LOPDGDD / RGPD

Dónde están los datos, qué sale del centro y cómo se protege

Este documento responde, en el orden en que suelen plantearse, a las preguntas que un delegado de protección de datos, un secretario o un equipo directivo hacen antes de instalar EduCronos. Describe la arquitectura real del producto en su versión actual; donde una opción depende de la configuración del centro, se indica. **No sustituye al análisis que corresponda al responsable del tratamiento**, que es siempre el centro educativo.

1. ¿Quién es el responsable y quién el encargado?

El **centro educativo** es el responsable del tratamiento: decide instalar EduCronos, qué personal se da de alta, qué módulos se activan y durante cuánto tiempo se conservan los datos. **Mediaconect**, como proveedor del software y del soporte, interviene únicamente cuando el centro lo solicita (instalación, actualización, incidencias), de forma puntual y bajo supervisión del centro, en condición de encargado del tratamiento conforme a lo que se acuerde con cada centro. Mediaconect no recibe copias de los datos ni tiene acceso permanente al servidor.

2. ¿Dónde residen los datos?

En un **equipo Windows del propio centro** (en Canarias, un PC del dominio medusa dedicado a la aplicación). EduCronos se ejecuta como servicio en ese equipo y guarda toda la información en una base de datos local (archivo SQLite junto a la aplicación). Las **copias de seguridad** se generan en ese mismo equipo y, si el centro lo configura, se replican a los terminales de fichaje del propio centro. No hay base de datos en la nube ni servidor de Mediaconect que almacene datos del centro.

3. ¿Qué datos personales trata?

- **Del profesorado y del PAS:** nombre y apellidos, DNI/NIE, número de tarjeta RFID (si la usa), correo electrónico (para los avisos), horario oficial, fichajes (fecha, hora y terminal), incidencias y justificaciones con su motivo, estatus (activo, baja, ausencia prevista con su motivo…), departamento y etapa, y el PIN de fichaje, que se almacena solo como resumen criptográfico (HMAC-SHA256 con *pepper*), nunca en claro.
- **De los usuarios del panel** (dirección, jefatura…): nombre de usuario, contraseña con PBKDF2-HMAC-SHA256 y permisos por apartado.
- Los **módulos opcionales** que el centro decida activar (por ejemplo, el fichaje del alumnado) tratan los datos que esos módulos requieran, siempre en el mismo servidor del centro y bajo su control.

Los listados que se importan proceden de Pincel Ekade; EduCronos avisa si se cargaron con los identificadores enmascarados y no admite horarios de otro curso.

4. ¿Qué sale de la red del centro?

Por defecto, ningún dato personal. Las comunicaciones salientes existen solo si el centro las configura, y son estas:

- **Correo electrónico** (SMTP del propio centro): avisos diarios a cada docente, resumen a Jefatura, envío de listados desde el portal del docente y, si se activa, el enlace al cuadrante de guardia.
- **Nube de la Consejería** (Nextcloud, nube.canariaseducacion.org): publicación del PDF del cuadrante de guardia del día en una carpeta de la cuenta institucional del centro, con una contraseña de aplicación que el centro puede revocar. El enlace solo abre con cuenta del dominio educativo.
- **Latido de salud** a un panel de monitorización (local del centro o externo), **desactivado de serie**: envía versión, estado del servicio, memoria y tamaño de la base de datos; nunca datos de personas.
- **Comprobación manual de actualizaciones**: al pulsar «Comprobar», el servidor consulta un archivo de versión en mediaconect.com; la petición solo identifica la versión instalada.

Los terminales EduPass y los navegadores de los usuarios se comunican con el servidor **dentro de la red del centro**. Las páginas de ayuda se abren en www.educronos.com sin enviar datos del centro.

5. ¿Qué medidas técnicas aplica?

Secretos de la instalación	Cifrados con DPAPI de Windows en ámbito de máquina: solo se descifran en el servidor en que se generaron. Cada instalación genera sus propios secretos.
Contraseñas	PBKDF2-HMAC-SHA256 con sal por usuario; contraseña inicial aleatoria y cambio obligatorio en el primer acceso (mínimo 10 caracteres).
PIN de fichaje	HMAC-SHA256 con *pepper* guardado fuera de la base de datos, en un archivo cifrado por DPAPI; comparación en tiempo constante.
Copias de seguridad	ZIP cifrado con Fernet (AES-128-CBC + HMAC-SHA256), clave derivada con PBKDF2 a 600.000 iteraciones y sal única por copia; programadas a diario y restaurables desde el panel.
Control de acceso	Autenticación obligatoria en todas las rutas del panel (denegación por defecto), permisos por apartado y por usuario, sesión única por usuario con expulsión inmediata al borrar o degradar la cuenta, cookies HttpOnly y SameSite, protección CSRF.
Terminales de fichaje	Token propio por terminal (almacenado solo como SHA-256), lista de IPs o redes autorizadas, rotación de tokens, última conexión y límite de intentos.
Portal del docente	Cada docente solo accede a sus propios datos: el ámbito lo fija el servidor a partir de la sesión, no el navegador. Una sesión por docente, caducidad por inactividad a los 15 minutos.
Trazabilidad	Registro de restablecimientos administrativos y de los cambios de estatus del docente; licencia firmada con RSA-2048 ligada al equipo.

6. ¿Cómo se atienden los derechos de las personas?

Desde el propio panel del centro: consulta y exportación de los fichajes e incidencias de una persona (acceso y portabilidad), corrección de datos y de justificaciones (rectificación), y baja o eliminación del docente con sus registros (supresión), siempre según los criterios de conservación que fije el centro. El portal del docente permite, además, que cada persona consulte y descargue sus propios registros sin intervención de Jefatura.

7. ¿Cuánto tiempo se conservan los datos y qué pasa si el centro deja de usar EduCronos?

El plazo lo decide el centro: EduCronos no envía nada fuera ni borra nada por su cuenta, y las copias de seguridad se conservan en el número que el centro indique, rotando las antiguas. Si el centro deja de usarlo, todo está en su equipo: puede exportar a Excel y PDF, y la base de datos y las copias quedan bajo su custodia; desinstalar no requiere intervención de Mediaconect ni deja datos en ningún servicio externo.

Orientación para el registro de actividades de tratamiento

Texto orientativo para el DPD del centro: **debe revisarse y adaptarse** a la normativa de personal aplicable y a los criterios de la Consejería; no constituye asesoramiento jurídico.

CAMPO	PROPUESTA
Actividad	Control de presencia y gestión organizativa del personal docente y no docente (fichajes, incidencias, guardias, actividades complementarias).
Finalidades	Registrar la presencia del personal, cruzarla con el horario oficial, gestionar guardias y sustituciones, comunicar incidencias y elaborar informes organizativos.
Interesados	Personal docente y personal de administración y servicios del centro.
Categorías de datos	Identificativos (nombre, DNI/NIE, correo, nº de tarjeta), laborales (horario, fichajes, incidencias, justificaciones, estatus). Sin categorías especiales.
Destinatarios y transferencias	No se ceden datos ni hay transferencias internacionales. Encargado puntual: Mediaconect (soporte). Comunicaciones por el correo propio del centro y, si se activa, publicación del cuadrante en la nube de la Consejería.
Medidas de seguridad	Las descritas en el apartado 5: residencia local, cifrado de secretos y copias, hashing de credenciales, control de acceso por usuario y terminal, trazabilidad.
Plazo de conservación	El que determine el centro (por ejemplo, el curso en vigor más el periodo necesario para la gestión de incidencias y responsabilidades).