Kiteworks

RESUMEN DE CUMPLIMIENTO

Soporte para el Cumplimiento de la Ley de Protección de Datos Personales de Colombia

Cómo Kiteworks aborda los requisitos de seguridad, gobernanza y responsabilidad de la Ley 1581 de 2012

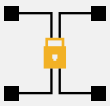
La Ley 1581 de 2012 de Colombia establece un marco integral de protección de datos personales que regula cómo las entidades públicas y privadas recopilan, almacenan, procesan y circulan datos personales, anclando estas obligaciones en el derecho constitucional al habeas data consagrado en el Artículo 15 de la Constitución Política de Colombia. La ley aplica a toda entidad que procese datos personales en territorio colombiano, así como a responsables y encargados extranjeros sujetos a la jurisdicción colombiana mediante acuerdos internacionales. Afecta a todos los sectores de la economía colombiana, incluyendo instituciones financieras, empresas comerciales, prestadores de servicios de salud y entidades gubernamentales que mantienen bases de datos personales. Las entidades tuvieron seis meses desde la promulgación de la ley en octubre de 2012 para adaptar sus operaciones, y los decretos reglamentarios expedidos en 2013 y 2015 definieron con mayor precisión las obligaciones de cumplimiento. Las organizaciones que incumplan se exponen a multas de hasta 2.000 salarios mínimos mensuales, suspensión de las actividades de tratamiento de datos por hasta seis meses y el cierre definitivo de operaciones que involucren datos sensibles. Kiteworks proporciona a las organizaciones los controles técnicos y las capacidades de gobernanza necesarios para contribuir al cumplimiento de los requisitos de la Ley 1581. A continuación se detalla cómo:

Medidas de Seguridad para la Integridad de los Datos Personales

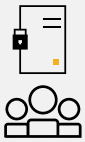
La Ley 1581 exige a los responsables y encargados del tratamiento aplicar las medidas técnicas, humanas y administrativas necesarias para prevenir la adulteración, pérdida, consulta no autorizada y el acceso fraudulento a los datos personales, conforme al principio de seguridad establecido en el Artículo 4(g) y las obligaciones de los Artículos 17 y 18. Kiteworks satisface estos requisitos a través de su dispositivo virtual endurecido, que protege la infraestructura de servidor subyacente frente a ataques externos y errores de configuración, y mediante cifrado doble en reposo, que garantiza que los datos personales almacenados permanezcan ilegibles sin la debida autorización. Cada Formulario de Datos Seguro de Kiteworks crea automáticamente una carpeta compartida segura asociada, de modo que los datos personales enviados a través del formulario quedan protegidos desde el momento de su recopilación. El Formato de Datos de Confianza (TDF) de Kiteworks envuelve la información sensible en cifrado persistente y controles de acceso que acompañan al archivo independientemente de dónde se almacene, comparta o procese, aplicando políticas de vencimiento automático de datos y manteniendo registros de auditoría incorporados que registran todos los intentos de acceso al contenido protegido.

Aspectos destacados de la solución

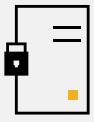
Dispositivo virtual endurecido



Cifrado doble robusto



RBAC y ABAC



Formularios de datos seguros

Registros de auditoría de cumplimiento

Gobernanza del Acceso y la Circulación de Datos Personales

La ley establece, además, que los datos personales solo pueden circular a partes autorizadas, que los Titulares conservan el derecho a conocer, actualizar y rectificar su información, y que el tratamiento debe obedecer a una finalidad legítima definida, conforme a los Artículos 4(b), 4(c), 8, 13 y 17. Los Responsables del Tratamiento deben restringir el acceso a personas no autorizadas y suministrar información a los Titulares ante solicitud de consulta dentro de los 10 días hábiles siguientes. Kiteworks respalda estas obligaciones a través del Motor de Políticas de Datos (DPE), que aplica permisos RBAC para definir qué usuarios pueden visualizar, descargar o colaborar con los datos almacenados en carpetas compartidas seguras. Las políticas de riesgo ABAC aplican decisiones de acceso dinámicas basadas en los atributos del archivo, el departamento del usuario y el contexto geográfico, garantizando que los datos personales no lleguen a partes no autorizadas. Los Formularios de Datos Seguros de Kiteworks aplican validación de campos incorporada — que verifica el formato del correo electrónico, el rango de fechas, la entrada numérica y las reglas de tipo de archivo — para asegurar que solo ingresen al sistema datos completos y precisos, en apoyo directo a los requisitos de veracidad y calidad del Artículo 4(a).

Auditoría, Retención y Documentación de los Derechos del Titular

Los responsables y encargados del tratamiento están obligados a mantener registros verificables de autorizaciones, atender las consultas y reclamos de los Titulares dentro de los plazos definidos, y demostrar el cumplimiento de las obligaciones de calidad y ciclo de vida de los datos conforme a los Artículos 7, 15, 17(b), 17(k), 18(f) y 19A. Las organizaciones deben conservar prueba del consentimiento y evidencia de sus medidas de cumplimiento para que los reguladores puedan auditar dichos registros durante las investigaciones. Los registros de auditoría de Kiteworks capturan toda la actividad de los usuarios sobre los datos personales almacenados en la plataforma, generando un registro rastreable de quién accedió, descargó o modificó cada archivo. Cada envío de formulario genera tanto un PDF legible por humanos como un archivo CSV legible por máquinas, almacenados en la carpeta compartida segura del formulario, lo que produce documentación estructurada que respalda las consultas de los Titulares y las solicitudes de verificación de autorización. El cifrado TDF persistente incorpora metadatos del registro de auditoría directamente en los archivos protegidos, garantizando que los registros de acceso acompañen a los datos y estén disponibles para revisión regulatoria.

Kiteworks equipa a las organizaciones que operan bajo la Ley 1581 de 2012 de Colombia con los controles técnicos y operativos necesarios para cumplir los requisitos de seguridad, gobernanza y responsabilidad de la ley en cada etapa del tratamiento de datos personales. El dispositivo virtual endurecido y la arquitectura de cifrado de la plataforma protegen los datos personales en reposo y en tránsito, mientras que el Motor de Políticas de Datos aplica controles de acceso basados en roles y atributos que hacen cumplir los requisitos de circulación restringida de la ley. Los Formularios de Datos Seguros capturan datos completos y los colocan de inmediato bajo controles de carpeta gobernados, en respaldo de los principios de calidad que la Ley 1581 exige desde el punto de recopilación. Los registros de auditoría completos y los registros de envío estructurados proporcionan a los responsables y encargados del tratamiento la documentación verificable que los reguladores esperan al evaluar el cumplimiento de las obligaciones de autorización, consulta y atención de reclamos.