Kiteworks

RESUMEN DE CUMPLIMIENTO

Kiteworks protege datos personales bajo la Ley 25.326 de Argentina

Protección de datos personales según la Ley 25.326

La Ley 25.326 de Argentina, conocida como Ley de Protección de Datos Personales (PDPL), establece un marco integral para la protección de datos personales almacenados en bases de datos, registros y archivos públicos y privados en todos los sectores. La ley aplica exclusivamente dentro de Argentina y abarca todas las instituciones públicas y entidades privadas que recolectan, procesan, almacenan o transfieren datos personales de residentes argentinos. Todas las industrias que manejan datos personales están sujetas a esta normativa, desde servicios financieros y salud hasta agencias de marketing y organismos gubernamentales. Promulgada el 4 de octubre de 2000, la ley exigió que los archivos de datos existentes se registraran ante la autoridad reguladora dentro de los 180 días posteriores a su decreto de implementación. Las organizaciones que no cumplen enfrentan sanciones administrativas que van desde advertencias formales y suspensiones operativas hasta multas entre $1,000 y $100,000 pesos, cancelación de bases de datos y sanciones penales, incluyendo prisión por insertar datos falsos a sabiendas o acceder ilegalmente a bases de datos protegidas. Kiteworks proporciona a las organizaciones las capacidades de gobernanza segura de contenido necesarias para respaldar los requisitos de la PDPL. Así es como lo hace:

Medidas de seguridad técnicas y organizativas

La PDPL de Argentina exige que los responsables y usuarios de datos adopten las medidas técnicas y organizativas necesarias para garantizar la seguridad y confidencialidad de los datos personales, prevenir accesos o alteraciones no autorizadas y prohibir el almacenamiento en sistemas que no cuenten con condiciones de integridad y seguridad (Artículos 9.1, 9.2, 21.2). Las bases de datos registradas también deben documentar los medios utilizados para garantizar la seguridad de los datos e identificar las categorías de personal con acceso al procesamiento de datos. Kiteworks responde a estos requisitos a través de su dispositivo virtual reforzado, que proporciona cifrado doble en reposo para todos los datos almacenados. El control de acceso basado en roles (RBAC) asegura que solo los usuarios autorizados accedan a archivos sensibles en los niveles de permiso definidos por el generador de formularios, mientras que el control de acceso basado en atributos (ABAC) aplica políticas de riesgo dinámicas que evalúan la clasificación de archivos, la autorización del usuario y factores contextuales. La validación de certificados TLS protege los datos en tránsito al terminar automáticamente las conexiones que no superan las verificaciones de certificados, evitando interceptaciones o ataques de suplantación.

Aspectos destacados

- **Dispositivo virtual reforzado**
- **Cifrado doble robusto**
- **Control de acceso basado en roles (RBAC)**
- **Validación de certificados TLS**
- **Registros de auditoria robustos**

Gobernanza de acceso y gestión del ciclo de vida de los datos

La PDPL exige que los datos personales se almacenen de manera que permita a los titulares ejercer su derecho de acceso, restringe las transferencias a partes con intereses legítimos, prohíbe transferencias a países sin protección adecuada y exige que los datos en revisión sean bloqueados o marcados durante los procedimientos de rectificación (Artículos 4.6, 4.7, 11.1, 12.1, 16.6). Los responsables también deben destruir los datos que ya no sean necesarios para los fines por los que fueron recolectados. Kiteworks respalda estos requisitos mediante su Data Policy Engine (DPE), que aplica permisos RBAC y ABAC en cada carpeta y archivo, asegurando que el acceso esté alineado con los roles de usuario definidos y la sensibilidad de los datos. Las políticas de invitación a carpetas del DPE permiten a los administradores bloquear el uso compartido con dominios restringidos o requerir aprobaciones antes de proceder con transferencias, apoyando directamente las restricciones de transferencias internacionales. La función de Verificación Directa de Archivos por el Operador confirma, valida y revisa archivos antes de su eliminación, asegurando que la destrucción de datos siga un proceso controlado y auditable.

Controles de auditoría, retención y revocación

La PDPL establece que los titulares de datos tienen derecho a la rectificación, eliminación, actualización y confidencialidad de sus datos personales, y que los datos deben conservarse solo durante los períodos definidos legal o contractualmente. Los procesadores externos deben destruir los datos al finalizar el contrato, y las personas pueden solicitar la eliminación de sus datos de bases de datos publicitarias en cualquier momento (Artículos 16.1, 16.7, 25.2, 27.3). Kiteworks respalda estos requisitos de seguimiento y ciclo de vida mediante su arquitectura de carpetas compartidas seguras, que almacena todas las presentaciones de formularios bajo condiciones de retención definidas y aplicadas por el Data Policy Engine. La función de Programación de Formularios permite a los administradores controlar con precisión cuándo está activa la recolección de datos, permitiendo la desactivación inmediata ante solicitudes de retiro. La función de Verificación Directa de Archivos por el Operador realiza una confirmación estructurada antes de cualquier eliminación, generando un registro defendible de la acción. Los responsables de cumplimiento pueden monitorear todas las actividades a través de los informes estándar de cumplimiento y registros de auditoría de Kiteworks, proporcionando evidencia de respuestas oportunas a las solicitudes de derechos de los titulares.

Kiteworks ofrece a las organizaciones que operan bajo la Ley de Protección de Datos Personales de Argentina una plataforma unificada para cumplir con las obligaciones de seguridad, gobernanza y ciclo de vida de los datos en todo el alcance de la ley. Su dispositivo virtual reforzado y cifrado en capas protegen los datos personales en reposo y en tránsito, mientras que los controles de acceso basados en roles y atributos garantizan que solo el personal autorizado acceda a contenido sensible. El Data Policy Engine gestiona cada archivo y carpeta según los permisos definidos, aplicando automáticamente restricciones de transferencias internacionales y bloqueando el uso compartido no autorizado. La Programación de Formularios y la Verificación Directa de Archivos por el Operador brindan a los equipos de cumplimiento un control preciso y auditable sobre la actividad de recolección de datos y los flujos de trabajo de eliminación, permitiendo respuestas oportunas a las solicitudes de derechos de los titulares. Los registros de auditoría integrales y los informes de cumplimiento crean el historial probatorio que las organizaciones necesitan para demostrar responsabilidad ante la autoridad reguladora de Argentina.