

Kleos

el entorno de trabajo más seguro

La seguridad es nuestra mayor prioridad. Trabajamos con los líderes y estamos certificados, junto con nuestros partners, en los últimos estándares de la industria.

Kleos es el entorno de trabajo más seguro para tus datos. Los datos de tu empresa y de tus clientes están protegidos y aislados, por lo que sólo será accesible por ti. De esa manera, se pueden mantener los más altos estándares de privacidad y confidencialidad con tus propios clientes.

Los datos están alojados en una empresa certificada de Deutsche Telekom, con servidores ubicados en Alemania y que cumple con las reglas de privacidad de datos de la UE y con los más altos estándares de seguridad del mercado. La granja se controla continuamente 24/7, **con sistemas de acceso restringidos y controlados tanto en edificios y sistemas como en servidores, los cuales están protegidos contra intrusiones y accidentes.** Nos aseguramos de que haya alta disponibilidad, continuidad del negocio, recuperación de desastres y copia de seguridad nocturna de datos. Kleos también está certificado con auditorías de seguridad diarias del sitio web y de transmisión de datos encriptados HTTPS:



Además de los piratas informáticos, la mayoría de los problemas de seguridad se deben a errores humanos o infidelidades. Por ello, ponemos tanto énfasis en los “procedimientos de gestión de seguridad y personas” como en el aspecto técnico, es por eso que contamos con la certificación **ISO 27001**.

El lugar más seguro para tus datos.



SITIO WEB SEGURO Y CERTIFICADO

El sitio web está protegido contra virus, malware, y phishing por McAfee y Norton, que examinan también otros tipos de vulnerabilidad



CONEXION HTTPS SEGURA Y CERTIFICADA DURANTE LA TRANSFERENCIA DE DATOS

la transmisión HTTPS de datos se cifra con un certificado PKI de 2048 bits y está certificada por Norton



Autenticación

CENTRO DE DATOS SEGURO WK DE ALTA CALIFICACIÓN, GRANJA CERTIFICADA EN UE

- Centro de datos **ubicado en Alemania**, con alojamiento dedicado para Wolters Kluwer por **T-Systems** (Deutsche Telekom)
- Cumple con las **normas de protección de datos de la UE**
- Certificados en más altos estándares del mercado de seguridad e informes **(ISO 27001, SAS-70Tipo II)**
- Alta disponibilidad, Continuidad del Negocio y **24/7 sistema de monitoreo**
- **Copia de seguridad cifrada y réplicas de recuperación de desastres en un sitio remoto**
- No hay conexión de datos para personas no autorizadas
- Los **datos de cada cliente están aislados con una instancia privada**
- Los **edificios y los servidores protegidos contra intrusiones y ataques**



Firewall



PREGUNTAS FRECUENTES

¿Es la nube lo suficientemente segura?

La seguridad se aumenta al utilizar soluciones en la nube, debido a los estrictos estándares de seguridad que los proveedores de nube deben cumplir, además de las auditorías de seguridad y la presentación de informes que se hacen regularmente. Esto significa que no habrá más preocupaciones acerca de portátiles perdidos con datos confidenciales y amenazas de piratería o copias de seguridad perdidas. Y Kleos se encuentra dentro de los sitios más seguros con la mayor calificación y certificación de seguridad en el almacenamiento de datos, transmisión y acceso.

¿Realiza controles de seguridad Kleos?

El sistema de Kleos está continuamente monitorizado

- Controles precisos 24/7 de seguimiento del sistema y rendimiento de la aplicación.
- Se realizan pruebas de intrusión cada año por una empresa externa independiente.
- Por otra parte, el sistema de detección de intrusiones está siempre disponible y da alarmas en tiempo real
- La página web Kleos también está certificada
 - *Certifica que el sitio web es seguro y resistente a virus e intrusiones, protegido contra ataques de piratas informáticos en servidores y transmisiones.*
 - *Se notifica en tiempo real acerca de cualquier riesgo que pudiera ocurrir de manera que podamos bloquear cualquier ataque inmediato.*
 - *Se puede ver el certificado en <https://www.mcafeesecure.com/verify?host=kleos.wolterskluwer.com>*
- Norton Symantec controla continuamente la transmisión de datos cifrados a través de certificado SSL
 - *Mensualmente se lleva a cabo un “análisis de vulnerabilidades”.*
 - *Se puede ver el certificado en https://trustsealinfo.verisign.com/splash?form_file=fd/splash.fdf&dn=kleos.wolterskluwer.*
- El acceso a datos de Kleos es limitado, con control de personas y procesos en la granja y en nuestras oficinas
 - *La Granja de T-System y Wolters Kluwer están certificados en ISO 27001*
 - *Hemos puesto en marcha más de un centenar de controles sobre los servicios Kleos basado en la norma ISO 27001*
 - *Tenemos procedimientos específicos ISO 27001 para la gestión de la seguridad en los servicios Kleos como soporte de tercer nivel, infraestructura, aseguramiento de calidad*

¿Expira el valor de las certificaciones en algún momento?

- No
- McAfee y Norton de Symantec aseguran chequeos continuos mensualmente / diariamente del sitio web de Kleos y de la transmisión de datos.
- Mientras mantenemos nuestro nivel de seguridad, Kleos será certificado.
- Si se produce algún ataque, McAfee y Norton nos alertan de inmediato para que podamos actuar y bloquearlo, para mantener sus datos seguros.
- Las certificaciones del Data Center se renuevan y se verifican cada año en la certificación ISO 27001. Nuestro servicio para Kleos es verificado, renovado y ampliado cada año



¿Dónde están mis datos alojados, y cómo están protegidos?

Kleos utiliza los más avanzados servicios de seguridad de alojamiento de datos en la granja Deutsche Telekom / T-Systems:

- T-Systems es una empresa certificada de Deutsche Telekom, con servidores ubicados en la UE (en Alemania) y compatible con las normas de protección de datos de la UE y los más altos valores estándares del mercado.
- Otorga certificados de seguridad internacional, alineados con los más altos estándares del mercado (ISAE 3470, ISO / IEC 27001, SAS-70 Tipo II)
- Continuamente monitorizado 24/7
- Alta disponibilidad, continuidad del negocio y recuperación de desastres:
 - *Los datos de los clientes están siempre accesibles: cada componente tecnológico de Kleos es, en cualquier capa, totalmente redundante*
 - *Se puede acceder a los Documentos del Cliente también en el remoto en caso de indisponibilidad del servicio, gracias a un servicio de “modo seguro”*
 - *Los datos del cliente se replican a otro centro de datos T-System “espejo” (geográficamente separados, pero también en Alemania), para ser recuperado en caso de desastre en el principal centro de datos.*
- Incidentes, problemas y gestión del cambio con respecto a la infraestructura Kleos se gestionan a través de procesos específicos basados en ITIL v3 para proteger los datos.
- Los datos de los clientes siempre están guardados en copias de seguridad para ser protegidos por cualquier tipo de accidentes.
- Acceso restringido y controlado a todos los edificios en los centros de datos, están protegidos contra intrusiones y accidentes.
 - *El acceso a los edificios está bajo las normas más estrictas y solo se permite el acceso a las personas autorizadas propietarias de una tarjeta inteligente personalizada.*
 - *Los edificios están diseñados para soportar el bombardeo C4, seguridad de alta incursión.*
- Acceso restringido y controlado a los sistemas y servidores:
 - *El acceso a los sistemas y servidores está bajo las más estrictas normas y se deja sólo acceder a los administradores autorizados.*
 - *Los administradores, para acceder a los sistemas, deben poseer una cuenta específica.*
 - *Pueden tener acceso al sistema sólo por razones de mantenimiento y a los datos únicamente con la autorización explícita por parte del cliente.*
 - *Cualquier acceso se registra y guarda de forma permanente a través de un servicio de certificación externa cumpliendo con la Ley de Protección de Datos.*

¿Qué pasa con mis datos durante la transferencia a la granja?

Kleos certifica el acceso, la comunicación de datos de los clientes (carga / descarga), la encriptación y el aislamiento

- Los datos desde el cliente al servidor se cifran con un certificado PKI 2048 bits
- Se evitan las técnicas de secuestro en el tráfico.
- Los datos son aislados, cada cliente tiene una instancia privada física. Nada se comparte con otros clientes.
- El acceso a los datos del cliente desde Internet está controlado en última instancia por la propia aplicación con un conjunto de credenciales.
- El Firewall, protección contra virus y corrupción de los datos impiden intrusiones de datos que vienen hacia el interior del centro de datos y se filtra por dispositivos de hardware especializados que realizan tanto inspección de paquetes (SPI) como de detección de intrusiones (ID).



Contacto:
Wolters Kluwer
C/ Collado Mediano 9
28231 Las Rozas de Madrid
España
902 250 500
clientes@wolterskluwer.com
www.kleos.wolterskluwer.com/es/