Evaluación de riesgos

DocClar · Versión 1.1 · 11 de octubre de 2026
Responsable: Dmytro Shelest · seguridad@docclar.com

Una evaluación breve de los riesgos para los datos personales de los documentos que tratamos por cuenta de nuestros clientes. Cada medida es una que el programa aplica hoy. El riesgo residual es nuestra valoración cualitativa (bajo, medio, alto) después de aplicar la medida.

Riesgo	Medida aplicada	Riesgo residual
Acceso a los documentos desde internet durante el procesamiento	Procesamiento en un entorno del sistema operativo que deniega toda operación de red; comprobado cada día.	Bajo
Robo o pérdida del equipo de trabajo	Disco cifrado; archivos de cada encargo cifrados con su propia clave, guardada en el llavero del sistema operativo y nunca en un archivo.	Bajo
Un revisor copia o divulga datos personales	Solo fragmentos, con DNI/NIE, correos, teléfonos, IBAN y direcciones tapados; marca de agua con su identificador; sin descarga del documento; cada vista registrada; compromiso escrito de confidencialidad; con dos o más revisores, los fragmentos se reparten.	Medio: el ocultado automático no reconoce los nombres de personas ni datos con formatos poco habituales.
Acceso no autorizado a la aplicación de revisión	Solo accesible desde el propio equipo y una red privada cifrada; contraseña guardada como hash PBKDF2; sesiones firmadas; límite de peticiones; cabeceras de seguridad.	Bajo
Envío de documentos a un servicio externo de IA	Herramientas propias en el equipo; cualquier otro servicio externo solo con un anexo firmado aparte por el cliente.	Bajo
Conservación más larga de lo necesario	Borrado automático a los 30 días de la entrega: primero la clave (borrado criptográfico), después los archivos; las fichas se reducen a estadísticas sin texto.	Bajo
Filtración desde una copia de seguridad	Copias diarias cifradas, sin documentos de clientes, conservadas 30 días.	Bajo: las fichas de revisión (textos breves) están en las copias cifradas hasta su reducción.
Texto de los documentos en registros técnicos	Los registros no guardan el contenido de los documentos; comprobado cada día.	Bajo
Secretos o credenciales expuestos	Claves y credenciales en el llavero del sistema operativo; archivos de configuración sin secretos y con permisos restringidos; comprobado cada día.	Bajo
Vulnerabilidad conocida en un componente de software	Auditoría de dependencias con pip-audit y actualizaciones de seguridad periódicas.	Medio: entre una vulnerabilidad nueva y su corrección pasa un tiempo.

Riesgo	Medida aplicada	Riesgo residual
Datos de los encargos en los avisos internos del equipo	Los avisos de gestión pueden llevar el nombre del cliente y del archivo, no el contenido del documento; quien revisa ve un seudónimo en lugar del nombre del cliente.	Bajo: el nombre de un archivo puede contener datos personales si el cliente los pone en él.
Documentos en la carpeta compartida	La carpeta es del cliente y está en Google Workspace, cuyo acuerdo de tratamiento ampara las transferencias en el Marco de Privacidad de Datos UE-EE. UU. y en las cláusulas contractuales tipo.	Depende de cómo el cliente configure y comparta su carpeta.
Avería o pérdida del único equipo de trabajo	Copias diarias cifradas en dos proveedores distintos (Google Drive y Cloudflare R2), comprobadas cada domingo y con una prueba real de restauración; los originales siguen en la carpeta del cliente.	Medio: no hay un segundo equipo preparado y el tiempo de instalar el servicio en otro equipo no está medido.
La página completa vista en la comprobación final	Solo quien dirige el servicio, y solo en la comprobación final de cada documento.	Aceptado: es necesario para entregar un documento revisado.

Ningún sistema elimina todos los riesgos. Revisamos esta evaluación cuando cambia el servicio o después de un incidente.