GUÍA SOBRE TRATAMIENTOS EN EL CONTROL DE ACCESO MEDIANTE SISTEMAS BIOMÉTRICOS		
Cuestión	**Qué plantea el borrador de la AEPD**	**Dónde**
1. Qué se entiende por control de acceso biométrico	Comprende tanto **identificación** como **autenticación** biométrica. Abarca el registro previo, almacenamiento de referencias biométricas y su comparación para autorizar o denegar el acceso. No se limita al ámbito laboral.	**Apartados 2.4 y 2.5, págs. 5-6**
2. Identificación vs. autenticación	Diferencia entre autenticación **1:1** —la persona declara previamente su identidad— e identificación **1:N**, en la que se compara la biometría con una base de datos de personas registradas.	**2.5, págs. 5-6**
3. Idoneidad del sistema	La empresa debe poder acreditar objetivamente que el sistema biométrico sirve realmente para la finalidad perseguida. La Guía contempla métricas como falsos positivos/negativos y capacidad de flujo.	**3.1.1, págs. 6-7**
4. Necesidad: comparación con alternativas	No basta con que la biometría sea útil. Debe analizarse si existen **alternativas menos intrusivas con una eficacia equivalente**. La Guía reconoce, a la vez, que tarjetas o códigos pueden resultar inadecuados cuando puedan compartirse o utilizarse por terceros.	**3.1.2, págs. 7-8**
5. Proporcionalidad	Debe ponderarse el beneficio obtenido frente a la injerencia en derechos y libertades. Un sistema puede resultar desproporcionado si genera alto riesgo y existen alternativas igualmente eficaces y menos arriesgadas.	**3.1.3, págs. 8-9**
6. Datos biométricos como categoría especial	Cuando se utilizan para identificar/autenticar a una persona en un control de acceso, entran en el régimen del **art. 9 RGPD**, independientemente de que la comparación sea 1:1 o 1:N.	**3.2, págs. 9-10**

7. Consentimiento y alternativa no biométrica	El consentimiento puede utilizarse en determinados supuestos, pero debe ser libre, específico, informado e inequívoco. Debe existir una **alternativa real**, que no suponga mayor espera, coste, penalización o menoscabo para quien no quiera utilizar biometría.	**3.2.1, pág. 10**
8. Habilitación legal	También puede levantarse la prohibición mediante una habilitación legal en los supuestos previstos por el art. 9.2 RGPD. La norma debe determinar suficientemente la finalidad y establecer garantías adecuadas.	**3.2.2, pág. 10**
9. Decisión automática de denegar el acceso	Si el sistema biométrico decide automáticamente impedir el acceso y ello produce efectos jurídicos o afecta significativamente a la persona, entran en juego las garantías del **art. 22 RGPD**, incluida la intervención humana en determinados casos.	**3.4, págs. 11-12**
10. Evaluación de Impacto obligatoria	El borrador concluye que, **antes de iniciar el tratamiento**, debe realizarse una **EIPD**, documentando además el triple juicio de idoneidad, necesidad y proporcionalidad.	**4 y 4.1, págs. 12-13; conclusiones, pág. 20**
11. Qué sistemas considera de mayor riesgo	Señala, entre otros factores: almacenamiento biométrico bajo control exclusivo de la empresa, referencias reversibles/vinculables/irrevocables, registro remoto o sin supervisión, tratamientos masivos y participación de terceros.	**4.2, págs. 13-14**
12. Garantías organizativas	Métodos alternativos de acceso, información previa al usuario, evitar captar biometría de terceros, limitar conservación y eliminar los datos cuando dejan de ser necesarios.	**4.5.1, págs. 15-16**
13. Garantías técnicas	Separación de identificadores y referencias biométricas, revocabilidad, cifrado, dispositivos certificados y seguros, procesamiento local y minimización de transmisiones.	**4.5.2, págs. 16-17**

14. Quioscos o puntos biométricos de acceso público	Deben situarse en lugares con privacidad y seguridad adecuadas y el borrador señala que **no deben estar conectados a Internet**.	**4.5.2, pág. 17**
15. IA aplicada a biometría	Cuando el sistema incorpore IA, además del RGPD deberán cumplirse las prohibiciones, limitaciones y obligaciones derivadas de la normativa europea de IA.	**Introducción, pág. 3; conclusiones, pág. 21**
16. Ámbito laboral y registro horario	Solo aquí entra específicamente en trabajadores. Señala que la normativa laboral española actual **no contiene una habilitación suficientemente específica** para utilizar biometría para control horario, aunque analiza también la vía del consentimiento y el posible papel de los convenios colectivos.	**Capítulo 5, págs. 17-20**
17. Contratas y subcontratas	Una empresa contratante no puede legitimar el uso de biometría simplemente imponiéndolo contractualmente a una contratista; deben cumplirse las condiciones del RGPD.	**5.3, págs. 19-20**