Kiteworks

RESUMEN DE CUMPLIMIENTO

Kiteworks y la Ley No. 172-13 de la República Dominicana: Protección de Datos Personales

Cómo Kiteworks Habilita el Manejo Seguro de Datos, los Derechos de los Titulares y los Controles Transfronterizos bajo el Marco de Protección de Datos Personales de la República Dominicana

La Ley No. 172-13 sobre Protección de Datos de Carácter Personal, promulgada por el Congreso de la República Dominicana el 13 de diciembre de 2013 y publicada en la Gaceta Oficial No. 10737 el 15 de diciembre de 2013, establece requisitos integrales de protección de datos para todas las entidades públicas y privadas que traten datos personales dentro del territorio dominicano. La ley aplica a entidades gubernamentales, empresas privadas de todos los sectores, incluyendo finanzas, salud, telecomunicaciones y comercio minorista, así como a las Sociedades de Información Crediticia que manejan datos de historial crediticio. La regulación cubre toda la República Dominicana y aplica a cualquier organización que mantenga bases de datos, registros públicos o sistemas técnicos de procesamiento de datos que contengan información personal. Las organizaciones enfrentan sanciones administrativas por incumplimiento, incluidas multas que van de 10 a 100 veces el salario mínimo nacional y, en el caso de infracciones graves, sanciones penales que incluyen prisión de seis meses a dos años. La Superintendencia de Bancos es designada como el organismo de control para las Sociedades de Información Crediticia bajo el Artículo 29; fuera del sector de informes crediticios, no se ha establecido una autoridad nacional de protección de datos. Kiteworks apoya a las organizaciones que trabajan hacia el cumplimiento de la Ley No. 172-13. A continuación se explica cómo:

Protección de Datos Personales en Tránsito y en Reposo

El Artículo 5 establece que los responsables del tratamiento deben implementar medidas técnicas, organizativas y de seguridad para salvaguardar los datos personales y prevenir alteraciones, pérdidas o accesos no autorizados. El Artículo 13 refuerza este requisito, exigiendo que las organizaciones mantengan la información bajo las condiciones de seguridad necesarias para evitar adulteraciones, pérdidas o consultas no autorizadas. El Artículo 54 requiere que las Sociedades de Información Crediticia presenten manuales de seguridad a la Superintendencia de Bancos detallando las medidas mínimas de seguridad para el transporte de datos, seguridad física, logística y protección de comunicaciones, mientras que el Artículo 63 exige que las SIC adopten las medidas de seguridad y control necesarias y protejan sus algoritmos y tecnologías. Kiteworks se implementa como un dispositivo virtual reforzado que contiene todos los archivos y el software necesarios dentro de múltiples capas de protección que minimizan la superficie de ataque. La plataforma implementa doble cifrado para los archivos de los clientes en reposo, cifrando tanto los archivos individuales como el almacenamiento de disco subyacente para proteger contra intrusos que obtienen acceso al sistema operativo.

Aspectos destacados de la solución

- **Doble cifrado robusto**
- **Cifrado TLS 1.2+**
- **Autenticación multifactor**
- **Controles de acceso RBAC y ABAC**
- **Registros de auditoría integrales con integración SIEM**
- **Controles de geovalla y soberanía de datos**

Para los datos en tránsito, Kiteworks emplea protocolos de cifrado TLS 1.2+ con cifrado AES-256 por defecto. El firewall de red integrado bloquea todos los puertos no utilizados del tráfico externo, mientras que el antivirus F-Secure incorporado pone en cuarentena el malware al momento de carga y descarga. Los mecanismos de autenticación incluyen autenticación basada en credenciales, autenticación basada en certificados (CBA), autenticación multifactor (MFA) e integración de inicio de sesión único SAML 2.0 con Microsoft Entra ID.

Gestión del Control de Acceso y los Derechos de los Titulares de Datos

Los Artículos 8, 10 y 14 otorgan a los titulares de datos derechos de acceso, rectificación, actualización y solicitud de eliminación de sus datos personales, mientras que los Artículos 11 y 12 establecen procedimientos específicos para que las Sociedades de Información Crediticia proporcionen informes crediticios dentro de cinco días hábiles. El Artículo 21 requiere que las organizaciones mantengan un seguimiento adecuado durante los procedimientos de hábeas data. El Artículo 13 exige que el acceso a la información se restrinja únicamente a personas autorizadas. Kiteworks habilita estos requisitos a través de su API REST, permitiendo a las organizaciones desarrollar aplicaciones personalizadas para gestionar solicitudes de titulares de datos e integrarlas con los flujos de trabajo existentes. El cumplimiento con SCIM 2.0 (Sistema de Gestión de Identidad entre Dominios) permite la gestión centralizada de cuentas a través de soluciones externas de gestión de identidad, facilitando actualizaciones y eliminaciones oportunas. Los Formularios de Datos Seguros recopilan datos estructurados aprovechando las políticas de seguridad centralizadas y el registro de auditoría unificado. Para los procedimientos de acceso, la plataforma genera puntos de conexión HTTPS únicos para cada instancia de formulario, admitiendo envíos de formularios públicos autenticados y no autenticados según la configuración. El control de acceso basado en roles (RBAC) garantiza que las operaciones de IA hereden los permisos del usuario autenticado, evitando el acceso más allá de los niveles de autorización. El control de acceso basado en atributos (ABAC) evalúa atributos de archivos, atributos de usuarios y atributos contextuales para aplicar decisiones de acceso detalladas. El sistema de registro de auditoría integral limpia, normaliza, estandariza y agrega automáticamente todas las actividades relacionadas con la seguridad y el cumplimiento en un único flujo, con etiquetado automático de archivos de datos al ingresar al sistema a través de cargas web, correo electrónico, API o complementos.

Control de Transferencias Transfronterizas de Datos

El Artículo 6 (numeral 20) define las transferencias internacionales de datos como el tratamiento que implica la transmisión de datos fuera del territorio dominicano, mientras que el Artículo 6 (numerales 13 y 15) define a los importadores y exportadores de datos. El Artículo 80 establece las condiciones bajo las cuales se permiten dichas transferencias, incluidos los requisitos de adecuación para el país receptor y la autorización libre y consciente del titular de los datos. El Artículo 27 establece excepciones para el tratamiento de datos de salud y procedimientos de disociación. Kiteworks implementa estos controles a través de su Motor de Políticas de Datos, que aplica políticas dinámicas basadas en atributos de los activos de datos, atributos del remitente y del destinatario, y acciones del usuario. Para las transferencias internacionales, la plataforma ofrece capacidades de geovalla que restringen el inicio de sesión según la configuración geográfica a nivel de usuario individual, perfil o sistema. El Servidor MFT se conecta a repositorios de almacenamiento, recursos compartidos de archivos en la nube y aplicaciones empresariales, admitiendo además la integración directa de Kiteworks a Kiteworks que evita protocolos intermediarios menos seguros. Para los datos de salud bajo las excepciones de cooperación médica del Artículo 27, el Formato de Datos de Confianza (TDF) de Kiteworks permite transferencias seguras entre hospitales, clínicas, investigadores y compañías de seguros, con controles alineados con HIPAA a través del cifrado persistente basado en OpenTDF y ABAC. Esto proporciona cifrado persistente con políticas de control de acceso basadas en atributos incorporadas, lo que permite a los remitentes definir el acceso según la habilitación de seguridad, la afiliación organizacional, la ubicación o el rol operativo. Para las transferencias financieras, TDF asegura datos de transacciones financieras, registros y registros de auditoría entre instituciones, reguladores y socios con control granular. Los registros de auditoría de la plataforma mantienen los estándares de privacidad al tiempo que permiten la revisión del administrador cuando se requiere verificación detallada.

Kiteworks proporciona a las organizaciones capacidades integrales para abordar los multifacéticos requisitos de la Ley No. 172-13 en materia de protección de datos, control de acceso y gestión de transferencias. Para las obligaciones de protección, la plataforma ofrece seguridad reforzada mediante doble cifrado en reposo, cifrado TLS en tránsito y autenticación multifactor, incluidas opciones biométricas requeridas para las Sociedades de Información Crediticia. Para los requisitos de control, Kiteworks habilita los derechos de los titulares de datos a través de API REST e integración SCIM 2.0, al tiempo que aplica un acceso granular mediante marcos RBAC y ABAC con registros de auditoría integrales. Para el tratamiento transfronterizo, la plataforma implementa geovallas, transferencias internacionales seguras a través del Servidor MFT y cifrado en Formato de Datos de Confianza con políticas de acceso incorporadas para intercambios de datos de salud y financieros. A través de este enfoque de plataforma unificada, Kiteworks empodera a las organizaciones del sector público y privado de la República Dominicana para mantener el cumplimiento mientras gestionan de forma segura los datos personales a lo largo de su ciclo de vida.