Actualización del uso de la Biometría para el Registro de Jornada y Control de Accesos

25/06/2024

hrlog

Agenda

- 0. Introducción y conceptos previos
- 1. Proceso de uso de la Biometría en Control de Presencia
- 2. Principios de RPGD
- 3. Usos Autorizados de la Biometría
- 4. Objecciones de AEPD para su uso en el Control de Presencia
- 5. Evaluación de Impacto para la Protección de Datos
- 6. Conclusiones
- 7. Alternativas disponibles con HRLOG

0 Introducción: La Guía

0 Introducción: La Guía

GUÍA SOBRE TRATAMIENTOS DE CONTROL DE PRESENCIA MEDIANTE SISTEMAS BIOMÉTRICOS

La razón de la emisión de la guía es proporcionar orientación específica sobre el uso y tratamiento de **sistemas biométricos** en el **control de presencia y acceso** en **entornos laborales** y otros contextos.

La guía tiene como objetivo asegurar que estos sistemas **se utilicen de manera conforme a la normativa de protección de datos, garantizando los derechos y libertades de las personas**.

Además, busca proporcionar **pautas claras** para cumplir con las obligaciones legales en cuanto a la minimización de datos, protección desde el diseño, gestión de riesgos y **evaluación de impacto en la protección de datos (EIPD).**

0 Conceptos Previos

BIOMETRÍA

La biometría se refiere a los **sistemas de procesamiento de datos** que recogen y procesan **datos personales relativos a las características físicas, fisiológicas o conductuales** de las personas físicas.

Estos sistemas utilizan **dispositivos o sensores** para crear **plantillas biométricas**, también conocidas como **firmas o patrones**, que permiten la identificación, seguimiento o perfilado de las personas

DATOS BIOMÉTRICOS

Los datos biométricos son definidos por el Reglamento General de Protección de Datos (RGPD) en su artículo 4.14 como "**datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos**"

PATRÓN BIOMÉTRICO

- Es una forma de escritura de una característica biométrica humana (rostro o una huella dactilar).
- Sea interpretable por una máquina de forma eficiente y eficaz para un propósito determinado.
- No está diseñado para ser interpretado por una persona, sino que está orientado a ser tratado en un proceso automatizado.
- Permite singularizar a un individuo y ejecutar acciones de forma automática.

0 Conceptos Previos

La guía señala que **a partir de una plantilla biométrica**, por ejemplo, de huella dactilar, **no se puede reconstruir la huella original**.

Este hecho se considera **irrelevante** en el contexto de su uso, ya que la plantilla biométrica actúa como un **identificador único que singulariza unívocamente a una persona dentro de un proceso automatizado**.

Es decir, aunque no se pueda obtener la imagen original del rostro a partir de la plantilla, esta sigue siendo un identificador eficaz para los fines de identificación y autenticación.

Por lo tanto:

Una plantilla biométrica con propósito de identificación o autenticación es un dato personal per se y un identificador único

hrlog

1

Uso de la Biometría

hrlog

1 Uso de la Biometría

Registro de Jornada

Su finalidad es controlar el desarrollo de la jornada laboral, conforme al **Real Decreto-Ley 8/2019** que establece la obligatoriedad del registro diario de jornada, incluyendo el horario concreto de inicio y finalización de la jornada de cada trabajador

Control de Acceso

Este tipo de tratamiento **supervisa la entrada y/o salida** a determinados recintos y puede tener finalidades laborales o no laborales.

🚨 En ambos casos estos tratamientos **deben cumplir con los principios, derechos y obligaciones establecidos en el RGPD**.

🚨 La implementación mediante sistemas biométricos añade **consideraciones adicionales** para asegurar el cumplimiento del RGPD

1 Proceso de uso de la Biometría

Recolecta y Procesamiento

- **Sensores** y dispositivos
- Características **físicas**, fisiológicas o conductuales
- **Creación de patrón** biométrico

Tratamiento Automatizado

- **No** destinado a **humanos**
- **Comparación** datos biométricos en **tiempo real** con patrón

Autenticación

- **Confirmar** que una persona es quien dice ser
- Comparación **uno contra uno**
- **Verificar** la identidad de una persona cuando ésta es provista

Identificación

- Determinar persona **dentro de un grupo**
- Comparación **uno contra muchos**
- Reconocer una persona **sin que declare su identidad** previamente

2

Principios RGPD

hrlog

2

Principios RGPD

1

Principio de Minimización de Datos

Definición: Los datos personales deben ser **adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados** (Art. 5.1.c RGPD).

Justificación: Los datos que no son necesarios para cumplir con la finalidad del tratamiento no deben ser tratados. Este principio aplica especialmente a tratamientos que **impliquen un riesgo para los derechos y libertades de las personas físicas.**

2

Protección de Datos desde el Diseño

Definición: Incorporar **medidas técnicas y organizativas apropiadas desde el inicio del diseño del tratamiento de datos** para asegurar el cumplimiento de los principios de protección de datos (Art. 25 RGPD).

Objetivo: **Garantizar y poder demostrar** que el tratamiento es conforme con el RGPD, minimizando el riesgo y **asegurando la protección** de los datos personales durante todo el ciclo de vida del tratamiento.

2 Principios RGPD

Minimización en el Tratamiento del Control de Presencia y Accesos 🚶

- **Datos Necesarios:** Solo deben tratarse los datos estrictamente necesarios para el objetivo del control de presencia (registro de jornada y control de acceso).
- **Evaluación de Alternativas:** Considerar alternativas menos intrusivas y justificar cualquier tratamiento adicional de datos.
- **No Exclusividad Tecnológica:** Evaluar opciones tecnológicas, humanas, jurídicas y organizativas para implementar el tratamiento de manera menos intrusiva.

Minimización en las Técnicas de Recogida de Información Biométrica ℹ️

- **Adecuación de Tecnologías:** Seleccionar tecnologías que no recojan más datos de los necesarios. La tecnología utilizada debe ser adecuada, pertinente y limitada a la finalidad del tratamiento.
- **Configuración del Sistema:** Ajustar y configurar los sistemas biométricos para que no se recojan datos innecesarios y cumplir con el principio de minimización de datos desde el diseño (Art. 25.1 RGPD).
- **Evaluación Objetiva:** Realizar evaluaciones objetivas para asegurar que no se recogen datos excesivos y proteger los derechos y libertades de los interesados.

2 Principios RGPD

Categorías Especiales de Datos 💥

Definición y Marco Legal:

Artículo 9.1 y 51 del RGPD: Establece una prohi**bición general sobre el tratamiento de categorías especiales de datos personales, incluyendo datos biométricos** destinados a identificar de manera unívoca a una persona física.

🚨 Prohibido su tratamiento excepto en determinadas ocasiones 🚨

Datos Biométricos como Categoría Especial: 👣

Identificación y Autenticación: Los **datos biométricos** utilizados para identificar o autenticar a una persona son considerados **categorías especiales de datos personales**. Esto incluye tecnologías de reconocimiento facial, huellas dactilares, análisis de voz, entre otros .

Ejemplos de Datos Sensibles: Información sobre la salud, origen racial o étnico, datos genéticos, creencias religiosas, opiniones políticas, vida sexual, entre otros .

2 Principios RGPD

Tratamiento de Fotografías 📸

- **No Sistemáticamente Biométrico:** El tratamiento de **fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales** de datos personales.

- **Condición para ser Biométrico:** Las fotografías solo se consideran datos biométricos cuando el tratamiento con medios técnicos específicos permite la **identificación o autenticación** unívocas de una persona física.

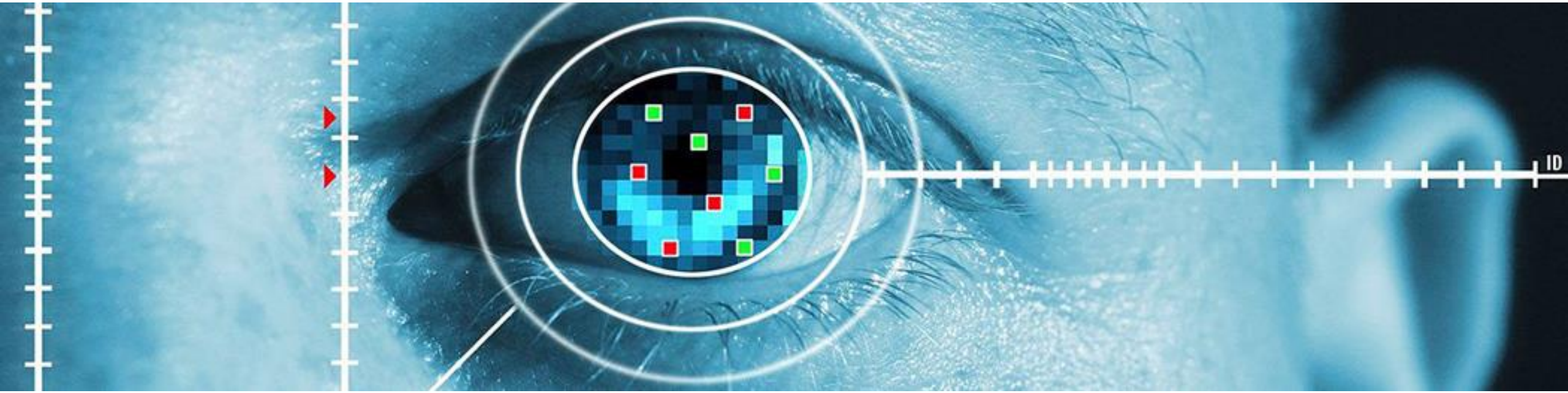
Ejemplos y Aplicaciones 🔐

- **Reconocimiento Facial:** Si una fotografía se utiliza en un sistema de **reconocimiento facial para identificar** de manera única a una persona, se clasifica como un dato biométrico.

- **Sistemas de Seguridad:** Fotografías usadas en sistemas de seguridad que emplean **técnicas biométricas** para **autenticación** también se consideran datos biométricos.

hrlog

3 Uso autorizado de Biometría



Levantamiento de la prohibición de tratar categorías especiales de datos:

- **Legalidad :** el tratamiento debe estar amparado por una norma de rango legal
- **Necesidad:** el tratamiento debe de ser “necesario”
- **Idoneidad:** el tratamiento deberá respetar el principio de proporcionalidad

hrlog

3 Uso autorizado de Biometría

Necesidad de una Norma de Rango Legal 👩‍⚖️

1. **Fundamento Jurídico:** El artículo 9.2.b del RGPD establece que la prohibición del tratamiento de categorías especiales de datos, como los biométricos, se puede levantar **si el tratamiento es necesario para el cumplimiento de obligaciones y derechos específicos en el ámbito laboral y de la seguridad social**.

2. **Requisito de Legalidad:** En España, esta excepción requiere una **norma de rango legal** que ampare dicho tratamiento, conforme a lo dispuesto en el artículo 53.1 de la Constitución Española.

3. **Seguridad Jurídica:** La normativa debe ser clara y específica, garantizando la certeza y previsibilidad necesarias para la protección de los derechos fundamentales, según la Sentencia del Tribunal Constitucional 76/2019.

Registro de Jornada ❌

Real Decreto-Ley 8/2019 que establece la obligatoriedad del registro diario de jornada, incluyendo el horario concreto de inicio y finalización de la jornada de cada trabajador

Control de Acceso ❌

No existe norma que obligue a la **supervisión de la entrada y/o salida** a determinados recintos y puede tener finalidades laborales o no laborales.

3 Uso autorizado de Biometría

Justificación de la Necesidad 🔍

1. **Condición de Necesidad:** El artículo 9.2.b del RGPD no solo exige una habilitación legal sino también que el tratamiento sea **estrictamente necesario**.

2. **Historial de Sistemas de Control:** Se han utilizado sistemas no biométricos para el control de jornada y de accesos durante décadas, demostrando que no siempre es necesario recurrir a datos biométricos.

3. **Alternativas Menos Intrusivas:** Es necesario **justificar** por qué no se pueden utilizar otros sistemas de registro de presencia menos intrusivos, como tarjetas, códigos o métodos de verificación manual.

3 Uso autorizado de Biometría

Evaluación de la Idoneidad ✅

1. **Finalidad y Calidad:** El tratamiento debe permitir alcanzar la finalidad del control de presencia con niveles adecuados de **calidad y precisión**, evitando errores y fraudes.

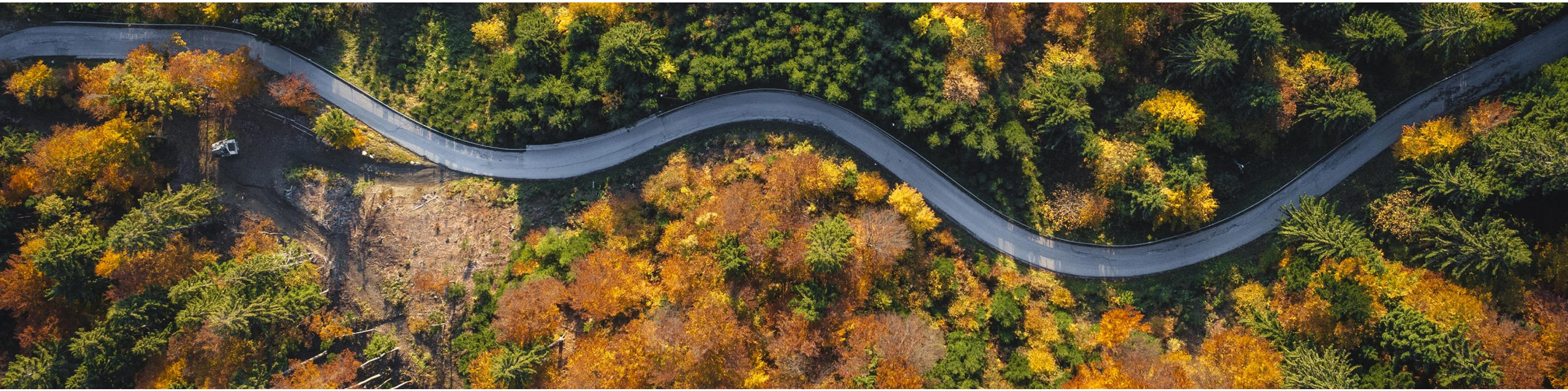
2. **Métricas y Rendimiento:** Se deben definir métricas claras sobre el rendimiento de los sistemas biométricos y **compararlas con otras opciones técnicas disponibles**.

3. **Análisis de Riesgos:** Evaluar posibles sesgos, identificaciones incorrectas, discriminación y otros riesgos asociados con el uso de biometría. La técnica debe ser esencial para cumplir la finalidad **sin existir alternativas equivalentes menos intrusivas.**

hrlog

4

Objecciones AEPD



4 Objecciones AEPD

Condiciones del Consentimiento de usos biométricos en Registro de Jornada y Control de Accesos

Definición (Art. 4.11 RGPD): Manifestación de voluntad libre, específica, informada e inequívoca para aceptar el tratamiento de datos personales.
Requisitos: Información clara sobre los riesgos del tratamiento, especialmente para personas vulnerables.

Contexto Laboral

Desequilibrio de Poder: Existe un desequilibrio entre empleado y empleador que dificulta la libre concesión del consentimiento. Por ello, el consentimiento no es válido en este contexto (Directrices 5/2020 del CEPD).

Control de Presencia y Registro de Jornada

- **No Aplicable:** El consentimiento no es válido para el tratamiento de datos biométricos en el registro de jornada debido a la obligación laboral del empleado.
- **Alternativas:** Podría considerarse válido solo si existen alternativas equivalentes y menos intrusivas para cumplir con la obligación sin el uso de datos biométricos.
- **Evaluación de Necesidad:** La disponibilidad de **alternativas** hace que el uso de datos biométricos no sea necesario, incumpliendo así el principio de minimización de datos del RGPD.
- **Implicaciones:** Si se pueden emplear **métodos alternativos de registro de jornada, el consentimiento para el uso de biometría pierde validez, ya que no se justifica su necesidad**.

4 Objecciones AEPD

Decisiones **Automatizadas** Restricciones y Garantías (Art. 22 RGPD)

Proceso automatizado sin intervención humana que produzca efectos jurídicos sobre el interesado o le afecte significativamente. Ejemplos:

1. Denegación automática de acceso a un lugar que afecta al salario o empleo.
2. Impedimento automático de acceso a una actividad o servicio contratado, limitando la libertad de movimientos.

Medidas de Protección

Derechos del Interesado:

- obtener intervención humana.
- expresar su punto de vista.
- impugnar la decisión.

Evaluación de Impacto: Obligatoria antes de la implementación para asegurar conformidad con el RGPD y minimizar riesgos.

hrlog

5

Evaluación EIPD

5 Evaluación EIPD

Procedimiento para Solicitar la Evaluación de Impacto para la Protección de Datos (EIPD) 🔐

Pasos para Solicitar una EIPD:

- Identificación del Tratamiento:
- Determinar si el tratamiento de datos personales implica un **alto riesgo para los derechos y libertades** de las personas.

Realización de la EIPD:

- Elaborar un **informe detallado** que incluya análisis de **idoneidad, necesidad y proporcionalidad** del tratamiento.
- Incluir la participación del Delegado de Protección de Datos si existe.

Consulta Previa:

- **Enviar la EIPD a la Agencia Española de Protección de Datos** (AEPD) si no se pueden mitigar todos los riesgos identificados.
- Esperar la **revisión** y las recomendaciones de la AEPD antes de proceder con el tratamiento .

5 Evaluación EIPD

Condiciones de Aceptación ✅

Triple Juicio de **Idoneidad, Necesidad y Proporcionalidad**:

1. **Idoneidad:** Demostrar que el tratamiento es adecuado para alcanzar los objetivos.
2. **Necesidad:** Probar que no existen alternativas menos intrusivas para lograr los mismos fines.
3. **Proporcionalidad:** Asegurar que los beneficios del tratamiento superan los riesgos para los derechos y libertades de los interesados.

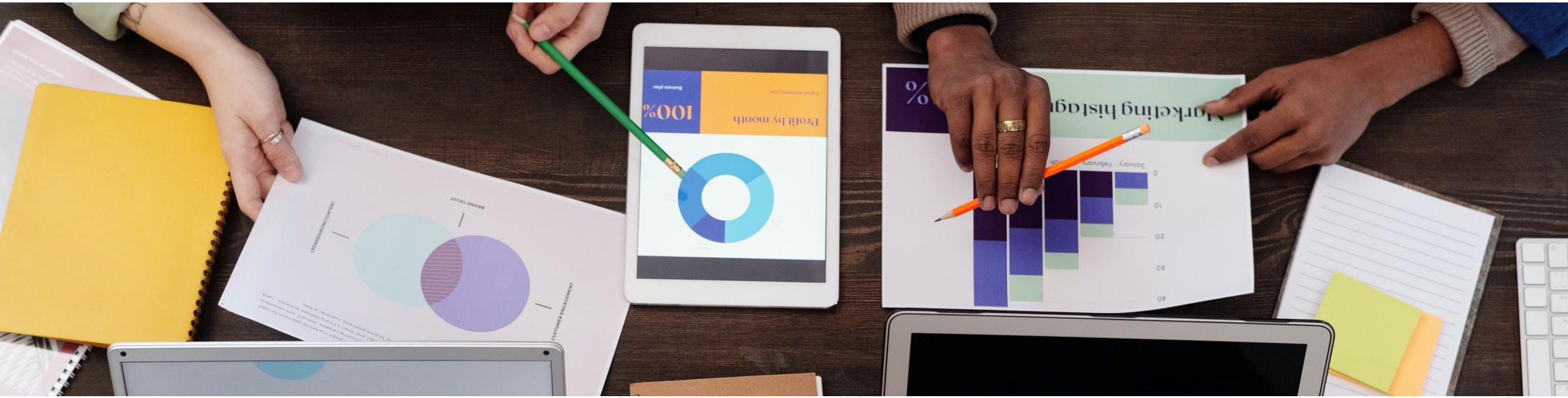
Gestión de Riesgos:

- Implementar medidas técnicas y organizativas para mitigar los riesgos identificados.
- Demostrar una **evaluación objetiva de los riesgos y las medidas adoptadas para minimizarlos**.

Documentación y Evidencia:

- Proporcionar toda la documentación justificativa del análisis y las medidas adoptadas.
- Incluir evidencia de la participación del DPD y cualquier consulta previa realizada .

6 Conclusiones



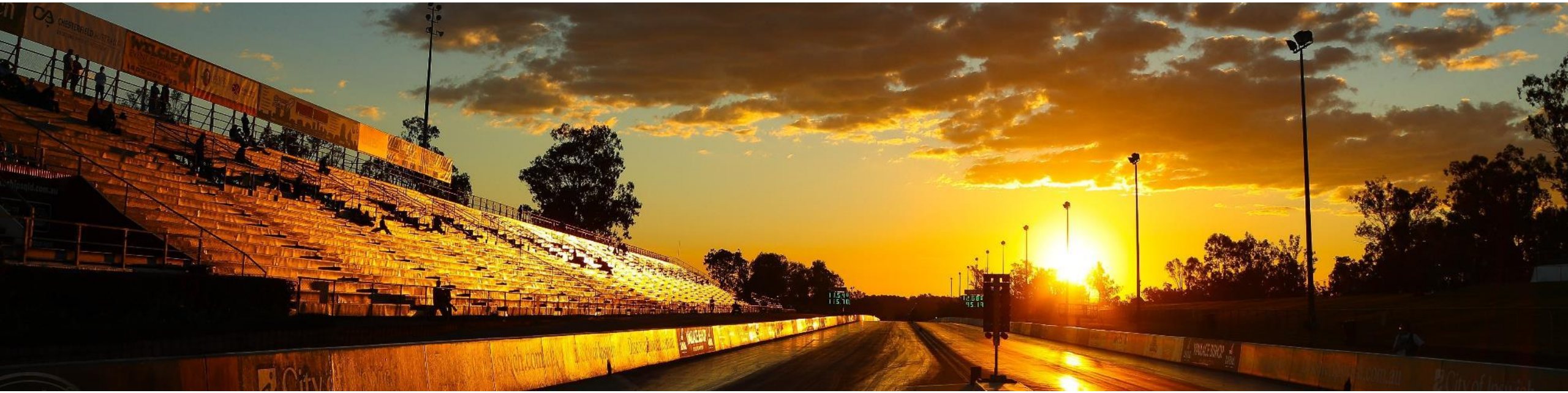
6 Conclusiones

Conclusiones Principales 📒

- **Tratamiento de Alto Riesgo:** El uso de tecnologías biométricas en el control de presencia implica un alto riesgo y el tratamiento de categorías especiales de datos.
- **Cumplimiento de Principios:** Es crucial cumplir con los principios de **minimización** y protección de datos desde el **diseño** y por defecto, usando **medidas alternativas menos intrusivas**.
- **Levantamiento de la Prohibición:** Necesario tener una norma con rango de ley que permita el uso de datos biométricos, la cual no existe en la normativa española actual.
- **No Válido en Contexto Laboral:** El **consentimiento** no puede usarse como base legal debido al desequilibrio de poder entre empleado y empleador.
- **Evaluación de Impacto:** Obligatoria la superación favorable de una EIPD **antes del inicio del tratamiento**, documentando la idoneidad, necesidad y proporcionalidad del tratamiento.
- **Medidas Específicas:** Implementar garantías organizativas, técnicas y jurídicas adecuadas para proteger los derechos de los interesados.

hrlog

7 Alternativas



7 Alternativas

APP: accesos propios e intrasferibles:

Tus empleados tendrán su **usuario y contraseña** tanto para el acceso web como su **aplicación móvil.**

Así es más complicada la transferencia de identidades.

Geolocalización:

Activa la geolocalización de los fichajes de tus trabajadores.
Los trabajdores podrán fichar desde su APP y tu podrás saber **desde donde se ha realizado cada fichaje**.

Además, podrás **definir un rango de restricción** de fichaje para que salte en tu cuadro de control si algún empleado no ha fichado dentro del radio.

7 Alternativas

APP mostrador

Es una APP diseñada específicamente para fichar **solo en presencial.**

Se puede complementar a otros tipos de fichajes dentro de HRLOG.

O bien **anexar a métodos internos** de cámaras directas o un personal de vigilancia que puedan **verificar el registro** de aquellos fichajes que no nos cudren o no entren dentro de la normalidad.

hrlog

7

Alternativas

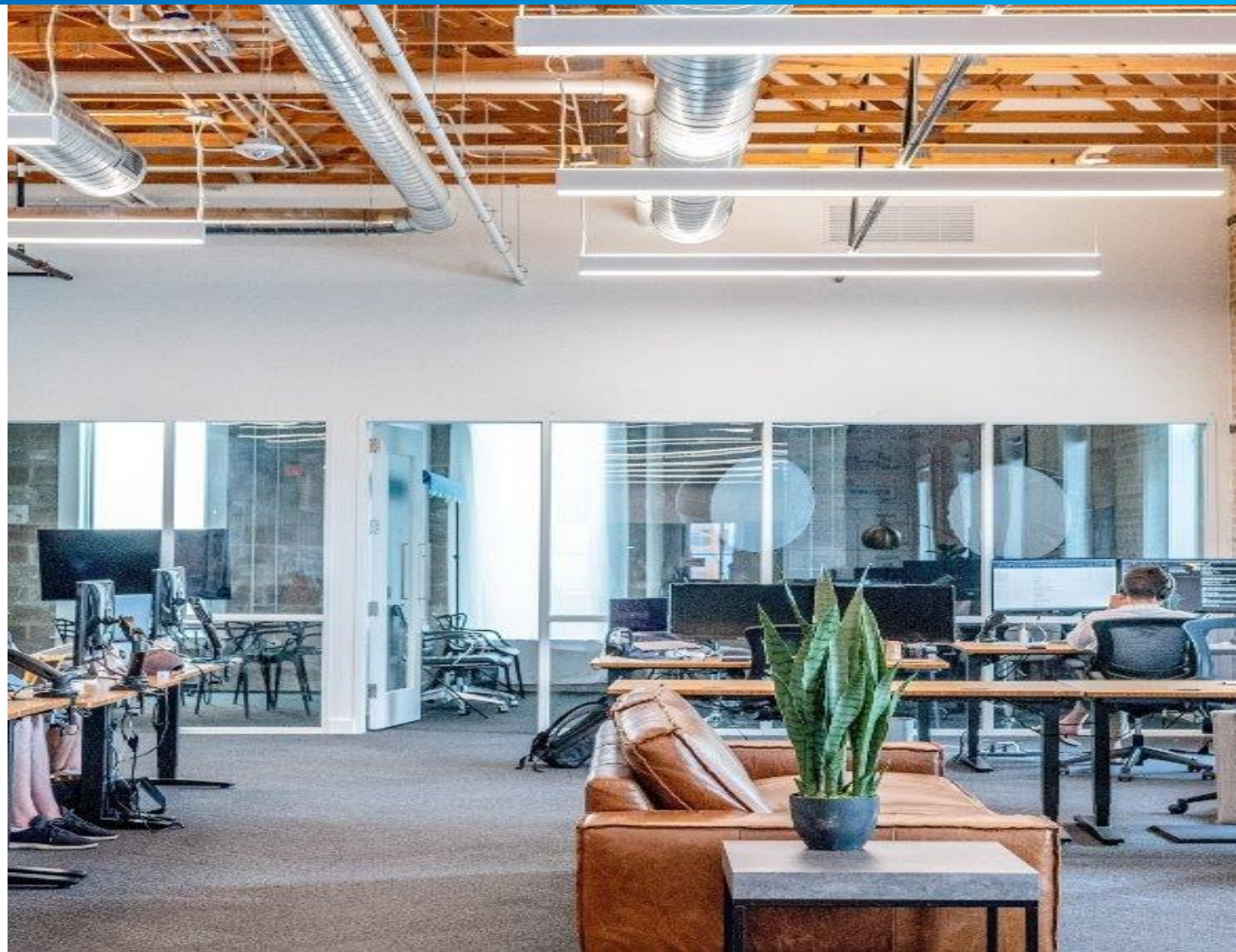
Control del tipo de fichaje:

Ficha desde el ordenador
Accede al apartado de empleados de nuestra web y ficha cómodamente.

Ficha con tu móvil
Descarga la app y ficha automáticamente desde tu móvil.

Mediante código QR
Útil para el uso de tarjetas o incluso desde el propio teléfono móvil.

Código alfanumérico
Asignando un código de números y letras a cada empleado.



¡Muchas gracias!

Contacto

Vanesa López Rueda
638 94 09 91
vlopez@hrlog.es

Hugo Martínez Lacalzada
621 12 05 99
hmartinez@hrlog.es