KRITER
SOFTWARE

Arquitectura, privacidad y seguridad de los productos y servicios de Kriter Software: KRITER ERP (onpremise, Cloud), PREK, KriterStore y servicios de sistemas.

Los objetivos principales de Kriter Software en cuanto a la GDPR son dos:

- Ofrecer el máximo nivel posible de seguridad y privacidad de los datos que almacenamos de nuestros clientes.
- Garantizar que nuestros productos y servicios cumplan con los requerimientos técnicos recomendaos en la GDPR.

Esta documentación describe la arquitectura técnica y los controles administrativos, técnicos y físicos aplicables para todos los productos y servicios bajo la marca Kriter Software.

Arquitectura del software

Los productos de Kriter Software operan en una arquitectura “Single Tenant” (una o varias bases de datos por cliente). Las diferentes arquitecturas de nuestros productos proporcionan los mecanismos configuración de acceso y protección de datos necesarios para que sea el cliente el que defina, mediante un esquema de ROL/Usuario, los privilegios de acceso a los mismos.

Control de procesamiento de datos

Kriter Software ha implantado los procedimientos necesarios para asegurar que los datos son procesados exactamente como ha establecido el cliente en toda la cadena de actividades de proceso de datos.

Funcionalidades de terceros

Algunas características de Kriter Software son proporcionadas por Software de terceros. Kriter garantiza que sus datos no serán transmitidos a los mismos sin el consentimiento expreso del cliente.

Auditorías y certificaciones

Todos nuestros productos cumplen con los estándares de calidad del Software certificados con la ISO 15504-5:2012, Software Process Improvement Capability Determintation y ISO 9001:2015. Por otro lado, todos nuestros productos son auditados periódicamente internamente y externamente para garantizar la protección y privacidad de los datos en todo momento.

Controles de seguridad

Todos nuestros productos incluyen un conjunto de controles de seguridad que permiten a nuestros clientes establecer sus propios protocolos de seguridad en cuanto al uso de nuestros productos.

Procedimientos y políticas de seguridad

- Las contraseñas de los clientes se guardan siempre codificadas (HASH).
- Nuestros productos registran todos los accesos al software, cada registro contiene, fecha, hora, usuario, identificador, operación realizada y contra que datos.
- Si hay una sospecha de un acceso inapropiado, Kriter Software ayuda a sus clientes en las tareas de análisis forenses proporcionando acceso al LOG interno del sistema.
- Las contraseñas nunca son guardadas sin encriptar.
- El personal de Kriter Software nunca puede manipular las contraseñas de acceso de nuestros clientes.

Detección de intrusos

Todos los productos de Kriter Software monitorizan el acceso al sistema, pero es responsabilidad de nuestros clientes en determinar que es y qué no es un acceso indebido. Para nuestros productos en la nube y que den servicio a través de Internet, se monitoriza el software a nivel de host, no de cliente, En dichos productos sí se recogen (No monitorizan) datos de cliente con el objetivo de establecer si los dispositivos y software de acceso cumplen con los requerimientos de seguridad de nuestros productos.

Manejo de incidencias

Todos los productos de Kriter Software tiene su propio protocolo de manejo de incidencias en cuanto a privacidad y protección de datos. En el caso de que la incidencia sea propia del producto, no de su uso, el equipo de Kriter Software comunicará los afectados la incidencia e implementará la solución para subsanarla.

Autenticación de usuarios

El acceso a todos nuestros productos siempre es realzado mediante un sistema de autenticación usuario y contraseña. En el caso de acceso satisfactorio nuestros programas generan y guardan una identificación de sesión aleatoria que se utiliza para los posteriores accesos durante el tiempo de vida de la sesión. Dependiendo de cada producto, el final del tiempo de vida de una sesión viene dado por: el cierre del programa, el cierre del navegador, el “logout” del sistema o después de un tiempo e inactividad por parte del cliente.

Seguridad física

La seguridad física de los sistemas donde se alojan nuestros productos depende del modelo de contratación del cliente. En el caso de contratar nuestro servicio CLOUD es Kriter Software que mantiene la integridad de todos los sistemas en relación nuestros productos. Si el cliente tiene contratado nuestros servicios de hosting (alojados en Amazon AWS o Nexica) la seguridad física viene dada por estos 2 proveedores:

- Amazon AWS (visitar: All AWS Services GDPR ready | AWS Security Blog) https://aws.amazon.com/es/blogs/security/all-aws-services-gdpr-ready/

- Nexica (visitar: Condiciones generales de servicio) https://www.nexica.com/es/condiciones-generales-de-contratacion-ok)

Por último, en el caso de que nuestros clientes tengan contratados nuestros servicios de sistemas e mantenimiento de infraestructura, será Kriter que mantendrá la infraestructura a nivel de seguridad y privacidad en relación con los productos de KRITER.

En cualquier de las modalidades de contratación Kriter no cubrirá problemas derivados del mal uso de los mismos, o falta de protocolos y medidas de seguridad por parte del cliente que deriven en no cumplimiento de la GDPR.

Backup

Todos nuestros productos y software de terceros relacionados con los mismos, disponen de sistemas de Backup y recuperación de datos que deben ser configurados debidamente por los departamentos de IT del cliente.

Recuperación ante desastres

Los productos de Kriter Software están preparados para aplicar el protocolo pertinente de recuperación de datos.

No se cubren los desastres derivados de plataformas de terceros como serían las caídas del servicio AMAZON AWS o Nexica.

Virus y ataques externos

Se requiere que todos nuestros clientes tengan una política de protección de virus, malware y ataques externos que protejan el software instalado en su infraestructura. En caso de que sea Kriter la encargada de su mantenimiento se notificará al cliente de las posibles vulnerabilidades y se realizarán las tareas necesarias para subsanarlas. Nunca será responsabilidad de Kriter los desastres provocados por mal uso del software o negligencias realizadas por el cliente.

Encriptación de datos

Todos nuestros productos en la nube pueden operar bajo HTTPS. Es el cliente que contratará a Kriter o a un tercero para la implantación del HTTPS. En el caso específico de utilizar nuestro producto Kriter ERP en modalidad Cloud las comunicaciones entre la organización y el cliente se realizará mediante una red virtual privada (VPN) con los protocolos de comunicación completamente cifrados.

Devolución y borrado de los datos de Usuario

En los 30 días después de finalizar el contrato, todos nuestros clientes pueden requerir la devolución de los datos enviados a Kriter.

Mensajes transaccionales

Kriter Software puede contactar al usuario para el envío de información sobre transacciones realizadas entre ambos o, también a nivel comercial acerca de sus productos y servicios. Kriter ofrece a sus clientes un correo electrónico (gdpr@kriter.net) para ejercer sus derechos y definir qué tipo de relación a nivel de Comunicación quieren mantener con Kriter.