Requisitos legales y técnicos del registro horario digital

Llinars Computer – División Empresarial

Fecha: 14/12/2025

1. Introducción y objetivo del documento

La implantación del registro horario digital obligatorio a partir de 2026 no es solo un cambio operativo, sino también un reto legal y tecnológico para las empresas.

Este documento tiene como objetivo aclarar los requisitos legales, explicar su aplicación técnica y ayudar a evitar errores que pueden derivar en sanciones o conflictos laborales.

2. Marco legal del registro horario en España

La obligación de registrar la jornada laboral se fundamenta principalmente en el Real Decreto-ley 8/2019, que modificó el Estatuto de los Trabajadores estableciendo la obligación de llevar un registro diario de la jornada.

La normativa prevista para 2026 refuerza los mecanismos de control, elimina los sistemas manuales e introduce requisitos tecnológicos para garantizar registros objetivos, verificables y no manipulables.

3. Obligaciones empresariales según la normativa laboral

- Registrar diariamente la jornada de cada trabajador.
- Garantizar que el registro sea objetivo, fiable y accesible.
- Poner los registros a disposición de trabajadores, representantes e Inspección de Trabajo.
- Conservar los registros durante un mínimo de 4 años.
- Asegurar trazabilidad e integridad en el registro digital.

La empresa es la responsable última del cumplimiento, independientemente del proveedor tecnológico utilizado.

4. Integridad, trazabilidad e inalterabilidad de los registros

Los registros no pueden modificarse libremente. Cualquier corrección debe quedar registrada y debe ser posible reconstruir el historial completo de cada jornada.

- Trazabilidad: qué ha ocurrido con cada registro.
- Auditoría: quién hizo qué y cuándo.
- Inalterabilidad lógica: no se pueden borrar o alterar datos sin dejar rastro.

5. Identificación del trabajador y sistemas de fichaje

El sistema debe vincular cada marcaje a la identidad del trabajador, evitando suplantaciones.

- Credenciales únicas, PIN, tarjeta o aplicación con autenticación.
- Biometría: requiere especial atención RGPD y justificar la necesidad.
- Principios: unicidad, seguridad y proporcionalidad.

6. Correcciones, modificaciones y auditorías

Las correcciones por incidencias son posibles, pero el sistema debe garantizar que los registros originales no se eliminan y que cualquier cambio deja rastro.

- Logs de auditoría (quién, qué, cuándo).
- Control de roles y permisos.
- Histórico completo de cambios y motivo de la corrección.

Los sistemas que permiten modificar o borrar datos sin trazabilidad no cumplen los requisitos legales.

7. Acceso de la Inspección de Trabajo

La Inspección podrá acceder a los registros de forma remota e inmediata, sin necesidad de desplazamiento ni aviso previo.

- Acceso seguro y controlado a la información.
- Consultas por periodo, trabajador o centro de trabajo.
- Visualización y exportación en formato comprensible y estructurado.

La empresa es responsable de garantizar este acceso, aunque el sistema esté externalizado o en la nube.

8. Conservación de datos y custodia del registro

Los registros deben conservarse durante un mínimo de 4 años. La custodia efectiva implica garantizar integridad, disponibilidad y continuidad, también en caso de cambios de sistema.

- Almacenamiento seguro con copias de seguridad automatizadas.
- Redundancia para evitar pérdida de datos.
- Mecanismos de exportación en caso de cambio de proveedor.
- Conservación de históricos aunque se cambie de sistema.

9. Protección de datos y RGPD aplicado al registro horario

El registro horario digital trata datos personales y debe cumplir RGPD y LOPDGDD.

- Principios: licitud, finalidad, minimización, integridad y confidencialidad.
- Medidas: cifrado, control de accesos, registro de accesos y operaciones, eliminación segura.
- Biometría/geolocalización: puede requerir Evaluación de Impacto (EIPD) y medidas reforzadas.

Un sistema que cumpla la normativa laboral pero incumpla protección de datos puede generar sanciones adicionales.

10. Errores habituales en las empresas

- Continuar con papel/Excel o sistemas no adaptados.
- Permitir modificaciones sin rastro.
- Registro incompleto (pausas, horas extra, guardias).
- Identificación débil o compartida.
- Mala conservación y copias de seguridad insuficientes.
- Incumplimientos RGPD en soluciones sensibles (biometría/geolocalización).

11. Buenas prácticas legales y tecnológicas

- Implantar un sistema fiable con auditoría y trazabilidad.
- Definir protocolos internos y formar a la plantilla.
- Controlar permisos y realizar revisiones periódicas.
- Integrar el control horario con la gestión laboral.
- Aplicar privacy by design y minimización de datos.
- Anticiparse a la entrada en vigor y planificar la adaptación.

12. Recomendaciones profesionales de Llinars Computer

En Llinars Computer, S.L. – División Empresarial recomendamos un enfoque mixto de consultoría y tecnología.

- Análisis inicial de la situación de la empresa.
- Selección e implantación de soluciones seguras y escalables.
- Acompañamiento, formación y soporte continuo.
- Revisión de cumplimiento legal y de protección de datos.

Contacta con nosotros para preparar tu empresa con garantías.