.

De la reacción a la prevención (privacy by design): la protección de datos deja de abordarse únicamente cuando ocurre un incidente. La nueva normativa promueve la incorporación de medidas preventivas siguiendo principios como privacy by design o privacidad desde el diseño, que exige a las organizaciones incorporar la protección de los datos personales desde la fase inicial de diseño de un producto, sistema o servicio.

Supervisión centralizada: la creación de una autoridad especializada permitirá fiscalizar el cumplimiento de la ley, emitir lineamientos, gestionar reclamaciones y aplicar sanciones, fortaleciendo la consistencia y efectividad del sistema.

Del control organizacional al control del titular: la ley fortalece los derechos de las personas, otorgándoles mayor visibilidad sobre el uso de sus datos y la posibilidad de exigir mayor transparencia y responsabilidad a las organizaciones que los tratan.

Derechos de las personas sobre sus datos personales

Uno de los pilares de la nueva Ley de Protección de Datos en Chile es el fortalecimiento de los derechos de las personas sobre su información. El cambio es relevante: los titulares dejan de tener un rol pasivo y pasan a contar con mecanismos concretos para conocer, corregir, limitar o eliminar el uso de sus datos personales.

Derechos ARCO ampliados

Los derechos de los titulares, conocidos tradicionalmente como derechos ARCO, garantizan a las personas la posibilidad de decidir sobre el uso de su propia información.

Entre los principales derechos se encuentran:

- **Acceso:** saber qué datos tiene una organización y cómo los utiliza.
- **Rectificación:** corregir información incorrecta o desactualizada.
- **Cancelación o Supresión:** solicitar la eliminación de datos cuando ya no sean necesarios.
- **Oposición:** negarse al uso de datos en determinados contextos.
- **Portabilidad:** trasladar los datos de una organización a otra.
- **Bloqueo:** limitar temporalmente el uso de la información.

Transparencia, consentimiento y respuesta operativa

Para que estos derechos sean ejercibles, las organizaciones deberán informar de forma clara qué datos recopilan, con qué finalidad los utilizan, durante cuánto tiempo los conservan y cómo pueden las personas ejercer sus derechos.

El consentimiento adquiere un estándar más exigente: para ser válido, debe ser libre, informado, específico, inequívoco y, en todo momento, revocable por el titular.

Esto obliga a las empresas a contar con canales visibles, procesos internos definidos y coordinación entre áreas para responder solicitudes dentro de los plazos legales. La gestión de derechos deja de ser un proceso informal y pasa a convertirse en una obligación operativa.

Obligaciones de las organizaciones

La nueva Ley de Protección de Datos en Chile no solo fortalece los derechos de las personas. También redefine el rol de las organizaciones, que deberán gestionar los datos personales con mayor control y responsabilidad.

Gobernanza de datos y bases legales

Uno de los primeros desafíos será entender qué datos personales maneja la organización, dónde se almacenan, quién accede a ellos, con qué finalidad se utilizan y con quién se comparten. Este ejercicio de inventario o mapeo de datos es la base de cualquier estrategia de cumplimiento.

A partir de esa visibilidad, las empresas deberán definir roles, responsabilidades, políticas internas y criterios claros para la toma de decisiones. También deberán identificar la base legal que justifica cada tratamiento. El consentimiento es una de las más relevantes, pero no la única; cuando se utilice, deberá cumplir con los estándares establecidos por la ley.

Gestión de derechos, terceros e incidentes

Las organizaciones deberán implementar mecanismos efectivos para responder a las solicitudes de los titulares. Esto requiere canales accesibles, procesos documentados y coordinación entre áreas legales, tecnológicas, comerciales y de atención al cliente.

La responsabilidad también se extiende a proveedores y terceros que participan en el tratamiento de datos personales. Por ello, será necesario revisar contratos, exigir garantías adecuadas y supervisar el tratamiento externalizado.

Finalmente, la protección de datos exige medidas técnicas y organizativas proporcionales al riesgo. Esto implica proteger la información frente a accesos no autorizados, detectar incidentes, gestionarlos oportunamente y notificar cuando corresponda.

Durante años se dijo que los datos eran el nuevo petróleo. Hoy, con el avance de la inteligencia artificial, esa afirmación cobra más fuerza que nunca. Los datos se han convertido en uno de los activos más importantes de las organizaciones, y la forma en que una empresa los gestione marcará su estrategia, su capacidad para innovar y la eficiencia de su negocio.

Sergio Severo
Managing Director LATAM, Sovos

La Agencia de Protección de Datos en Chile

Uno de los cambios más relevantes de la nueva ley es la creación de una autoridad especializada: la Agencia de Protección de Datos Personales. Su existencia marca el paso desde un modelo principalmente declarativo hacia un sistema con fiscalización efectiva.

La agencia tendrá facultades para supervisar el cumplimiento de la normativa, recibir reclamos de los titulares, investigar infracciones, emitir lineamientos y aplicar sanciones cuando corresponda.

Para las organizaciones, esto introduce un nuevo nivel de exigencia. Las prácticas internas podrán ser revisadas, las decisiones sobre datos deberán estar justificadas y los procesos deberán ser demostrables.

En este escenario, las empresas deberán probar que cumplen. Esto implica anticiparse, documentar decisiones, fortalecer la trazabilidad y adoptar una lógica preventiva frente al tratamiento de datos personales.

GDPR y Ley de Protección de Datos en Chile: similitudes y diferencias

La nueva Ley de Protección de Datos en Chile forma parte de una tendencia global hacia marcos regulatorios más exigentes en materia de protección de datos personales. En ese proceso, el Reglamento General de Protección de Datos de la Unión Europea (GDPR) es una de las principales referencias.

Ambos marcos comparten principios relevantes: reconocen que los datos personales pertenecen a las personas, fortalecen los derechos de los titulares, elevan el estándar de transparencia y exigen medidas de seguridad acordes al riesgo.

También comparten el principio de responsabilidad demostrable, o accountability. Esto significa que, además de cumplir con la ley, las organizaciones deben ser capaces de acreditar que cuentan con procesos, controles y criterios adecuados para gestionar los datos personales.

La principal diferencia está en el nivel de madurez regulatoria. El GDPR cuenta con años de aplicación, criterios interpretativos consolidados y una práctica regulatoria activa. En cambio, la ley chilena comienza ahora su proceso de implementación, por lo que su alcance práctico se irá definiendo progresivamente a partir del rol de la Agencia y de los casos que se presenten.

Para las organizaciones con operaciones internacionales, el desafío será mantener estándares consistentes de protección de datos en distintas jurisdicciones.

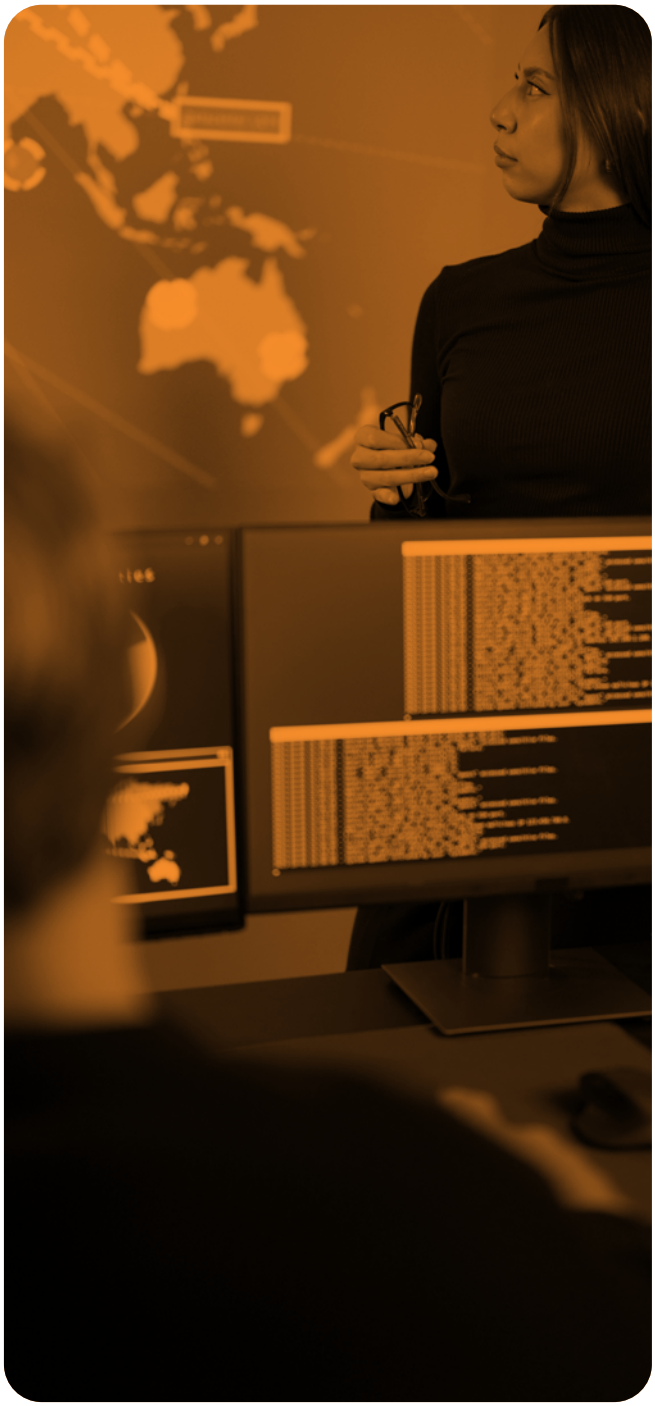
Ciberseguridad y protección de datos

Hablar de Ley de Protección de Datos en Chile sin hablar de ciberseguridad es incompleto. No es suficiente definir cómo deben tratarse los datos personales si no existen medidas para protegerlos frente a accesos no autorizados, filtraciones o usos indebidos.

Del cumplimiento legal a la gestión de riesgos

Durante años, muchas organizaciones abordaron la protección de datos desde una perspectiva principalmente legal o documental. En la actualidad, los datos personales se han convertido en uno de los principales objetivos de ataques cibernéticos, y los incidentes pueden generar impactos económicos, reputacionales, regulatorios y operativos.

La nueva normativa exige medidas técnicas y organizativas acordes al riesgo del tratamiento. No se trata de aplicar una lista única de controles, sino de justificar que las medidas implementadas son proporcionales al tipo de datos, al contexto y a los riesgos involucrados.



En la práctica, esto implica avanzar en cuatro capacidades clave:

- **Identificación de riesgos**: entender dónde están los datos personales y qué tan expuestos se encuentran.
- **Controles técnicos y organizativos:** implementar medidas que reduzcan la probabilidad de accesos indebidos o filtraciones.
- **Monitoreo continuo**: detectar comportamientos anómalos, accesos no autorizados o vulnerabilidades.
- **Respuesta ante incidentes:** contar con procedimientos para contener, analizar, recuperar y notificar cuando corresponda.

Protección de datos desde el origen

La protección de datos y la ciberseguridad no deberían abordarse como disciplinas separadas. La seguridad debe incorporarse desde las etapas iniciales de diseño y operación de procesos, productos y servicios, considerando todo el ciclo de vida de la información.

Esto implica que cada decisión sobre datos —desde la recolección hasta la eliminación— contemple no solo su uso, sino también su protección.

En este contexto, la resiliencia organizacional se vuelve clave. No se trata únicamente de evitar incidentes, sino de desarrollar la capacidad de anticiparlos, responder adecuadamente y recuperarse con rapidez cuando ocurren.

Inteligencia artificial y protección de datos

La inteligencia artificial también impacta en la forma en que las organizaciones recopilan, procesan y utilizan datos personales.

Mientras más sofisticados son los sistemas, mayor suele ser su dependencia de grandes volúmenes de información. Esto amplifica tanto el valor de los datos como los riesgos asociados a su uso.

IA y tratamiento de datos personales

La IA permite automatizar procesos que antes dependían de intervención humana, desde la verificación de identidad hasta la segmentación de clientes, la detección de fraude o la evaluación de riesgos.

Este escenario amplía el alcance de la protección de datos: además de almacenar la información de forma segura, las organizaciones deben comprender cómo se utiliza para tomar decisiones que pueden afectar a las personas.

Riesgos, transparencia y explicabilidad

El uso de datos en sistemas automatizados puede generar riesgos como sesgos, discriminación, opacidad o decisiones difíciles de explicar. En muchos casos, las personas no saben que están siendo evaluadas por un algoritmo ni cómo se llega a determinados resultados.

Por eso, la transparencia adquiere un rol central. Las organizaciones deberán ser capaces de explicar, en términos comprensibles, cómo utilizan datos personales en sistemas de IA, sin que ello implique revelar detalles técnicos o algoritmos propietarios.

Gobernanza para una IA responsable

La adopción de IA exige fortalecer los modelos de gobernanza de datos.
Esto implica definir qué información puede utilizarse, con qué propósito, bajo qué controles y quién responde por los resultados generados.

También exige revisar la calidad de los datos utilizados, la existencia de sesgos, los criterios de supervisión humana y los mecanismos para corregir errores.

La inteligencia artificial puede mejorar procesos, fortalecer la detección de fraude y generar nuevas eficiencias operativas, pero requiere un equilibrio entre innovación y responsabilidad.
La confianza dependerá de que las organizaciones puedan demostrar que usan estas tecnologías de forma segura, transparente y alineada con la protección de datos personales.

Cómo prepararse para cumplir la Ley de Protección de Datos en Chile

Cumplir con la Ley de Protección de Datos no es un proyecto puntual, sino un proceso continuo que requiere estructura, coordinación y una mirada estratégica, donde las organizaciones deberán integrar la protección de datos en su operación diaria.

Algunas prácticas clave permiten avanzar en esa dirección:

Inventario y entendimiento de datos

El primer paso es tener claridad sobre qué datos personales maneja la organización, con qué finalidad se recopilan, dónde se almacenan, quién tiene acceso y durante cuánto tiempo se conservan.

Sin esta visibilidad, cualquier esfuerzo posterior se construye sobre una base incompleta. A partir de este diagnóstico, resulta posible definir responsabilidades, establecer políticas internas y construir una gobernanza de datos que permita tomar decisiones de manera consistente y demostrar cumplimiento frente a la autoridad.

Privacidad y seguridad desde el diseño

Cada nuevo proceso, producto o servicio debería considerar desde el inicio cómo se recopilarán, utilizarán, protegerán y eliminarán los datos personales. Esto permite reducir riesgos antes de que se conviertan en problemas operativos o regulatorios.

Gestión de derechos y terceros

Las organizaciones deberán contar con canales claros para atender solicitudes de los titulares y procesos internos para responder dentro de los plazos legales. También deberán extender sus estándares de protección a proveedores y terceros que participen en el tratamiento de datos.

Seguridad continua y cultura interna

Las medidas de seguridad deben actualizarse de forma permanente, considerando nuevas amenazas, cambios tecnológicos y riesgos operativos. Al mismo tiempo, resulta fundamental que las personas comprendan su rol en la protección de los datos, mediante capacitación continua y responsabilidades claramente definidas.

Cuando las personas dentro de la organización entienden el valor de los datos y los riesgos asociados, el cumplimiento deja de ser una obligación aislada y se transforma en una práctica cotidiana.

> **Las organizaciones pueden enfrentar los cambios regulatorios de forma reactiva o aprovecharlos para transformarse. La verdadera oportunidad no está solo en cumplir la ley, sino en utilizar ese proceso para fortalecer la estrategia del negocio.**
>
> **Sergio Severo**
> Managing Director LATAM, Sovos

Lecciones para construir confianza digital en la nueva era de los datos

Aprendizajes del Sovos Digital Trust Summit 2026

A medida que las organizaciones avanzan en la implementación de la Ley de Protección de Datos en Chile, surgen desafíos que van mucho más allá del cumplimiento normativo.

¿Cómo se gestiona el consentimiento en entornos digitales complejos? ¿Qué implica demostrar cumplimiento? ¿Cómo se integran ciberseguridad e inteligencia artificial?

Estas preguntas ya están siendo abordadas por empresas, expertos y reguladores.

Los siguientes aprendizajes surgen de las conversaciones desarrolladas durante el **Sovos Digital Trust Summit 2026,** un espacio de reflexión sobre los desafíos que plantea la nueva regulación y su impacto en la construcción de confianza digital.

Si existe un elemento común entre todas las discusiones, es que la protección de datos dejó de ser un tema exclusivamente regulatorio. Hoy involucra decisiones de negocio, cultura organizacional, tecnología, gestión de riesgos y construcción de confianza.

Estos son algunos de sus principales insights.

1. La nueva ley redefine la relación de las organizaciones con los datos personales

Nueva Ley de Protección de Datos: ¿Cómo deben prepararse las empresas?

La nueva Ley de Protección de Datos responde a un cambio profundo en la forma en que las organizaciones utilizan la información personal. En un entorno donde los datos se han convertido en un activo estratégico para la economía digital, la normativa introduce nuevas obligaciones para las organizaciones y fortalece los derechos de las personas sobre su información.

Como planteó Javier Carreras, VP, Global Commercial & DPO en Sovos, al abrir la conversación, el desafío para las organizaciones, más allá de comprender una nueva regulación, está en prepararse para un cambio que impacta procesos, tecnología, gobernanza y cultura organizacional.

A partir de esa premisa, los panelistas abordaron los principales desafíos que plantea la implementación de la ley.

Las organizaciones dejan de ser dueñas de los datos para convertirse en responsables de su tratamiento: La nueva normativa modifica la forma en que las organizaciones se relacionan con los datos personales. Estos dejan de entenderse como un activo propio para convertirse en información cuyo tratamiento debe justificarse, protegerse y documentarse. Esto supone un cambio en las responsabilidades de las organizaciones, que deberán demostrar que el tratamiento de los datos respeta los derechos de las personas y cumple con las obligaciones establecidas por la ley.

> **Los datos personales dejaron de ser un activo de las organizaciones para convertirse en información sobre la cual tienen responsabilidades. Ya no basta con utilizarlos: las empresas deben rendir cuentas sobre cómo los obtienen, cómo los protegen y para qué los utilizan.**

Marcelo Drago
Presidente de AGPD y socio de DataCompliance

La confianza digital requiere trazabilidad y transparencia: la nueva normativa fortalece los derechos de los titulares y exige a las organizaciones contar con mecanismos que permitan identificar y documentar el tratamiento de los datos personales. Esa trazabilidad será fundamental para responder al ejercicio de los derechos que reconoce la ley y acreditar el cumplimiento de las obligaciones que esta establece.

> **La nueva ley busca devolver a las personas el control sobre su información. Reduce la asimetría entre organizaciones y titulares de los datos, permitiendo saber quién los utiliza, con qué finalidad y durante cuánto tiempo.**

Roberto Guerrero
Counsel LATAM Commercial, Sovos

La adecuación comienza con un diagnóstico, no con la tecnología: antes de evaluar herramientas o proyectos tecnológicos, el primer paso consiste en comprender qué datos existen dentro de la organización, dónde se encuentran, quién tiene acceso a ellos, bajo qué base legal son tratados y qué brechas deben abordarse para cumplir con la normativa. Este trabajo requiere revisar procesos, identificar responsables y coordinar a las distintas áreas involucradas en el tratamiento de los datos personales. Sin ese diagnóstico inicial, cualquier estrategia de cumplimiento corre el riesgo de quedarse en el plano documental y no generar cambios reales.

La lección principal: la adecuación a la nueva ley comienza mucho antes de una fiscalización. Requiere comprender cómo se gestionan los datos dentro de la organización, identificar brechas y desarrollar capacidades que permitan demostrar el cumplimiento de las nuevas obligaciones.

2. La experiencia europea ofrece una advertencia para Chile

Lecciones desde Europa: aprendizajes del GDPR para la implementación de la ley en Chile

La implementación del GDPR en Europa dejó aprendizajes que hoy resultan especialmente relevantes para las organizaciones chilenas insertas en un proceso de adecuación. La experiencia europea permite anticipar escenarios, comprender las dificultades que implica este tipo de transformación y entender que la adecuación a una nueva regulación no se limita al cumplimiento jurídico.

> **La adopción de esta legislación representa una gran oportunidad para Chile. Facilita la confianza, reduce las fricciones en la economía digital y nos acerca a los estándares internacionales que hoy exigen los mercados.**

Javier Carreras
VP, Global Commercial & DPO, Sovos

El mayor riesgo es creer que aún queda tiempo: la experiencia europea mostró que muchas organizaciones postergaron sus procesos de preparación pese a contar con amplios períodos de transición.

Implementar un programa serio de protección de datos requiere tiempo, coordinación interna y gestión del cambio. El período de adecuación solo resulta suficiente cuando las organizaciones lo entienden como una oportunidad para prepararse y no como una razón para postergar las decisiones.

La protección de datos es un cambio cultural, no un proyecto de cumplimiento: el cumplimiento no puede recaer únicamente en las áreas legales o tecnológicas. Debe incorporarse como una práctica transversal mediante capacitación, responsabilidades distribuidas y participación de todas las áreas de la organización.

Esto exige que el conocimiento y las responsabilidades no permanezcan concentrados en una sola persona, sino que se distribuyan progresivamente entre los distintos equipos mediante referentes internos con capacitación especializada.

> **La protección de datos no es un tema técnico ni legal; es un tema profundamente humano. La formación sigue siendo la inversión más rentable que puede hacer una organización, porque la mayoría de los incidentes tiene su origen en las personas.**

Leocadio Marrero
CEO de GRCx3, DPO y director académico en Diplomados de Protección de Datos

La confianza digital también genera valor económico: una gestión responsable de la información fortalece la confianza de clientes, socios y mercados, facilita la operación internacional y puede transformarse en una ventaja competitiva. Al mismo tiempo, contribuye a construir relaciones más sólidas con los clientes y a consolidar una economía digital basada en datos de calidad y confianza.

> **El eslabón más débil entre una empresa y un cliente digital es la confianza. Los clientes están a un clic de quedarse o irse. La diferencia la marca el nivel de confianza que la organización sea capaz de generar.**

Leocadio Marrero
CEO de GRCx3, DPO y director académico en Diplomados de Protección de Datos

La lección principal: La experiencia europea demuestra que la adecuación a una nueva normativa no termina con su entrada en vigor. La protección de datos es un proceso continuo que exige fortalecer capacidades, promover una cultura organizacional orientada al tratamiento responsable de la información y adaptarse de forma permanente a un entorno regulatorio en evolución.

3. Ciberseguridad, gobernanza y protección de datos deben avanzar juntas

Ciberseguridad y cumplimiento: medidas técnicas y organizativas bajo la nueva ley

La protección de datos ya no puede abordarse únicamente desde el cumplimiento normativo ni desde la tecnología de forma aislada. La nueva ley exige integrar seguridad, gobernanza y gestión de riesgos en una misma estrategia.

Al mismo tiempo, la innovación requiere incorporar principios de privacidad y protección de datos desde el diseño de los procesos y las tecnologías. La protección de la información deja de ser una etapa posterior y pasa a formar parte del desarrollo de soluciones como la inteligencia artificial o los modelos predictivos.

La responsabilidad no termina en la propia organización: la seguridad de los datos depende también de terceros. Una organización puede implementar controles robustos internamente y seguir expuesta a riesgos derivados de proveedores, plataformas o servicios externos. Esto exige incorporar requisitos de seguridad y protección de datos en los contratos, verificar las prácticas de los proveedores y asegurar que toda la cadena opere bajo estándares compatibles con la nueva normativa.

La seguridad de una organización también depende de la seguridad de sus proveedores. Si uno de ellos sufre un incidente, ese riesgo termina trasladándose a toda la cadena y la responsabilidad sigue siendo de la organización.

Romina Torres
PhD Engineer

La evidencia será tan importante como la protección: la normativa exige implementar medidas de seguridad, pero también demostrar que estas existen y funcionan. La capacidad de registrar eventos, conservar evidencia y reconstruir lo ocurrido tras un incidente será fundamental para acreditar el cumplimiento de las obligaciones que establece la ley. Esto implica contar con registros y mecanismos de trazabilidad que permanezcan disponibles incluso después de un incidente, permitiendo demostrar qué ocurrió, cómo se respondió y qué medidas de protección estaban implementadas.

La ley cambia completamente la lógica frente a un incidente. No basta con decir que existían medidas de seguridad; la organización debe ser capaz de demostrarlo. Por eso la evidencia —logs, registros y trazabilidad— pasa a ser tan importante como la protección misma.

Romina Torres
PhD Engineer

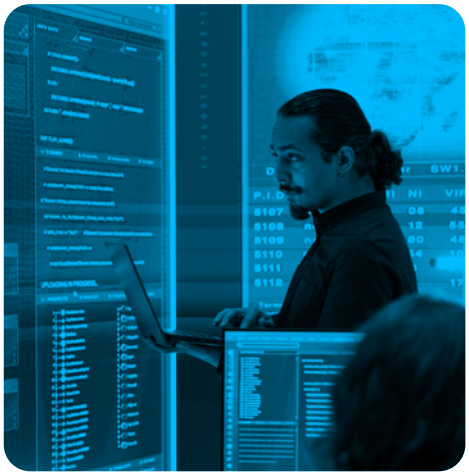
La inteligencia artificial exige nuevas salvaguardas: incorporar IA no solo implica evaluar su precisión, sino también asegurar transparencia, explicabilidad y protección de los datos utilizados para entrenar o alimentar los modelos. El uso de herramientas generativas, agentes inteligentes y servicios externos obliga a revisar cuidadosamente qué información se comparte, cómo será utilizada y qué controles existen para evitar filtraciones o usos no autorizados.

> **La privacidad no puede convertirse en un obstáculo para la innovación. El desafío es diseñar tecnologías que protejan los datos sin impedir que sigamos desarrollando soluciones que aporten valor a las personas.**

Romina Torres
PhD Engineer

La protección de datos debe incorporarse desde el diseño: la nueva normativa exige que las organizaciones definan desde el inicio qué datos realmente necesitan, con qué finalidad serán utilizados y durante cuánto tiempo serán conservados. El consentimiento, la minimización de datos y la privacidad por defecto dejan de ser requisitos formales para convertirse en principios de diseño de los sistemas y servicios.

La lección principal: la protección de datos exige una estrategia donde ciberseguridad, gobierno de datos, cumplimiento e innovación avancen de manera coordinada. Proteger la información ya no depende únicamente de implementar controles técnicos, sino de diseñar procesos, tecnologías y relaciones con terceros que permitan prevenir riesgos, responder ante incidentes y demostrar que las medidas adoptadas cumplen efectivamente con la normativa.



4. La confianza en la IA dependerá de cómo se gestionen sus riesgos

¿Podemos confiar en la IA para verificar identidad? Una mirada desde la innovación, riesgos y cumplimiento

La inteligencia artificial está transformando los procesos de verificación de identidad y prevención del fraude. Sin embargo, su incorporación plantea nuevos desafíos en materia de transparencia, explicabilidad, regulación y gestión de riesgos. Aunque los modelos generativos han impulsado un renovado interés por la IA, representan solo una parte de una disciplina con décadas de desarrollo y no todas las tecnologías son adecuadas para resolver los mismos problemas.

La IA es una herramienta poderosa, pero no infalible: los sistemas de IA son modelos predictivos, no mecanismos deterministas. Pueden alcanzar niveles muy altos de precisión, pero siempre existe la posibilidad de error. Comprender esa diferencia resulta fundamental para definir en qué procesos pueden utilizarse, qué nivel de supervisión requieren y cuáles son sus límites.

No toda la inteligencia artificial sirve para resolver los mismos problemas: los grandes modelos de lenguaje (LLM) fueron diseñados para generar contenido, no para tomar decisiones críticas. La elección de una tecnología debe responder al problema que se busca resolver y al nivel de precisión, control y explicabilidad que exige cada caso, especialmente cuando las decisiones afectan directamente a las personas.

La explicabilidad será tan importante como la precisión: el desafío no consiste únicamente en lograr modelos más precisos, sino también en ser capaces de explicar cómo y por qué toman determinadas decisiones. A medida que avanzan las regulaciones sobre inteligencia artificial y protección de datos, las organizaciones deberán demostrar que sus sistemas son transparentes, auditables y comprensibles. La responsabilidad sobre las decisiones sigue recayendo en la organización, incluso cuando intervienen modelos de IA.

Un modelo puede tomar una buena decisión y aun así no ser capaz de explicar cómo llegó a ella. Ahí aparece el verdadero desafío de la explicabilidad: no basta con obtener buenos resultados; también debemos poder entender y justificar cómo se producen.

John Atkinson
Founder and CEO, AI-Empowered

La innovación debe comenzar por el problema, no por la tecnología: el interés por incorporar inteligencia artificial no siempre va acompañado de un diagnóstico sobre los problemas que realmente se busca resolver. Antes de seleccionar herramientas o modelos, resulta indispensable comprender los procesos de negocio, identificar dónde la IA puede aportar valor y evaluar si existen otras alternativas más adecuadas para alcanzar ese objetivo.

Estamos tan enfocados en la última herramienta de moda que muchas veces olvidamos hacernos la pregunta más importante: ¿qué problema estamos tratando de resolver?

John Atkinson
Founder and CEO, AI-Empowered

La lección principal: la inteligencia artificial puede convertirse en un aliado para fortalecer la verificación de identidad y prevenir el fraude, siempre que se utilice con objetivos claros, modelos adecuados para cada problema y mecanismos que permitan supervisar, explicar y validar sus decisiones. La confianza no depende únicamente del rendimiento de los modelos, sino de la capacidad de las organizaciones para utilizarlos de forma responsable.

Podemos usar inteligencia artificial para verificar identidad. Los modelos predicen muy bien, pero hay que entender que son probabilísticos, no deterministas. Esa diferencia es clave para comprender tanto sus capacidades como sus límites. La IA es una herramienta extraordinaria, siempre que tengamos claro qué problema queremos resolver antes de incorporarla en procesos críticos.

Tomás Castañeda
Senior Director, Product Development, Sovos

5. La protección de datos comienza por conocer la información que se gestiona

De la teoría a la práctica: cómo las organizaciones están protegiendo los datos de sus clientes.

Los desafíos de la protección de datos se vuelven más concretos cuando las organizaciones intentan llevar las políticas a la práctica. La preparación para la nueva ley comienza mucho antes de incorporar nuevas tecnologías: exige conocer la información disponible, definir responsabilidades, fortalecer el gobierno de datos y alinear la tecnología con los objetivos del negocio.

El primer paso no es la tecnología, es conocer los datos: antes de incorporar nuevas tecnologías, automatización o inteligencia artificial, resulta indispensable identificar qué datos existen, dónde están almacenados, quién los utiliza y qué tan confiables son. Sin esa base, las organizaciones difícilmente podrán proteger la información o construir soluciones que realmente aporten valor.nologías, automatización o inteligencia artificial, resulta indispensable identificar qué datos existen, dónde están almacenados, quién los utiliza y qué tan confiables son. Sin esa base, las organizaciones difícilmente podrán proteger la información o construir soluciones que realmente aporten valor.

Si no conocemos nuestra organización y dónde están los datos, es imposible protegerlos. Primero hay que identificarlos, mapearlos y documentarlos. Pero no basta con saber que existen: también es necesario comprender su calidad para poder gestionarlos correctamente. Solo sobre esa base tiene sentido hablar de herramientas o inteligencia artificial.

Helder Branco
VPTI – IT Operations

La protección de datos es una responsabilidad de toda la organización: esta tarea no puede recaer exclusivamente en las áreas de tecnología. Requiere una estructura de gobierno que involucre distintas disciplinas, responsables claramente definidos y mecanismos de coordinación entre las diferentes áreas de la organización. Durante la sesión también se destacó la importancia de crear referentes internos capaces de impulsar estos principios en cada equipo y mantener un lenguaje común en toda la organización.

El gobierno de los datos no es solo tecnológico. También requiere una mirada regulatoria, legal y organizacional. No basta con proteger la información desde la infraestructura; distintas áreas y distintos especialistas deben participar para identificar riesgos, definir responsabilidades y asegurar que las reglas realmente se cumplan.

Alberto Juárez
VP Digital ID & Trust, Sovos

La tecnología debe responder a un propósito de negocio: La incorporación de nuevas herramientas solo tiene sentido cuando responde a necesidades concretas del negocio. Comprender los procesos, identificar los problemas que se busca resolver y acercar las áreas de tecnología a la operación permite construir soluciones que aporten valor y faciliten una implementación responsable de nuevas capacidades como la inteligencia artificial.

Las áreas de TI tienen que transformarse en áreas mucho más cercanas al negocio. Solo entendiendo el negocio, sus datos y sus procesos podremos construir soluciones que realmente respondan a sus necesidades.

Helder Branco
VPTI – IT Operations

La incorporación responsable de IA comienza mucho antes de implementarla: este proceso exige un trabajo previo de organización y diagnóstico. Antes de automatizar procesos resulta necesario comprender qué información existe, por qué se recopila, quién es responsable de ella y con qué propósito será utilizada. Ese trabajo interno constituye la base para cualquier estrategia tecnológica posterior.

> **El ejercicio empieza mucho antes de implementar inteligencia artificial. Empieza por entender qué datos tenemos, por qué los tenemos, dónde están y para qué los utilizamos. Solo cuando esas bases están claras es posible incorporar inteligencia artificial de manera responsable.**
>
> **Alberto Juárez**
> VP Digital ID & Trust, Sovos

La lección principal: la protección de datos comienza mucho antes de implementar nuevas herramientas. Exige conocer la información que gestiona la organización, fortalecer su gobierno, definir responsabilidades y alinear la tecnología con los objetivos del negocio. Solo sobre esa base resulta posible incorporar inteligencia artificial, responder a las exigencias regulatorias y construir organizaciones preparadas para los desafíos que vienen.

Lo que deja este recorrido

Las cinco conversaciones desarrolladas durante el Summit mostraron que la nueva Ley de Protección de Datos trasciende el cumplimiento normativo. La adecuación exige articular gobierno de datos, ciberseguridad, tecnología, cultura organizacional e innovación.

En conjunto, estos aprendizajes refuerzan una idea central: proteger los datos exige comprender la información que se gestiona, asumir responsabilidades sobre su tratamiento y desarrollar capacidades permanentes para responder a un entorno regulatorio y tecnológico en evolución.

El valor estratégico de la protección de datos

La forma en que una organización gestiona los datos personales influye directamente en la confianza que es capaz de generar. En un entorno donde las interacciones digitales son cada vez más frecuentes, demostrar transparencia, seguridad y responsabilidad se transforma en una capacidad estratégica.

Las organizaciones que desarrollen capacidades de gobernanza, protección de datos y gestión de riesgos estarán mejor preparadas para cumplir con la normativa, y al mismo tiempo podrán fortalecer su reputación, reducir fricciones operativas y construir relaciones más sólidas con sus distintos grupos de interés.

En suma, la protección de datos ya no es únicamente una obligación legal. Es parte de la forma en que las organizaciones construyen confianza y sostienen su crecimiento en la economía digital.

¿Tu organización está preparada para la Ley 21.719?

Evalúa tu preparación. Habla con un experto.

Preguntas frecuentes sobre la Ley de Protección de Datos en Chile

¿Qué cambia con la nueva Ley de Protección de Datos en Chile?

La nueva normativa introduce mayores exigencias en el tratamiento de datos personales, fortaleciendo los derechos de los titulares y estableciendo obligaciones más claras para las organizaciones, junto con un régimen de fiscalización y sanciones más robusto.

¿A quién aplica la Ley de Protección de Datos en Chile?

Aplica a todas las organizaciones —públicas o privadas— que traten datos personales en Chile, independientemente de su tamaño o industria.

¿Cuáles son los principales riesgos de no cumplir?

El incumplimiento puede derivar en sanciones económicas, daños reputacionales y pérdida de confianza por parte de clientes y usuarios, además de posibles interrupciones operativas.

¿Qué rol cumple la ciberseguridad en esta normativa?

La ciberseguridad es esencial, ya que la ley exige implementar medidas técnicas y organizativas que garanticen la protección de los datos frente a accesos no autorizados, pérdidas o filtraciones.

¿Cómo pueden prepararse las organizaciones?

El primer paso es realizar un diagnóstico del estado actual en materia de protección de datos. A partir de ahí, es clave definir una estrategia que incluya gobernanza, tecnología, procesos, gestión de riesgos y capacitación interna.

SOVOS