

Kiteworks apoya la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, Ley N.º 8968

SafeVIEW y el motor de políticas de datos convierten los derechos de acceso de Costa Rica en controles ejecutables

SOLUCIONES DESTACADAS



Doble cifrado robusto



Firewall de aplicaciones web integrado



Detección de intrusiones y anomalías



SafeVIEW y SafeEDIT



Formularios de datos seguros



Motor de políticas de datos con ABAC



Registro de auditoría inmutable

VISIÓN GENERAL

La Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales de Costa Rica, Ley N.º 8968, fue promulgada el 7 de julio de 2011 y publicada en La Gaceta N.º 170 el 5 de septiembre de 2011. Conforme al [Artículo 1](#), esta ley protege a las personas físicas sin importar su nacionalidad, residencia o domicilio. El [Artículo 2](#) establece el ámbito material: la ley se aplica a los datos personales contenidos en bases de datos automatizadas o manuales de organizaciones públicas o privadas. El [Artículo 28](#) establece una estructura de sanciones de tres niveles: las faltas leves conllevan multas de hasta cinco salarios base, las faltas graves de cinco a veinte salarios base y las faltas muy graves de quince a treinta salarios base de un puesto auxiliar judicial, además de la suspensión del funcionamiento de la base de datos de uno a seis meses por faltas muy graves. Kiteworks apoya a las organizaciones que trabajan para cumplir con la ley de protección de datos de Costa Rica. Así es cómo:

01 – ARQUITECTURA DE SEGURIDAD

Proteja los datos con una arquitectura de brecha asumida

El [Artículo 10](#) exige que los responsables de las bases de datos adopten las medidas técnicas y organizativas necesarias para proteger la seguridad de los datos personales y prevenir su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizados. Kiteworks implementa una arquitectura de brecha asumida mediante el doble cifrado de archivos y discos que minimiza las superficies de ataque incluso si los intrusos obtienen acceso al sistema operativo. El firewall de aplicaciones web integrado de la plataforma funciona como una barrera sin gestión frente a toda actividad ajena a Kiteworks, incluido el tráfico de red sospechoso, las firmas de ataque conocidas, la inyección SQL, la exfiltración y los intentos de comando y control. La detección de intrusiones y anomalías basada en IA mantiene una biblioteca de patrones en constante evolución para detectar actividades sospechosas en la red y dentro del dispositivo virtual de Kiteworks. Estas defensas en capas se alinean con los estándares del Marco de Ciberseguridad del NIST para proteger los datos personales frente a todo el espectro de amenazas especificadas en el [Artículo 10](#).

Derechos del titular de los datos a través de ocho artículos de control

Los [Artículos 5, 6, 7 y 14](#) establecen derechos integrales del titular de los datos que exigen consentimiento expreso, controles de calidad de los datos, derechos de acceso y rectificación, y restricciones de transferencia. Los Formularios de Datos Seguros de Kiteworks generan endpoints HTTPS únicos para cada instancia de formulario, lo que permite una recopilación de consentimiento conforme con opciones de autenticación para el envío público o basado en SSO, creando archivos PDF legibles por personas para cada envío almacenados en carpetas compartidas seguras. El cumplimiento de SCIM 2.0 de la plataforma habilita la gestión centralizada de identidades para mantener la exactitud de los datos según los requisitos de exactitud del [Artículo 6](#). SafeVIEW ofrece acceso de solo lectura con descargas opcionales con marca de agua, mientras que SafeEDIT permite la edición sin posesión, en la que los documentos nunca abandonan el entorno seguro de Kiteworks, cumpliendo con los derechos de acceso, rectificación, supresión y consentimiento para la cesión del [Artículo 7](#). Para los controles de transferencia del [Artículo 14](#), la plataforma aplica controles de acceso basados en atributos según los atributos del activo de datos, los atributos del usuario y las acciones solicitadas, con un intercambio seguro de archivos mediante paquetes protegidos por ACL, controles de caducidad, requisitos de autenticación y marcas de agua de huella digital. Los controles de acceso basados en tiempo y la programación de limpieza de retención garantizan la vigencia de los datos según el [Artículo 6](#), mientras que las capacidades de retirada de archivos por parte legal/administrativa con eliminación con registro de motivos respaldan los derechos de rectificación.

03 – REGISTRO DE AUDITORÍA

Requisitos de registro de auditoría conforme a la Ley 8968

Aunque la Ley 8968 no contiene un mandato explícito de registro de auditoría, el cumplimiento depende de documentación que pueda producirse a demanda. El [Artículo 16](#) otorga a la Prodhab acceso de inspección a las bases de datos y los protocolos de tratamiento, el [Artículo 7](#) exige a las organizaciones demostrar qué datos existen y cómo se han tratado, y el [Artículo 25](#) establece plazos de respuesta a reclamaciones de tres días. Kiteworks aborda estas obligaciones implícitas de conservación de registros mediante un registro de auditoría consolidado que captura [632 tipos de eventos distintos](#) —incluidos el acceso a archivos, las cargas, las descargas, los inicios de sesión, las acciones administrativas y las actividades de MFT— exportable a cualquier SIEM mediante syslog, con integraciones nativas para Splunk, IBM QRadar, ArcSight y LogRhythm. Este registro integral documenta la recopilación de consentimiento, las respuestas de acceso del titular de los datos, las autorizaciones de transferencia y el acceso al sistema en el formato que requieren los inspectores de la Prodhab.

RESUMEN

Por qué Kiteworks para la Ley N.º 8968

Kiteworks proporciona la base técnica que exige la Ley N.º 8968 de Costa Rica en tres dimensiones críticas para su aplicación. La arquitectura de brecha asumida de la plataforma —doble cifrado de archivos y discos, WAF integrado y detección de anomalías basada en IA— cumple con el mandato integral de seguridad del [Artículo 10](#). Los Formularios de Datos Seguros, la gestión de identidades conforme a SCIM, SafeVIEW, SafeEDIT y los controles de transferencia basados en atributos operacionalizan los derechos de acceso, rectificación, supresión y consentimiento para la cesión garantizados en los [Artículos 5, 6, 7 y 14](#). Y un registro de auditoría consolidado que captura 632 tipos de eventos distintos, con exportación a SIEM en tiempo real, prepara a las organizaciones para responder a las inspecciones de la Prodhab, satisfacer los requisitos de transparencia del tratamiento del [Artículo 7](#) y cumplir con los plazos de respuesta a reclamaciones de tres días del [Artículo 25](#). A medida que las organizaciones navegan la estructura de sanciones de tres niveles de la Ley N.º 8968 —multas de hasta treinta salarios base y suspensión de la base de datos para las infracciones más graves—, Kiteworks funciona como la plataforma unificada donde las capacidades de protección, control y auditoría convergen para salvaguardar los datos personales en todas las operaciones reguladas.

Copyright © 2026 Kiteworks. La misión de Kiteworks es empoderar a las organizaciones para gestionar eficazmente el riesgo en cada envío, intercambio, recepción y uso de datos privados. La plataforma Kiteworks ofrece a los clientes un intercambio seguro de datos que brinda gobernanza, cumplimiento y protección de datos en un plano de control unificado. Kiteworks unifica, rastrea, controla y protege los datos sensibles que se mueven dentro, hacia y fuera de su organización, mejorando significativamente la gestión de riesgos y garantizando el cumplimiento normativo en todos los intercambios de datos privados. Con sede en Silicon Valley, Kiteworks protege a más de 100 millones de usuarios finales y a miles de empresas y organismos gubernamentales de todo el mundo.