

Las 10 acciones prioritarias que deben realizar las empresas para cumplir con la ley de datos personales

■ Abogado de HD Group llamó a las compañías a identificar los tipos de datos que manejan, a mapear las áreas críticas que tratan información personal y a tomar medidas de seguridad.

POR MARCO ZECCHETTO

En diciembre de 2026 entrará en vigencia la Ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, la que establece obligaciones y multas a las organizaciones –personas naturales, jurídicas y órganos del Estado– que no las cumplan.

El abogado y director de Protección de Datos Personales, Ciberseguridad y Nuevas Tecnologías de HD Group, Juan Pablo González, alertó que en las organizaciones persiste “una falta de cultura de tratamiento de datos” y ven la regulación como algo que hay que cumplir y no como un tema que impacta su negocio. En el año y medio que resta, llamó a abordar el tema de forma “integral” en la estrategia corporativa y a empezar a ejecutar 10 acciones clave.

1 Identificar los datos personales que manejan

La ley distingue entre datos personales generales –como nombre o RUT– y datos sensibles (biométricos, de salud o geolocalización) y estos últimos están sujetos a reglas específicas. Para González lo primero es saber qué tipo de datos se tienen almacenados, para adoptar medidas diferenciadas de gestión y tratamiento según los requisitos legales.

2 Conocer las fuentes de obtención

El abogado dijo que la ley no exige expresamente identificar el origen de los datos,

pero señaló que esto permite distinguir las distintas bases de licitud –habilitantes legales– para poder tratarlos. Recomendó mapear los canales de captura (como sitios web, proveedores o eventos) para vincular cada flujo de información con la base de licitud correspondiente, como el consentimiento o un contrato.

3 Establecer un uso explícito

El principio de finalidad obliga a que los datos solo se utilicen para propósitos específicos, explícitos y lícitos. Si bien muchas empresas tienen información obtenida para fines concretos, “está esa visión de poder usarla para otros fines”.

González señaló que deberán identificar los usos, pues con la ley deberán informar a los titulares de los datos qué tratamiento les darán.

4 Mapear las áreas críticas del negocio

El abogado recomendó identificar en las organizaciones las áreas que manejan mayor volumen de información personal –como ventas o servicio al cliente– para optimizar recursos, prevenir infracciones en zonas de alta exposición y priorizar la adopción de medidas técnicas y organizativas para el tratamiento de datos.

5 Informar las políticas de tratamiento de datos

La normativa exige informar de manera “precisa, clara, inequívoca y gratuita” al titular de los datos

toda la información necesaria para el ejercicio de sus derechos. Para eso recomendó tener actualizadas y accesibles las políticas y las prácticas sobre el tratamiento de los datos personales, las que deberán estar a disposición de los usuarios.

6 Definir estándares y reglas con proveedores

Los proveedores deben tratar datos a nombre de una empresa bajo instrucciones claras y alineadas a los estándares de la organización. González dijo que muchas veces estas prácticas están cubiertas por acuerdos de confidencialidad, “pero no necesariamente a prácticas asociadas al tratamiento de datos personales, y se pueden producir situaciones como almacenar indefinidamente esos datos, lo que puede ser un riesgo de incumplimiento”.

7 Gestionar bien los derechos de los titulares

La ley reconoce derechos de

acceso, rectificación, supresión, oposición y portabilidad de los datos personales; y los titulares pueden usar diferentes vías para ejercerlos, como correo, teléfono o formularios. González señaló que la organización debe tener protocolos definidos para gestionarlos y responderlos a tiempo, y así evitar exponerse a una infracción.

8 Definir plazos de conservación de los datos

El principio de calidad de los datos obliga a las empresas a saber qué información tienen y a mantenerla actualizada, mientras que el de proporcionalidad exige tener solo la data “necesaria” para fines de tratamiento y “pide almacenar la información durante el tiempo que es indispensable” para su uso y tratamiento. Dijo que las empresas deben eliminar información “proactivamente” cuando ya no sea necesaria, para reducir riesgos de filtración, mal uso o incumplimiento.

9 Implementar medidas de seguridad

González señaló que cada organización debe adoptar estándares y medidas de seguridad para el tratamiento de datos. Estas van desde la definición de roles, la generación de políticas, cláusulas contractuales, etiquetado de datos hasta tecnologías como encriptación, autenticación multifactor y VPN (red privada virtual).

10 Capacitar a las distintas áreas

El abogado dijo que todas las áreas deben comprender sus responsabilidades en el uso y resguardo de datos personales, y que la capacitación contribuye a crear una cultura organizacional “estratégica” en torno al tratamiento responsable de la información, y a “entender que no es solo un conjunto de políticas internas”.



Juan Pablo González,
director de Protección
de Datos Personales,
Ciberseguridad y
Nuevas Tecnologías
de HD Group.