Medidas de seguridad

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

Estas son las medidas técnicas y organizativas (artículo 32 del RGPD) que DocClar aplica a los documentos de sus clientes. Son las del Anexo III del contrato de encargo del tratamiento que firmamos antes del primer documento, y cada una corresponde a lo que nuestro programa hace.

1. Procesamiento sin conexión a internet

Aislamiento de red: el procesamiento de los documentos (etiquetado, OCR, modelos de IA locales, validación) se ejecuta en un proceso sin acceso a la red; un control automático comprueba cada día que un intento de conexión desde ese proceso falla. Solo si el CLIENTE firma un anexo aparte que autorice un servicio externo concreto, el documento se procesa fuera de ese entorno para enviárselo.

2. Cifrado de cada encargo

Cifrado por encargo: cada encargo tiene su propia clave aleatoria de 256 bits (AES-256-GCM), guardada en el llavero del sistema operativo y nunca en un archivo. El original, la versión corregida, los informes y la caché de trabajo se guardan solo cifrados; para cada paso se descifra una copia temporal en una carpeta privada que se borra al terminar el paso. Disco del equipo de trabajo cifrado y cifrado en tránsito (TLS) en todas las transferencias.

Formato de los archivos cifrados: AES-256-GCM con un nonce aleatorio de 12 bytes y el identificador del encargo como dato asociado, de modo que un archivo no puede hacerse pasar por otro encargo. La copia temporal descifrada se crea en una carpeta privada (permisos 0700) y se borra en cuanto termina el paso.

3. Supresión a los 30 días de la entrega

Supresión a los 30 días de la entrega: se destruye primero la clave del encargo y después sus archivos (borrado criptográfico), de modo que ninguna copia del ENCARGADO puede volver a descifrarse; las fichas de revisión se reducen a datos estadísticos sin texto.

La carpeta compartida es del cliente: lo que hay en ella no lo borramos nosotros.

4. Copias de seguridad

Copias de seguridad diarias cifradas, conservadas un máximo de 30 días; no incluyen los documentos del CLIENTE, solo los registros de trabajo (con las fichas de revisión hasta su reducción).

Las copias se cifran (Fernet: AES-128 en modo CBC con HMAC-SHA256) con una clave guardada en el llavero del sistema operativo, se guardan en una carpeta privada de Google Drive y se conservan 30 días.

5. Revisión por fragmentos

Revisión por fragmentos: cada revisor accede solo a los fragmentos que revisa (la imagen y su pie, la cabecera de una tabla con las celdas difuminadas, la página difuminada con los bloques y sus primeras

palabras), con los datos personales detectables (DNI/NIE, correo electrónico, teléfono, IBAN, direcciones postales) ocultos automáticamente y una marca de agua con su identificador, y no puede descargar el documento. Con dos o más revisores, los fragmentos de un documento se reparten entre ellos. Cada visualización queda registrada (quién, qué fragmento, cuándo), sin el contenido. El ENCARGADO ve la página completa solo en la comprobación final.

Quien revisa sin permiso para ver los datos de clientes ve un seudónimo en lugar del nombre del cliente, también en el nombre del archivo.

6. Acceso restringido

Acceso restringido: cuentas personales con verificación en dos pasos; la aplicación de revisión solo es accesible desde una red privada cifrada, con contraseña, sesiones firmadas, límite de peticiones y cabeceras de seguridad; claves y credenciales guardadas en el llavero del sistema operativo.

La aplicación de revisión solo escucha en el propio equipo (127.0.0.1) y en su dirección de la red privada cifrada: no es accesible desde internet. Las contraseñas se guardan solo como hash PBKDF2. Al retirar a una persona o cambiar su contraseña, todas sus sesiones dejan de valer a la vez.

7. Personas y registros

Revisores con compromiso escrito de confidencialidad, con registro de acciones; los registros técnicos no contienen el contenido de los documentos.

8. Herramientas propias

Procesamiento con herramientas propias, sin enviar documentos a terceros salvo un anexo firmado aparte por el CLIENTE. Ningún servicio externo de inteligencia artificial recibe los documentos.

9. Actualizaciones y autocontrol diario

Actualizaciones de seguridad periódicas, revisión de vulnerabilidades conocidas de los componentes de software y supervisión automática del funcionamiento de los sistemas, con un autocontrol diario de las medidas 1, 2, 5, 6 y 7.

Cada mañana un autocontrol automático comprueba, entre otras cosas:

- que un intento de conexión (TCP y DNS) desde el entorno de procesamiento falla;
- que no queda ningún archivo de cliente sin cifrar y que cada encargo con archivos cifrados tiene su clave;
- que el disco del equipo de trabajo está cifrado;
- que las claves y credenciales están en el llavero del sistema operativo y no en archivos de configuración;
- que un texto de prueba con DNI/NIE, correo, teléfono, IBAN y dirección sale con esos datos tapados;
- que ningún registro técnico contiene texto de los documentos;
- que la última auditoría de dependencias (pip-audit, como máximo de hace 7 días) no encontró vulnerabilidades conocidas;
- que la aplicación de revisión envía sus cabeceras de seguridad y niega el PDF completo a quien revisa.

Si un control falla, quien dirige el servicio recibe un aviso con el detalle.

10. Gestión de incidentes

Procedimiento de gestión de incidentes con notificación al CLIENTE en un máximo de 48 horas (cláusula 12). El procedimiento está en el documento «Plan de respuesta a incidentes».

Plan de continuidad

- Hoy prestamos el servicio desde un único equipo de trabajo. No tenemos un segundo equipo preparado.
- Cada noche se hace una copia cifrada de nuestros datos de trabajo en Google Drive y una segunda copia cifrada de nuestros datos propios en Cloudflare R2, en la jurisdicción de la UE; se conservan 30 días. Los documentos de los clientes no se copian: se destruyen a los 30 días por diseño.
- Cada domingo se abre automáticamente la copia más reciente de cada sitio para comprobar que se puede restaurar.
- Los originales siguen en la carpeta compartida del cliente («En proceso»): si el equipo falla, un encargo en curso puede volver a procesarse desde ellos.

Última prueba real de restauración, con protocolo: 11 de octubre de 2026. Los datos de las dos copias se descifraron, se comprobaron archivo por archivo y se cargaron en una carpeta vacía en 6,3 segundos en total.

Lo que no está medido: instalar el servicio desde cero en otro equipo (sistema, programa, modelos locales y la clave de las copias). Hasta medirlo no damos un plazo para recuperar el servicio en otro equipo.

Lo que estas medidas no cubren

- La carpeta compartida está en Google Workspace (Google Drive): Google guarda allí los archivos según su contrato.
- Quien dirige el servicio ve la página completa en la comprobación final de cada documento.
- No hay un segundo equipo de trabajo preparado, y el tiempo de instalar el servicio en otro equipo no está medido.
- El ocultado automático no reconoce los nombres de personas ni datos con formatos poco habituales.
- Las fichas de revisión (textos alternativos, pies de imagen, cabeceras de tablas) no tienen clave propia: están en el disco cifrado hasta el borrado y en las copias de seguridad cifradas, que se conservan 30 días.
- No tenemos certificaciones ENS ni ISO 27001: todavía no.