Kiteworks facilita el cumplimiento de la Ley de Protección de Datos Personales del Paraguay (Ley N.º 7593/2025)

Kiteworks

RESUMEN DE CUMPLIMIENTO

Cómo Kiteworks ayuda a las organizaciones a operacionalizar las obligaciones de protección de datos del Paraguay antes del plazo de cumplimiento de noviembre de 2027

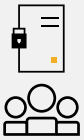
La Ley N.º 7593/2025 sobre Protección de Datos Personales en la República del Paraguay, promulgada el 27 de noviembre de 2025, establece requisitos integrales de protección de datos que entrarán en vigor 24 meses después de su publicación oficial (noviembre de 2027). La ley se aplica de manera transversal a responsables y encargados del tratamiento de los sectores público y privado, independientemente del sector, incluyendo (de forma ilustrativa) salud, finanzas, telecomunicaciones, comercio minorista, educación y administración pública. La regulación abarca cualquier tratamiento de datos personales dentro de la jurisdicción del Paraguay e incluye disposiciones para transferencias internacionales de datos, exigiendo niveles de protección adecuados para los flujos de datos transfronterizos. Si bien la ley establece la Agencia Nacional de Protección de Datos Personales como autoridad supervisora (una unidad desconcentrada dentro del Ministerio de Tecnologías de la Información y Comunicación con autonomía funcional, conforme al Artículo 34), dirigida por un Director General y un Director General Adjunto designados por Decreto Ejecutivo a partir de una terna propuesta por el MITIC tras concurso público (Artículo 37), con facultades para imponer sanciones administrativas que incluyen advertencias, multas de entre 20 y 2.500 jornales mínimos por infracciones generales (Artículo 46), hasta 5.000 jornales mínimos por infracciones que involucren datos sensibles, y hasta 10.000 jornales mínimos por infracciones que afecten datos sensibles de niños y adolescentes, así como la suspensión de las actividades de tratamiento de datos, las sanciones económicas específicas varían según la gravedad de la infracción y otros factores establecidos en el Artículo 47. Las multas se calculan en jornales mínimos, fijados periódicamente por resolución del MTESS en ₲ 111.502 a partir de julio de 2025, según la Resolución MTESS 677/2025. Kiteworks apoya a las organizaciones en su avance hacia el cumplimiento de la Ley N.º 7593/2025. Así es cómo:

Protección de Datos Personales Contra el Acceso No Autorizado y las Brechas de Seguridad

Los Artículos 4 y 16 exigen medidas técnicas y organizativas para prevenir brechas de datos, requiriendo que los responsables implementen y supervisen periódicamente salvaguardas de seguridad que protejan contra el acceso no autorizado, la alteración o la pérdida de datos personales. El Artículo 9 exige además que los responsables del tratamiento demuestren el cumplimiento mediante controles de seguridad adecuados al riesgo del tratamiento. El Artículo 22 aborda específicamente los datos de videovigilancia, estableciendo que las grabaciones que contengan evidencia de actos contra la integridad de las personas o la propiedad deben ser proporcionadas a las autoridades competentes dentro de las 72 horas siguientes al conocimiento de su existencia.

Aspectos destacados de la solución

Dispositivo virtual reforzado con cifrado doble



Motor de Políticas de Datos con ABAC y RBAC

Soberanía de datos y geovallado

Registros de auditoría i ntegrales con integración SIEM

Implementación del estándar OpenTDF

Controles de retención y vencimiento basados en tiempo

Formularios de Datos Seguros

Kiteworks responde a estos requisitos de protección a través de su modelo de implementación en dispositivos virtuales reforzados con múltiples capas de defensa, incluyendo cifrado doble que cifra los archivos de los clientes en reposo para minimizar la superficie de ataque. La plataforma implementa estándares de cifrado de nivel empresarial mediante un firewall de red integrado que bloquea los puertos no utilizados y un firewall de aplicaciones web integrado que proporciona protección automatizada contra amenazas basadas en la web. Para la protección persistente de datos, Kiteworks implementa el Estándar OpenTDF, que ofrece cifrado robusto con políticas de control de acceso basadas en atributos integradas en los datos durante todo su ciclo de vida. Las prácticas integrales de DevSecOps de la plataforma incluyen pruebas de seguridad shift-left y actualizaciones con un solo clic para mantener los parches de seguridad al día, mientras que la detección de configuraciones de riesgo alerta a los administradores sobre posibles configuraciones incorrectas de seguridad que requieren corrección.

Permisos, Transferencias Transfronterizas y Soberanía de Datos

Los Artículos 19 y 25 establecen requisitos estrictos para las transferencias internacionales de datos y los intercambios de datos entre instituciones públicas, exigiendo niveles de protección adecuados para los flujos transfronterizos y finalidades legítimas para el intercambio interinstitucional de datos. Los Artículos 23, 24 y 30 requieren controles específicos: el Artículo 23 regula el tratamiento de datos sobre asuntos penales; el Artículo 24 aborda el equilibrio entre el acceso a la información pública y la protección de datos; y el Artículo 30 establece el derecho de los titulares a oponerse al tratamiento por razones relacionadas con su situación particular. Los Artículos 4, 6 y 7 imponen principios de privacidad desde el diseño, mecanismos de consentimiento transparentes y protecciones especiales para los datos de menores. Kiteworks aplica estos requisitos de control a través del Motor de Políticas de Datos (DPE), que combina políticas ABAC en tiempo de ejecución y controles RBAC que regulan el acceso en función de los roles de los usuarios, los atributos de los datos y los factores contextuales. Las capacidades de soberanía de datos de la plataforma restringen el almacenamiento y el enrutamiento de datos a ubicaciones geográficas asignadas a través de atributos LDAP o SAML, mientras que los controles de geovallado limitan el acceso según la ubicación del usuario determinada por la dirección IP. Para la gestión del consentimiento, los Formularios de Datos Seguros permiten a las organizaciones recopilar datos estructurados con requisitos de autenticación configurables y políticas de términos de servicio que los usuarios deben aceptar antes de acceder a los datos protegidos. La plataforma aplica el principio de mínimo privilegio, asignando a los usuarios únicamente los permisos necesarios mediante perfiles asignados e invitaciones explícitas a los datos.

Registros de Auditoría, Retención y Derechos de los Titulares de Datos

El Artículo 17 exige la notificación de brechas a las autoridades supervisoras en un plazo de 72 horas, lo que requiere capacidades integrales de detección e información de incidentes. El Artículo 4 establece los principios de minimización de datos y limitación de los períodos de retención, exigiendo que los datos se conserven únicamente el tiempo necesario para los fines del tratamiento, con plazos a determinar por la autoridad supervisora. Los Artículos 27, 28 y 33 otorgan a los titulares de datos derechos específicos: el Artículo 27 establece el derecho a la información sobre el tratamiento de los datos; el Artículo 28 confiere el derecho a acceder a los datos personales y obtener copias; y el Artículo 33 establece el derecho a revisar e impugnar las decisiones automatizadas que afectan sus intereses. Kiteworks cumple estas obligaciones de seguimiento mediante registros de auditoría integrales que envían datos en tiempo real a sistemas SIEM, incluyendo QRadar, LogRhythm, ArcSight y Splunk a través de syslog, para la detección inmediata de amenazas y la presentación de informes regulatorios. La plataforma proporciona Notificaciones de Inteligencia de Amenazas que alertan a los administradores sobre riesgos de seguridad en tiempo real a través de banners en la consola de administración. Para el cumplimiento de la retención, los controles de tiempo y vencimiento eliminan automáticamente archivos y carpetas tras los períodos configurados, manteniendo registros de auditoría anonimizados que protegen la privacidad mediante sustitución por UUID. Los usuarios finales acceden a la información de seguimiento a través del panel de información y actividad registrada, que muestra quién accedió a sus datos y qué acciones se realizaron, con registros de auditoría exportables que incluyen marcas de tiempo para todas las interacciones de archivos y correos electrónicos entre usuarios internos y externos.

Kiteworks responde a los multifacéticos requisitos de la Ley N.º 7593/2025 a través de capacidades integradas que abarcan los tres ámbitos fundamentales de cumplimiento de la regulación. Para las obligaciones de protección de datos establecidas en los Artículos 4, 9 y 16, Kiteworks despliega dispositivos virtuales reforzados con cifrado doble, firewalls integrados e implementación del Estándar OpenTDF para proteger los datos personales contra el acceso no autorizado y las brechas de seguridad. Para cumplir con los mandatos de control de acceso de los Artículos 19, 23, 25 y 30, la plataforma aplica permisos granulares a través de su DPE que combina controles ABAC y RBAC, mientras que las funciones de soberanía de datos y el geovallado restringen las transferencias transfronterizas y garantizan los controles jurisdiccionales adecuados. Para los requisitos de seguimiento y retención establecidos en los Artículos 17, 22 y 27–33, Kiteworks ofrece registros de auditoría integrales con integración SIEM en tiempo real, políticas de retención automatizadas y seguimiento de actividad accesible para los usuarios que permite tanto la presentación de informes regulatorios como el cumplimiento de los derechos de los titulares de datos. A medida que las organizaciones se preparan para la implementación de la ley dentro del período de transición de 24 meses, Kiteworks ofrece una plataforma unificada que transforma las complejas obligaciones de protección de datos del Paraguay en controles de seguridad operacionalizados, posicionando a las empresas para cumplir con sus plazos de conformidad y mantener una colaboración segura en todos los intercambios de datos regulados.