



La protección de datos personales más allá de una perspectiva legal

En la era digital, la protección de datos personales se ha convertido en una prioridad crítica para las empresas que manejan información sensible de clientes, empleados, socios y demás agentes que hacen parte del ecosistema empresarial.

Elaborado por José Luis Jerez, socio de Deloitte Legal – área de Intangibles.

Más allá de ser un simple cumplimiento normativo, la protección de datos personales es un componente estratégico que sostiene la confianza y fidelidad de los clientes, actuando como

un activo intangible de gran valor. Por esta razón, un manejo inadecuado de estos datos no solo puede resultar en sanciones legales, sino que también puede dañar irreparablemente la reputación de una organización. ➡

La necesidad de proteger los datos personales está respaldada por estándares internacionales como la ISO 27001 y la ISO 27701.

Sumado a lo anterior, la necesidad de proteger los datos personales está respaldada por estándares internacionales como la ISO 27001 y la ISO 27701. La primera de estas establece un marco para la gestión de la seguridad de la información, mientras que la ISO 27701 extiende estos principios a la privacidad de los datos personales. Implementar estas normas no debe ser visto como una tarea administrativa, sino como una oportunidad para integrar prácticas de protección de datos en el ADN de la empresa, asegurando que todos los esfuerzos operativos y legales que se invierten en la elaboración, implementación y desarrollo de políticas, manuales y demás documentos afines, no se conviertan en letra muerta.

En ese sentido, la protección de datos personales requiere más que la simple adopción de políticas escritas. Es decir, implica un acompañamiento técnico que provea herramientas y medidas de seguridad adecuadas para la protección de los datos personales. Este tipo de herramientas van desde la implementación de sistemas de gestión de identidades y accesos hasta la utilización de tecnología de cifrado y anonimización, medidas que las empresas, idealmente, deben adoptar con un enfoque coherente con la estructura de sus documentos.

Bajo un escenario digital, omnipresente y retador, las empresas deben procurar la privacidad y seguridad de la información que gestionan. Para lograrlo, es fundamental considerar una serie de prácticas que no solo cumplan con los estándares internacionales, sino que también fortalezcan la confianza con los agentes relevantes de cada negocio. A continuación, se presentan cinco aspectos que las organizaciones deben tener en cuenta para fortalecer sus prácticas en materia de datos personales:



- 1. Implementar tecnologías avanzadas de seguridad:** las organizaciones deben invertir en tecnologías de vanguardia como el cifrado de datos, la autenticación multifactor y sistemas de detección y respuesta ante amenazas. Estas herramientas ayudan a proteger la información sensible contra accesos no autorizados y ciberataques. Además, el uso de inteligencia artificial y aprendizaje automático puede mejorar la capacidad de las empresas para anticipar y mitigar riesgos de seguridad.



- 2. Establecer políticas claras de manejo de datos:** es crucial definir y comunicar políticas internas que regulen cómo se recopilan, almacenan, procesan y comparten los datos personales. Estas políticas deben ser claras, accesibles y comprensibles para todos los colaboradores, garantizando que cada uno entienda sus responsabilidades y las mejores prácticas para proteger la información de los clientes y la empresa.

La protección de datos personales más allá de una perspectiva legal



3. Fomentar una cultura de concienciación entre los colaboradores: la seguridad de la información no es solo una cuestión tecnológica, sino también humana. Las empresas deben realizar capacitaciones regulares para educar a sus colaboradores sobre la importancia de la protección de datos, las tácticas comunes de ingeniería social y cómo identificar posibles amenazas. Al crear una cultura de seguridad, los colaboradores se convierten en la primera línea de defensa.



4. Realizar auditorías regulares de seguridad: estas auditorías son esenciales para evaluar la efectividad de las medidas implementadas y detectar vulnerabilidades antes de que puedan ser explotadas. Estas deben ser realizadas por profesionales capacitados y pueden incluir pruebas de penetración, revisiones de configuración de seguridad y análisis de políticas de acceso. Los resultados deben ser utilizados para mejorar continuamente las estrategias de seguridad y ciberseguridad.



5. Contar con un sólido acompañamiento legal, que garantice el cumplimiento normativo y la adaptación a cambios legislativos: dado el dinamismo del entorno legal en torno a la privacidad de los datos, es vital que las empresas cuenten con expertos legales que les asesoren en el cumplimiento de las normativas locales e internacionales, como el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) o las regulaciones de privacidad específicas de cada país de Latinoamérica. Este acompañamiento asegura que la empresa no solo cumpla con la ley, sino que también esté preparada para adaptarse rápidamente a cualquier cambio legislativo.

La protección de datos personales más que un mandato normativo es una responsabilidad ética y estratégica que requiere un enfoque proactivo y continuo. Al adherirse a estándares internacionales y adoptar una visión integral, las empresas pueden convertir la protección de datos personales en una ventaja competitiva. Así, las empresas deben priorizar la privacidad y seguridad de la información como un pilar fundamental de su estrategia de negocio. Implementar tecnologías avanzadas, establecer políticas claras, fomentar una cultura de concienciación, realizar auditorías regulares y contar con un sólido acompañamiento legal son acciones fundamentales para proteger los datos personales. Al hacerlo, no solo se mitigan riesgos potenciales, sino que también se fortalece la confianza de los clientes, los socios y demás actores relevantes. En última instancia, aquellas organizaciones que logren integrar de manera efectiva estas prácticas estarán mejor posicionadas para prosperar en el entorno digital actual y futuro.

**Este texto fue elaborado con la participación de Andrés Salazar, abogado senior de Deloitte Legal.*

Contáctanos:

José Luis Jerez
socio de Deloitte Legal – Intangibles
Tel: +57 316 7404363
Email: jjerez@deloitte.com

Deloitte se refiere a una o más entidades de Deloitte Touche Tohmatsu Limited ("DTTL"), su red global de firmas miembro y sus sociedades afiliadas a una firma miembro (en adelante "Entidades Relacionadas") (colectivamente, la "organización Deloitte"). DTTL (también denominada como "Deloitte Global") así como cada una de sus firmas miembro y sus Entidades Relacionadas son entidades legalmente separadas e independientes, que no pueden obligarse ni vincularse entre sí con respecto a terceros. DTTL y cada firma miembro de DTTL y su entidad relacionada es responsable únicamente de sus propios actos y omisiones, y no de los de las demás. DTTL no provee servicios a clientes. Consulte www.deloitte.com/about para obtener más información.

Deloitte presta servicios profesionales líderes de auditoría y assurance, impuestos y servicios legales, consultoría, asesoría financiera y asesoría en riesgos, a casi el 90% de las empresas Fortune Global 500® y a miles de empresas privadas. Nuestros profesionales brindan resultados medibles y duraderos que ayudan a reforzar la confianza pública en los mercados de capital, permiten a los clientes transformarse y prosperar, y liderar el camino hacia una economía más fuerte, una sociedad más equitativa y un mundo sostenible. Sobre la base de su historia de más de 175 años, Deloitte abarca más de 150 países y territorios. Conozca cómo los aproximadamente 460,000 profesionales de Deloitte en todo el mundo crean un impacto significativo en www.deloitte.com.

Tal y como se usa en este documento, "Deloitte S-LATAM, S.C." es la firma miembro de Deloitte y comprende tres Marketplaces: México-Centroamérica, Cono Sur y Región Andina. Involucra varias entidades legalmente separadas e independientes, las cuales tienen el derecho legal exclusivo de involucrarse en, y limitan sus negocios a, la prestación de servicios de auditoría, consultoría, consultoría fiscal, asesoría legal, en riesgos y financiera y otros servicios profesionales bajo el nombre de "Deloitte".

Esta comunicación contiene solamente información general y ni Touche Tohmatsu Limited ("DTTL"), su red global de firmas miembro o sus Entidades Relacionadas (colectivamente, la "organización Deloitte") está, por medio de esta comunicación, prestando asesoramiento profesional o servicio alguno. Antes de tomar cualquier decisión o tomar cualquier medida que pueda afectar sus finanzas o su negocio, debe consultar a un asesor profesional calificado.

No se proporciona ninguna representación, garantía o promesa (ni explícita ni implícita) sobre la veracidad ni la integridad de la información en esta comunicación, y ni DTTL, ni sus firmas miembro, Entidades Relacionadas, empleados o agentes será responsable de cualquier pérdida o daño alguno que surja directa o indirectamente en relación con cualquier persona que confíe en esta comunicación. DTTL y cada una de sus firmas miembro y sus Entidades Relacionadas, son entidades legalmente separadas e independientes.