Kiteworks

RESUMEN DE CUMPLIMIENTO

Kiteworks Apoya el Cumplimiento de la Protección de Datos Personales bajo la Ley N.º 29733 y el Decreto Supremo N.º 016-2024-JUS

Cómo Kiteworks ayuda a las organizaciones a cumplir los requisitos actualizados de protección de datos personales

La Ley N.º 29733, Ley de Protección de Datos Personales, establece el marco legal para la protección de datos personales en el Perú, garantizando el derecho fundamental de las personas a controlar la manera en que las organizaciones recopilan, procesan, almacenan y transfieren su información personal. La ley es de aplicación en todo el Perú y tiene alcance extraterritorial respecto de cualquier organización, nacional o extranjera, que trate datos personales de residentes peruanos o utilice medios ubicados en territorio peruano. Todos los sectores deben cumplirla, incluyendo los servicios financieros, las telecomunicaciones, la salud, la tecnología y la administración pública. Promulgada en 2011 y significativamente fortalecida mediante el Decreto Supremo N.º 016-2024-JUS, publicado el 30 de noviembre de 2024, el Reglamento actualizado entró en vigor 120 días calendario después de su publicación, con los requisitos de designación del Oficial de Datos Personales implementándose de forma progresiva entre uno y cuatro años según el tamaño de la empresa. Las organizaciones que incumplan enfrentan multas administrativas escalonadas por gravedad, medidas correctivas obligatorias y daño reputacional derivado de su inclusión en el registro público de sanciones. Kiteworks permite a las organizaciones cumplir los requisitos de la Ley N.º 29733 y del Decreto Supremo N.º 016-2024-JUS a través del intercambio seguro de archivos, las transferencias de datos gobernadas y las capacidades integrales de auditoría, tal como se detalla a continuación.

Appliance Virtual Reforzado y Cifrado para las Obligaciones de Seguridad Técnica

Los artículos 9 y 16 de la Ley N.º 29733, complementados por los artículos 48, 51 y 52 del Decreto Supremo N.º 016-2024-JUS, exigen a los titulares de bancos de datos personales adoptar medidas técnicas que prevengan la alteración, pérdida y acceso no autorizados, con controles de infraestructura alineados a la NTP-ISO/IEC 27001:2022. Kiteworks se despliega como un appliance virtual reforzado de un solo tenant con una superficie de ataque minimizada, gestión automatizada de parches, detección de intrusiones y análisis continuo de vulnerabilidades. Todos los datos personales en reposo se cifran con AES-256, y las organizaciones pueden utilizar sus propias claves de cifrado con soporte HSM para mantener la custodia completa de las claves. TLS 1.2 y 1.3 protege cada transmisión, mientras que la verificación de integridad automatizada basada en hash confirma la completitud de las copias de respaldo con una frecuencia mínima semanal, conforme lo exige el artículo 51. Para las transferencias electrónicas que salen de la infraestructura organizacional, Kiteworks aplica controles de autorización, utiliza certificados digitales y realiza verificación mediante checksum en todos los archivos enviados, satisfaciendo directamente los requisitos del artículo 52 sobre transferencias cifradas con firmas digitales y checksums de verificación.

Aspectos destacados de la solución

Appliance virtual reforzado de un solo tenant

Cifrado AES-256 con BYOK y soporte HSM

Control de acceso basado en roles y en atributos (RBAC y ABAC)

Motor de Políticas de Datos (DPE)

Retención y eliminación automatizada

Formularios de Datos Seguros

Registro de auditoría inmutable

Integración con SIEM en tiempo real

Motor de Políticas de Datos y Gobernanza de Acceso para los Requisitos de Consentimiento y Ciclo de Vida del Dato

El artículo 46 del Decreto Supremo N.º 016-2024-JUS exige a las organizaciones documentar e implementar la gestión del ciclo de vida del acceso con verificación periódica de privilegios con una frecuencia mínima semestral, mecanismos de autenticación multifactor que incluyan certificados digitales y tokens de hardware, y controles técnicos que impidan la reproducción no autorizada de datos. Los artículos 28 y 38 de la Ley N.º 29733 exigen que los bancos de datos personales almacenen la información de manera que permita el ejercicio de los derechos de sus titulares y que eliminen los datos automáticamente al vencimiento de los plazos de retención. Kiteworks atiende estas obligaciones mediante el control de acceso basado en roles (RBAC) y el control de acceso basado en atributos (ABAC), restringiendo a cada usuario al acceso que su rol autoriza expresamente, con flujos de trabajo automatizados de revisión semestral de privilegios que generan resultados de certificación documentados. El Motor de Políticas de Datos (DPE) aplica calendarios de retención configurables por clasificación de datos y espacio de trabajo, identificando y eliminando automáticamente los datos al vencer su plazo sin intervención manual. Para el consentimiento de datos sensibles conforme al artículo 13, numeral 6 de la Ley N.º 29733 y al artículo 8 del Reglamento, los Formularios de Datos Seguros de Kiteworks capturan los datos, almacenando los registros de consentimiento con doble cifrado reforzado, identificador de referencia y datos de fecha y hora.

Registro de Auditoría de Cumplimiento e Integración con SIEM para la Documentación de Incidentes y la Trazabilidad

El artículo 46 del Decreto Supremo N.º 016-2024-JUS establece que las organizaciones deben conservar registros de trazabilidad de todas las interacciones lógicas con los datos personales por un periodo mínimo de dos años, disponibles de manera inmediata a requerimiento. El artículo 35 exige que todo incidente de seguridad sea documentado con detalle completo de los hechos, sus efectos y las medidas adoptadas, para permitir la verificación por parte de la Autoridad Nacional de Protección de Datos Personales. Kiteworks genera un registro de auditoría de cumplimiento a prueba de manipulaciones que captura cada interacción con los datos personales, incluyendo eventos de procesamiento, visualización, modificación, eliminación, importación y exportación, cada uno con marca de tiempo y atribuido a un usuario autenticado específico con horas de inicio y cierre de sesión. Todos los registros se conservan por un periodo configurable que satisface el mínimo legal de dos años y se exportan en tiempo real a plataformas SIEM incluyendo QRadar, LogRhythm, ArcSight y Splunk. Cuando ocurre un incidente de seguridad, el registro de auditoría suministra de manera inmediata el paquete de documentación exigido por el artículo 34, incluyendo las categorías de datos afectados, el número aproximado de titulares involucrados y todas las acciones de remediación con sus marcas de tiempo, proporcionando a las organizaciones la base probatoria para cumplir el plazo de notificación de 48 horas a la Autoridad Nacional.

Kiteworks ofrece a las organizaciones que operan bajo la Ley N.º 29733 y el Decreto Supremo N.º 016-2024-JUS una plataforma unificada para satisfacer los tres dominios de cumplimiento centrales del Reglamento. Su infraestructura reforzada y el cifrado de extremo a extremo atienden las obligaciones de seguridad técnica aplicables a los datos personales, mientras que las herramientas integradas de gobernanza de acceso hacen cumplir los controles del ciclo de vida del consentimiento y las políticas automatizadas de retención de datos que exige el Reglamento. Cuando ocurre un incidente de seguridad, el registro de auditoría a prueba de manipulaciones produce de manera inmediata la documentación que requiere la Autoridad Nacional de Protección de Datos Personales, y la integración con SIEM en tiempo real mantiene a los equipos de operaciones de seguridad equipados para cumplir el plazo de notificación de 48 horas. En materia de protección, control y trazabilidad, Kiteworks traduce los requisitos legales actualizados del Perú en controles técnicos verificables y auditables que las organizaciones pueden demostrar ante los reguladores con plena confianza.