

1 · Quién presta el servicio

Titular	APRENDIZAJES DEL FUTURO, S.L. · NIF B23853310 · Passatge Domènech, 3, 08470 Sant Celoni (Barcelona).
Papel en el RGPD	Encargado del tratamiento (art. 28). La empresa cliente es la responsable de los datos de su plantilla. El contrato de encargo está publicado en ficheo.app/encargo-de-tratamiento y se acepta al contratar.
Contacto	hola@ficheo.app . Brechas de seguridad: se comunican al cliente en un máximo de 24 horas desde que se conocen.
Soporte	Tickets desde el panel o por correo, de lunes a viernes de 9 a 18 h (Madrid), sin festivos nacionales. Primera respuesta de una persona en 1 h laborable si no se puede fichar; lo demás, de 4 h a 3 días laborables según prioridad y plan. Cumplimiento publicado en ficheo.app/soporte-y-atencion . Sin teléfono ni guardia nocturna.
Uso de los datos	Solo para prestar el servicio. Ni publicidad, ni cesión, ni entrenamiento de sistemas automáticos.

2 · Dónde están los datos y quién más los toca

Alojamiento	Servidor de Hostinger International Ltd. en un centro de datos de París (Francia, UE). Sistema Ubuntu 24.04 LTS con las actualizaciones de seguridad automáticas encendidas y cortafuegos activo.
Base de datos	PostgreSQL en ese mismo servidor. No acepta conexiones desde Internet: solo desde la propia máquina.
Subencargados	Hostinger (alojamiento y entrega del correo del servicio, UE). Hetzner Online GmbH (servidor de respaldo, réplica de la base y de los archivos; UE, Núremberg). Backblaze (copias de seguridad cifradas antes de salir, con una clave que no tiene; UE, Ámsterdam). Stripe Payments Europe (cobro; solo datos de facturación del cliente, nunca de la plantilla, UE). Solo si el cliente los activa: Telegram (fichar por mensaje; fuera de la UE) y Google Ireland / Microsoft Ireland (entrar con la cuenta corporativa; UE). Un cambio de subencargado se avisa con 30 días.
Transferencias fuera de la UE	Ninguna, salvo Telegram si el cliente activa esa forma de fichar; se desactiva desde su panel.

3 · Acceso y protección

Cifrado en tránsito	Todo por HTTPS, solo con TLS 1.2 y 1.3, con certificados que se renuevan solos: la web, el panel, la app y la API.
Cifrado en reposo: archivos	Los archivos subidos (nóminas, contratos, partes de baja, tickets de gastos, adjuntos y correos de soporte) se guardan cifrados uno a uno con AES-256-GCM, y se descifran solo al entregarlos a quien tiene permiso. La clave vive en la configuración del servidor, fuera de la carpeta de los archivos, y se puede rotar. También va cifrado el DNI que se guarda para repartir nóminas.
Cifrado en reposo: disco	El disco de los servidores no está cifrado entero. La base de datos (fichajes, ausencias, nombres, correos, teléfonos) está en claro dentro del servidor, protegida por el acceso a él; todas sus copias salen cifradas. Cifrar los archivos protege si se filtra su carpeta o una copia; contra quien tuviera acceso de administrador al servidor encendido no protege ningún cifrado en reposo.
Acceso al servidor	Solo con clave criptográfica, nunca con contraseña; quien falla varias veces queda bloqueado. Base de datos sin puerto abierto a internet y cortafuegos activo.
Contraseñas	Guardadas como huella scrypt con sal propia por contraseña. Nadie puede leerlas, tampoco Ficheo; solo se sustituyen.
Freno de intentos	Tras 8 fallos hay que esperar 30 s, y la espera sube hasta 30 min. Cuenta por usuario y por dirección de origen a la vez. El mensaje de error no revela si la cuenta existe.

Verificación en dos pasos	Para quien gestiona el panel (administradores y encargados): además de la contraseña, un código de 6 cifras de una aplicación de autenticación (TOTP), con diez códigos de recuperación de un solo uso. La empresa puede hacerla obligatoria; se pide entre por donde se entre, también con Google o Microsoft, y cada entrada con código queda en el registro de accesos.
Inicio de sesión único	En el plan Pro: entrar con la cuenta de empresa por SAML 2.0 (Microsoft Entra ID, Okta, Google Workspace...), con firma, audiencia, caducidad y repetición comprobadas en cada entrada; opción «solo con la cuenta de empresa»; y altas y bajas automáticas por SCIM 2.0. Una baja nunca borra el registro de jornada.
Papeles	Trabajador, encargado, gestor y soporte. Un encargado solo puede lo que está en una lista cerrada: todo lo demás le está prohibido.
Aislamiento entre empresas	Cada empresa ve solo lo suyo. Antes de cada actualización del servidor, unas pruebas automáticas recorren las rutas del panel y de la app con datos de otra empresa; si alguna deja ver o cambiar algo ajeno, la actualización no sale.
Registro de accesos	Queda apuntado quién abrió la ficha o los datos de qué persona, y esa persona lo ve desde su app. No hay forma de borrarlo ni editarlo. Se conserva 730 días (el cliente lo fija entre 180 y 1.460).
Acceso de soporte	Si soporte de Ficheo entra en la cuenta de un cliente para ayudarle, queda registrado con fecha, hora y quién, y el cliente lo consulta. Soporte no puede descargar la exportación completa de la empresa.
Cambios en los fichajes	Cada alta, corrección o borrado guarda quién, cuándo, el antes, el después y el motivo. Ese historial no se puede borrar, y un mes cerrado ya no se puede tocar.

4 • Copias y continuidad

Copia	Completa cada noche: la base de datos y los archivos subidos (documentos, justificantes).
Comprobación	Cada copia se restaura en una base aparte y se cuentan sus filas contra las del momento de la copia: fichajes, personas, ausencias, documentos e historial. Si no cuadran, queda marcada como fallida.
Conservación de copias	Las de las 14 últimas noches y una por mes durante un año.
Copia fuera	Cada copia comprobada sale cifrada (AES-256) a un segundo proveedor en la UE, fuera del centro de datos de París. Con ella, volver a estar en pie en un servidor nuevo está probado y lleva 25-35 minutos.
Servidor de respaldo	Un segundo servidor en otro centro de datos y con otro proveedor (Hetzner, Núremberg, Alemania) recibe cada cambio de la base al momento. Si cae la máquina principal, se pasa a él con una sola orden en unos 5 a 10 minutos, sin perder lo registrado.
Vigilancia	Cada minuto. Si el programa deja de contestar, se reinicia solo en uno o dos minutos. Si cae la máquina entera, se pasa al servidor de respaldo.
Sin conexión	La app del móvil y la tablet de la entrada guardan los fichajes que no pueden enviar, con la hora del toque, y los mandan al volver; la hora se respeta durante 30 días. Quien no pudo fichar lo registra después, con rastro. Cada persona ve sus vacaciones aprobadas sin conexión, y el calendario del equipo se imprime desde el panel.
Disponibilidad	Medida cada minuto y publicada en ficheo.app/estado , con cada incidencia, su hora y lo que duró. Disponibilidad medida: 99,95 %; la incidencia más larga, 47 minutos el 17-oct-2026, por un apagado de la máquina por parte del proveedor: el caso que hoy cubre el servidor de respaldo. Compromiso del 99,9 % mensual; en los planes de pago, crédito del 10 % de la cuota del mes por debajo del 99,5 % y del 25 % por debajo del 99 % (condiciones, apartado 8).
Vigilancia desde fuera	Un servicio externo (UptimeRobot) comprueba Ficheo cada cinco minutos desde otra red y lo publica en stats.uptimerobot.com/SyZSaGqWEe , que sigue en pie aunque nuestro servidor no lo esté.

5 • Conservación, salida y derechos

Registro de jornada	Cuatro años como mínimo (art. 34.9 del Estatuto de los Trabajadores). Ninguna limpieza automática lo borra.
Llevarse todo	Quien administra descarga la empresa entera en un ZIP, sin pedirlo a nadie: un CSV por tabla y un JSON con todo (personas, fichajes, correcciones con su antes y después, ausencias, saldos, horarios) y los documentos subidos.

Derechos de cada persona	Cada trabajador descarga todo lo suyo desde su app, en HTML y JSON (arts. 15 y 20 del RGPD), y consulta quién ha mirado sus datos.
Al irse	Darse de baja de un plan de pago no borra nada: la cuenta pasa al plan Gratis. El borrado completo se pide por escrito y se hace en un máximo de 30 días, archivos incluidos; las copias desaparecen con su propio ciclo.
Biometría	No hay fichaje con huella dactilar, a propósito: la AEPD no la ve proporcionada habiendo PIN o tarjeta.

6 • Lo que hoy no hay

- × Certificaciones como ISO 27001 o el Esquema Nacional de Seguridad.
- × Cifrado del disco entero de los servidores. Sí van cifrados los archivos subidos, el DNI y todas las copias que salen del servidor.

Para comprobarlo sin creernos: el estado y cada incidencia en ficheo.app/estado; el detalle de la continuidad en ficheo.app/disponibilidad-y-continuidad; el contrato del art. 28 en ficheo.app/encargo-de-tratamiento.