

Kleos: Es el lugar más seguro para tus datos.

El Wolters Kluwer, la seguridad y la privacidad de tus datos son nuestra mayor prioridad. Kleos cumple los mejores estándares de la industria y todos los días se inspecciona y certifica.

Kleos aísla y protege tus despachos y los datos de tus clientes, evitando el acceso no autorizado. Con Kleos tus clientes se benefician de los mejores estándares de privacidad.

Con Kleos todos tus datos residen en la nube y pueden guardarse con un solo clic. Todos tus datos se guardan en servidores de seguridad de grado bancario, alojados en EU e ISO 27001 certificados.

Cada día se realizan copias de seguridad automatizadas y el lugar de los servidores es monitorizado 24/7 y protegidos ante intrusos y accidentes.

Se garantiza alta disponibilidad, continuidad de negocio y recuperación de desastres y copias de seguridad todas las noches. Kleos está certificado con McAfee y Norton Secured con inspecciones diarias del sitio web de HTTPS y la transmisión de datos encriptados.



ISO 27001

Además de ciber ataques y violaciones de datos, probablemente la mayor de las intrusiones son el resultado de errores humanos y utilización inseguro del usuario. En Wolters Kluwer creemos que los procedimientos y las personas son tan importantes para la gestión de la seguridad como el proceso tecnológico. Por eso estamos certificados en ISO 27001.

El sistema de dirección de seguridad ISO 27001 es reconocido globalmente por gestionar los riesgos de la seguridad de la información.

Todos los servicios alrededor de Kleos, apoyo, calidad de análisis y de gestión de infraestructuras están gobernados por un sistema de dirección de información segura, certificado por BSI, autoridad que previene el acceso no autorizado a datos.

El lugar más seguro para tus datos

Sitio web seguro y certificado.

Estando certificados por McAfee y Norton Secured, Kleos asegura la website que utilizas, está protegida ante virus, programas maliciosos, fraude electrónico u otras vulnerabilidades peligrosas.

Conexión 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.**

El centro de datos seguro de Wolters Kluwer está en los primeros del ranking de centros certificados en EU.

- **El centro de datos de mayor ranking en Alemania;** con alojamiento dedicado a Wolters Kluwer por T-Systems (Deutsche Telekom) con capacidad de respuesta inmediata a fallos.
- Cumpliendo con las **normas de protección de datos de la UE.**
- Certificados en los más altos estándares del mercado de seguridad e informes (**ISO 27011, SAS-70 Tipo II**)
- Alta disposición, continuidad del negocio y sistema monitorizado 24/7
- **Copia de seguridad cifrada y réplicas de recuperación de desastres en un sitio remoto.**
- **No permite el acceso a los datos a personas no autorizadas.**
- Los datos de cada cliente son físicamente aislados en un lugar privado y no son accesibles a otros usuarios.
- **Los edificios y los servidores protegidos contra intrusiones y ataques.**

Preguntas frecuentes

¿Es la nube suficientemente segura?

La nube es más segura que otros entornos tradicionales. En la nube tus datos residen lejos de cualquier desastre, protegidos contra intrusiones externas y con copias de seguridad automáticas 24/7.

Tus datos estarán seguros en la nube con un alto grado de seguridad y privacidad, debido a estándares de seguridad a los que los proveedores de la nube se tienen que adherir, además de las inspecciones de seguridad y reportes que deben garantizar.

Esto significa no más preocupaciones por la pérdida de ordenadores portátiles con datos confidenciales, y a los peligrosos ataques de hackers o a la pérdida de copias de seguridad. Y Kleos asegura y certifica el más alto nivel de seguridad en el almacenamiento de datos, transmisiones y accesos.

¿Cada cuánto tiempo se hacen chequeos del rendimiento de la seguridad en Kleos?

- Kleos es monitorizado de forma precisa 24/7: la salud del sistema y rendimiento se comprueban diariamente.
- Cada año una compañía independiente realiza test de intrusión.
- El sistema de detección de intrusos de Kleos está siempre encendido.

¿Tiene Kleos todas las certificaciones necesarias?

McAfee Seguridad inspecciona rigurosamente Kleos todos los días para asegurar que tus datos están protegidos de vulnerabilidades de seguridad y otras amenazas online.

- McAfee certifica que la página web de Kleos es segura y resistente a virus e intrusiones. Protegido contra ataques de piratas informáticos en servidores y transmisiones.
- Se notifica a tiempo real de cualquier riesgo, para que podamos, inmediatamente bloquear cualquier ataque.
- Se puede ver certificado en <https://www.mcafee.com/verify?host=kleos.wolterskluwer.com>.

Norton Symantec monitoriza y valida nuestra transmisión de datos encriptados vía certificado SSL.

- Mensualmente se lleva a cabo un “análisis de vulnerabilidades” y se reporta.
- Se puede ver certificado en https://trustsealinfo.verising.com/splash?form_file=fdf/splash.fdf&dn=kleos.wolterskluwer.com&lang=en

El acceso de datos a Kleos está estrictamente limitado.

- La granja de T-system y Wolters kluwer tienen el certificado ISO 27001.
- Hemos puesto en marcha más de un centenar de controles sobre los servicios Kleos, basados en ISO 27001-Annex A.
- Tenemos procedimientos específicos ISO 27001 para gestionar la seguridad en los servicios de Kleos, como el soporte de tercer nivel, infraestructuras y aseguramiento de calidad.

¿Expiran en algún momento, o pierden valor los certificados?

- No, no lo hacen.
- McAfee y Norton Symantec aseguran chequeos continuos diariamente/mensualmente del sitio web de Kleos y de la transmisión de datos.
- Mientras mantengamos nuestro alto nivel de seguridad de Kleos, permaneceremos certificados.
- Las certificaciones del Data Center se renuevan y verifican cada año.
- La certificación ISO 27001 de Wolters Kluwer en Kleos es verificada, renovada y ampliada todos los días.

¿Dónde están mis datos alojados y cómo están protegidos?

Kleos depende de los servicios de almacenamiento de datos de la más alta calidad y seguridad de Deutsche Telekom.

- Kleos ofrece estándares internacionales de seguridad y es compatible con los más altos estándares del mercado (ISAE 3470, ISO/IEC 27001, SAS-70 Tipo II)
- Alta disponibilidad, continuidad del negocio y recuperación de desastres:
 - Los datos del cliente siempre son accesibles: cada componente tecnológico de Kleos es, en cualquier capa, totalmente redundante.
 - En el extraño caso en que la aplicación falle, los datos críticos del cliente siguen siendo accesibles a través de un servicio de “modo seguro”.
 - La infraestructura de los datos almacenados y los datos del cliente se replican a otro Data Center 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 gestiona a través de procesos específicos basados en ITIL v3 para proteger los datos.
- Los datos del cliente siempre están guardados en copias de seguridad para ser protegidos por cualquier tipo de accidentes.
- Acceso restringido y controlado a todos los edificios de 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 ocurre con mis datos durante la transmisión?

La encriptación y el aislamiento de los datos que están siendo transmitidos (carga/descarga) entre el usuario de Kleos y nuestros servidores es una de las prioridades de Wolters Kluwer.

- 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 anti 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)

