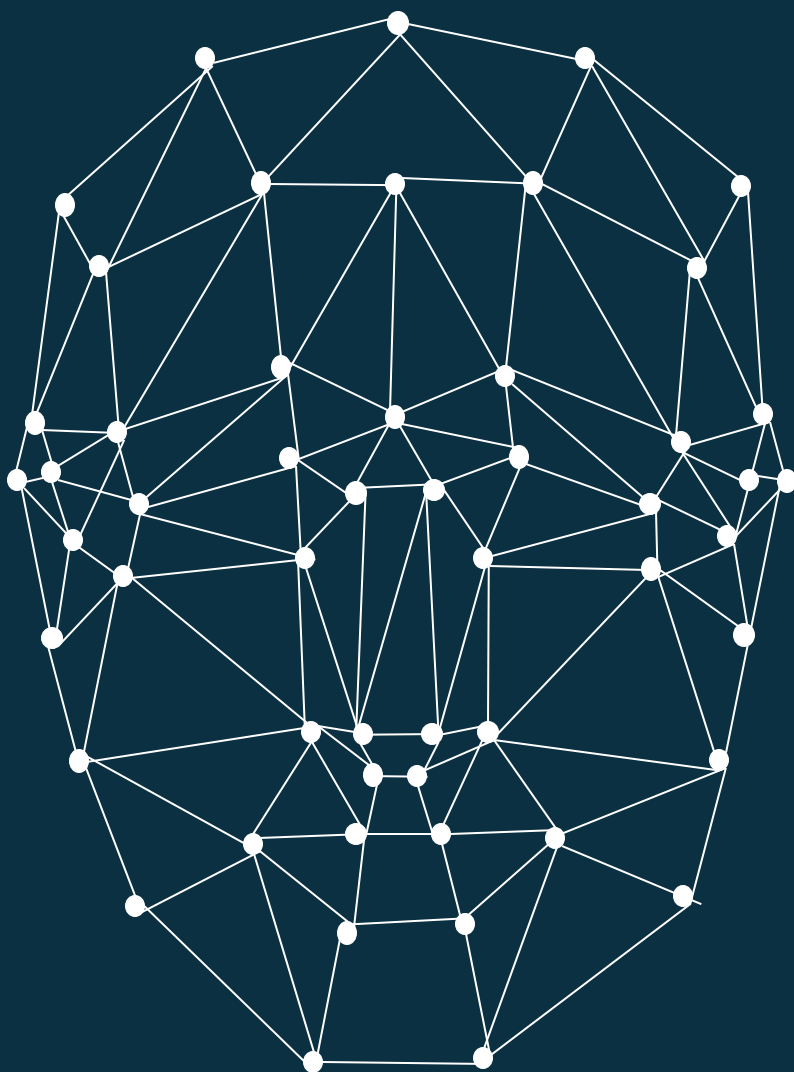




Datos biométricos: cambios decisivos

Versión 1.0 - Marzo 2025

Obsolescencia jurídica y tecnológica de la Guía de la AEPD de 2023

Análisis de los cambios normativos y tecnológicos relacionados con los datos biométricos que exigen una actualización de los criterios de la guía de la AEPD de 2023.

ribas

El objetivo de este documento es demostrar que desde el mes de noviembre de 2023 hasta ahora se han producido cambios legislativos y tecnológicos que hacen necesario actualizar la guía de la AEPD sobre tratamientos de control de presencia mediante sistemas biométricos y los criterios que en ella se incluyen.

Una resolución sancionadora que no tenga en cuenta los cambios tecnológicos y regulatorios que se están produciendo en la Unión Europea sería manifiestamente injusta.

Cambios relevantes en materia de datos biométricos

1. Junio de 2024 - El Reglamento de Inteligencia Artificial de la UE excluye los sistemas de verificación biométrica de la identidad con participación activa del interesado de los sistemas de alto riesgo, al ser su riesgo para los derechos fundamentales bajo o nulo.
2. Octubre de 2024 - Nuevos estándares del NIST sobre criptografía post-cuántica.
3. Octubre de 2024 - La Directiva 2024/2831 de 23 de octubre de 2024, relativa a la mejora de las condiciones laborales en el trabajo en plataformas digitales (Directiva PWD), prohíbe a las plataformas digitales el tratamiento de los datos biométricos de las personas que realizan trabajo en dichas plataformas digitales con fines de identificación (one-to-many identification). Por el contrario, excluye de dicha prohibición la verificación o autenticación biométrica (one-to-one verification or authentication) mediante el cotejo de sus datos biométricos con los datos proporcionados previamente por esa misma persona.
4. Diciembre de 2024 - Guía CCN-TEC 013 - Tecnologías biométricas seguras para el control de acceso.
5. Diciembre de 2024 - Preparación de normas por parte del CEN (Comité Europeo Normalización) y por parte del ETSI (Instituto Europeo de Normas de Telecomunicaciones), sobre seguridad de la información biométrica, que siguen los mismos fundamentos tecnológicos que la Norma ISO 24745:2022 y que contemplan el cambio tecnológico operado en la biometría.
6. Diciembre de 2024 - Los sistemas biométricos son reconocidos por el CCN (Centro Criptológico Nacional adscrito al CNI y al Ministerio de Defensa) como el único mecanismo automático que permite acreditar la identidad real.
7. Diciembre de 2024 - Suplantación de la identidad digital de 150 personas para obtener fármacos opioides y ansiolíticos.
8. Marzo de 2025 - La acumulación de avances tecnológicos en los sistemas de control biométrico es tan significativa que convierte en obsoletos los criterios aplicados hasta el momento por la Agencia Española de Protección de Datos y hace que las resoluciones sancionadoras basadas en estos criterios sean manifiestamente injustas.
9. Marzo de 2025 - La AEPD empieza a contemplar el impacto del Reglamento de IA en sus resoluciones, aunque no parece dispuesta a una aplicación retroactiva en favor del administrado, tal como establece la ley.
10. Marzo de 2025 - El Anteproyecto de ley para el buen uso y la gobernanza de la inteligencia artificial excluye de la lista de sistemas de IA de alto riesgo, en consonancia con el Anexo III.1 a) del Reglamento de IA, los sistemas para identificación biométrica remota cuya única finalidad sea confirmar que una persona física concreta es la persona que afirma ser.

Características que hacen que los datos biométricos destinados a la verificación de la identidad deban considerarse fuera del artículo 9.1 del RGPD, por tener una finalidad distinta y por generar un riesgo bajo o nulo para los derechos fundamentales

Inferencia de datos de salud, raza y otros datos sensibles

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Guía de la AEPD de 2023	Actualidad
La interpretación de los datos biométricos como categorías especiales de datos debe tener en cuenta la posibilidad de que, mediante el análisis biométrico, se puedan inferir y recoger otras categorías especiales de datos y, en particular, datos relativos a la salud o datos que revelen el origen racial o étnico entre otros. El desarrollo tecnológico está permitiendo extraer cada vez más detalles de los rasgos biométricos de una persona. Por ejemplo, un análisis biométrico de la voz humana puede recoger más de cien parámetros distintos que permiten extraer información de salud, problemas físicos o psicológicos, entre otros. En sistemas biométricos basados en el reconocimiento facial se pueden tratar datos que revelan el origen racial o étnico⁹, y también se puede extraer información de salud, problemas físicos o psicológicos como en el caso de la voz, incluso algunos sistemas de identificación mediante huella dactilar permiten el registro de parámetros como la temperatura o la presión sanguínea.	La plantilla biométrica RBR no contiene ningún tipo de característica biométrica concreta (no representa la distancia entre ojos, el color de piel, el sexo, etc.), sino únicamente datos derivados de las mismas. (Fuente: Guía del CCN)
	Estamos hablando de control de acceso, control de presencia y verificación de la identidad. Los datos biométricos que no son necesarios para estas finalidades son irrelevantes y no se obtienen ni se procesan.

Datos que puede revelar una fotografía y los datos biométricos destinados a control de acceso

En esta tabla se comparan los datos que puede revelar una simple fotografía y los que puede revelar una plantilla biométrica destinada al control de acceso

Datos que se pueden obtener a través de una foto o un vídeo	Datos que se pueden obtener a través los datos biométricos
Raza - Origen étnico	El interesado es, o no es, quien dice ser
Género aparente	
Contexto social o profesional	
Peso aproximado - Enfermedades o afecciones: anorexia, obesidad	
Vista corregida mediante gafas	
Color de la piel, nivel de bronceado, indicios de ictericia	
Color de los ojos	
Color del cabello	
Alopecia, rastros de quimioterapia	
Tipo de piel, sensibilidad al sol y riesgo de cáncer de piel	
Edad aproximada	
Estado anímico	
Tatuajes y piercings	
Indicios relativos a creencias religiosas: turbantes, tatuajes y piercings religiosos	
Características de la piel: arrugas, pecas y lunares, melanoma, textura, flacidez	
Características faciales: nariz fracturada, nariz desviada, orejas muy grandes...	
Parálisis facial, ceguera, estrabismo, hipertiroidismo, operaciones quirúrgicas...	
Y un largo etcétera	

Comparativa entre datos genéticos y datos biométricos utilizados para control de acceso

En esta tabla se comparan los datos que se pueden obtener con los datos genéticos y con los datos biométricos utilizados para control de acceso

Datos que se pueden obtener a través del ADN	Datos que se pueden obtener a través los datos biométricos
Origen étnico y geográfico de los ancestros	El interesado es, o no es, quien dice ser
Predisposición a enfermedades genéticas, mentales y neurológicas	
Predisposición a la obesidad	
Tolerancia a la lactosa y repuesta metabólica a cada tipo de alimento	
Tiempo de coagulación de la sangre estimado	
Predisposición a adicciones	
Respuesta a cada tipo de medicamento	
Rendimiento físico y deportivo estimado - Patrones de sueño	
Color de los ojos y del cabello	
Tipo de piel, sensibilidad al sol y riesgo de cáncer de piel	
Predisposición a la calvicie	
Relación de parentesco con otras personas	
Marcadores de edad biológica	
Tendencias de comportamiento	
Grupo sanguíneo y factor RH	
Características de la voz	
Sensibilidad a sabores y olores	
Y un largo etcétera	

Riesgos asociados a cada tipo de categoría especial de datos

En esta tabla se pueden ver ejemplos de riesgos asociados a cada tipo de dato incluido en el ámbito de aplicación del artículo 9.1 del RGPD

Categoría especial de datos	Ejemplos de riesgos	Ejemplo de valoración del riesgo
Datos biométricos con minimización extrema dirigidos exclusivamente a la autenticación biométrica en el control de acceso a la empresa.	El mayor riesgo es que el trabajador no pueda entrar y tenga que pasar por recepción	Muy bajo
Datos genéticos	Discriminación derivada del conocimiento de la predisposición a enfermedades Exclusión de seguros Exclusión de determinados puestos de trabajo o funciones	Alto
Datos de salud	Discriminación derivada del conocimiento de la predisposición a enfermedades Exclusión de seguros Exclusión de determinados puestos de trabajo o funciones	Alto
Datos sobre el origen étnico o racial	Discriminación salarial y profesional	Alto
Datos sobre opiniones políticas	Discriminación salarial y profesional	Alto
Datos sobre convicciones religiosas o filosóficas	Discriminación profesional	Medio
Datos sobre afiliación sindical	Discriminación profesional	Medio
Datos relativos a la vida sexual	Discriminación profesional	Medio
Datos relativos a la orientación sexual	Discriminación profesional	Medio

Riesgo bajo o nulo (I)

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Guía de la AEPD de 2023	Actualidad
La utilización de tecnologías biométricas de identificación y autenticación en el control de presencia supone un tratamiento de alto riesgo que incluye categorías especiales de datos.	En el Reglamento de IA de la UE los sistemas de identificación biométrica no remotos en los que existe participación activa del usuario, así como los sistemas de verificación biométrica no están prohibidos y están calificados de riesgo bajo o nulo. (Fuente: Guía del CCN).
En cuanto a los sistemas biométricos que sean implementados con técnicas de inteligencia artificial, habrá que tenerse en consideración la clasificación de dichos sistemas como de alto riesgo según el Anexo III de la propuesta de Regulación de Inteligencia Artificial.	El nuevo RIA considera que el uso de las tecnologías biométricas con la finalidad exclusiva de identificar a personas naturales, contando con su participación activa y en proximidad, mediante la comparación de sus datos biométricos con los contenidos en una base de datos de referencia – lista de control-, no representa un riesgo alto para los derechos fundamentales y la seguridad de los ciudadanos. (Fuente: Guía del CCN).
	Y esto es así porque las plantillas biométricas RBR no permiten inferir ninguna de las características anteriormente mencionadas (raza, salud, etc.), al no poder invertirse para obtener los datos brutos originales. (Fuente: Guía del CCN).

Riesgo bajo o nulo (II)

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Guía de la AEPD de 2023	Actualidad
La utilización de tecnologías biométricas de identificación y autenticación en el control de presencia supone un tratamiento de alto riesgo que incluye categorías especiales de datos.	El Anteproyecto de ley para el buen uso y la gobernanza de la inteligencia artificial excluye de la lista de sistemas de IA de alto riesgo, en consonancia con el Anexo III.1 a) del Reglamento de IA, los sistemas para identificación biométrica remota cuya única finalidad sea confirmar que una persona física concreta es la persona que afirma ser.
En cuanto a los sistemas biométricos que sean implementados con técnicas de inteligencia artificial, habrá que tenerse en consideración la clasificación de dichos sistemas como de alto riesgo según el Anexo III de la propuesta de Regulación de Inteligencia Artificial.	

Contradicciones y paradojas

La Agencia Española de Protección de Datos considera que la verificación biométrica realizada con la participación activa del usuario con el fin de autorizar su acceso a un sistema informático está incluida en la lista de categorías especiales de datos del artículo 9.1 del RGPD. Esta interpretación coloca esta finalidad, que el Reglamento de IA considera de bajo riesgo, por encima de otras finalidades de alto riesgo como la creación de una voz clonada o de un avatar con datos biométricos. En la siguiente tabla se describe la situación contradictoria y paradójica que genera mantener esta interpretación.

	Creación de una voz clonada o un avatar con datos biométricos del interesado	Verificación o autenticación biométrica
Función de los datos biométricos	Garantiza la máxima fidelidad en la reproducción de la voz y de la imagen de la persona clonada	Permite la autenticación de un usuario recurrente de un sistema informático comparando los datos biométricos de la voz o de la imagen suministrados en el momento de la solicitud de acceso con los que facilitó el propio usuario en el momento del registro.
Datos utilizados	Patrón biométrico obtenido a través de la voz o de la imagen	Patrón biométrico obtenido a través de la voz o de la imagen
Uso de los datos	La elaboración de patrones biométricos permite crear voces y avatares que reproduzcan los mismos patrones	Se compara el patrón biométrico creado en el momento del registro con el creado en el momento de la solicitud de acceso
Finalidad	Crear una voz o una imagen idéntica que la de la persona clonada, que sea capaz de leer textos o mantener una conversación.	Autorizar el acceso del usuario al sistema
Riesgos para el interesado	Atribución de acciones, infracciones y delitos a la persona clonada	Denegación del acceso y necesidad de registro como usuario
Nivel de riesgo para el interesado	Riesgo alto	Riesgo bajo
Riesgo según el legislador	No está previsto en el artículo 9.1 del RGPD	Interpretaciones discrepantes
Riesgo según la AEPD	No consta una valoración al respecto, por lo que se aplicaría la lista del artículo 9.1 del RGPD	Riesgo alto

Finalidad de datos biométricos incluidos en el artículo 9.1 del RGPD

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Finalidad incluida en el artículo 9.1	Finalidades no incluidas en el artículo 9.1
Identificación unívoca de una persona física	Tratamiento de datos biométricos destinado a la inferencia de emociones
	Categorización biométrica
	Tratamiento de datos biométricos destinado a la clonación de la voz
	Tratamiento destinado a la detección de voces clonadas
	Firma biométrica destinada a acreditar el consentimiento del interesado
	Verificación de la identidad con participación activa del interesado

Conclusiones del CCN

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Conclusiones de la guía del CCN sobre el uso de datos biométricos en el control de acceso
La plantilla biométrica RBR obtenida a partir de los rasgos (datos) biométricos es específica de una persona, pero no es en absoluto única ni tampoco permanente. Además, es privada, irreversible, no interoperable, revocable y múltiple.
Los mecanismos de control de acceso basados en la autenticación mediante comparación de una plantilla biométrica RBR dificultan la falsificación en comparación con otros métodos de autenticación, proporcionando una capa adicional de seguridad. El factor de inherencia propio de la biometría ofrece garantías de que la identidad es real, presentando ventajas significativas en comparación con factores de posesión o conocimiento que podrían ser cedidos o sustraídos por terceros.
El reglamento europeo de Inteligencia Artificial, que clasifica las aplicaciones de los sistemas de reconocimiento biométrico según el riesgo que puedan representar, califica las soluciones de uso de la biometría para el acceso con la intervención voluntaria del usuario y habitualmente en proximidad, como de bajo o nulo riesgo para los derechos fundamentales de las personas.
El Centro Criptológico Nacional recomienda para el nivel alto de seguridad el uso de sistemas de control de acceso basados en el uso de plantillas biométricas RBR (u otras que puedan surgir en un futuro que presenten protecciones equivalentes), evaluados y certificados conforme a las normas y estándares nacionales e internacionales sobre la materia.

Características que hacen que el control biométrico supere el triple juicio de idoneidad, necesidad y proporcionalidad

Esquema Nacional de Seguridad

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Guía de la AEPD de 2023	Actualidad
La guía de 2023 no analiza esta norma.	En el ENS la biometría se considera como un factor de autenticación. Hay 3 tipos de factores de autenticación: (1) Algo que se sabe, una contraseña o secreto. (2) Algo que se tiene, un token o autenticador. (3) Algo que se es, una característica biométrica. (Fuente: Guía del CCN y ENS).
	El ENS contempla como uno de los componentes que forma parte del sistema de identificación y autenticación de usuarios, que es parte de la medida [op.pl.2 Arquitectura de Seguridad]. También aparece como refuerzo en las medidas [op.acc.5 Mecanismo de autenticación (usuarios externos)] y [op.acc.6 Mecanismo de autenticación (usuarios de la organización)] (Fuente: Guía del CCN y ENS).

Comparativa entre factores de autenticación basada en el ENS

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Factor de autenticación	Ejemplos	Riesgo robo o de cesión a terceros
Algo que el interesado sabe	1. Contraseña. 2. PIN. 3. Secreto.	Muy alto
Algo que el interesado tiene	1. Código recibido por SMS. 2. Código QR. 3. Token. 4. Autenticador. 5. Tarjeta de acceso. 6. DNI o pasaporte.	Muy alto
Algo que el interesado es	Característica biométrica inherente al cuerpo del interesado e inseparable de él. Ejemplos: 1. Cara. 2. Huella dactilar. 3. Mano. 4. Voz. (Con sistema IA de detección de voz clonada) 5. Iris. 6. Otros.	Muy bajo

Criterios para valorar sistemas alternativos al control biométrico

Criterios utilizados en la valoración de sistemas alternativos al control biométrico y del riesgo de suplantación de identidad

Criterio
Riesgo de cesión del dispositivo, de la contraseña o de cualquier otro factor de autenticación por parte del interesado a un tercero no autorizado.
Riesgo de pérdida o extravío del dispositivo de identificación
Riesgo de sustracción del dispositivo de identificación
Riesgo de acceso no autorizado al contenido del dispositivo de identificación o a los datos asociados a él.
Riesgo de uso no autorizado del dispositivo de identificación.
Riesgo de réplica o duplicación del dispositivo de identificación.
Nivel de seguridad del dispositivo de identificación.
Credibilidad de la suplantación de identidad.
Duración máxima posible de la suplantación de identidad de acuerdo con las medidas de seguridad existentes en la empresa.
Riesgo de acceso físico no autorizado a la empresa gracias a la suplantación de identidad.
Riesgo de atribución al interesado de las acciones e infracciones realizadas con el dispositivo.

Factor de inherencia

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Guía de la AEPD de 2023	Actualidad
La guía de 2023 no analiza esta característica.	La utilización del factor de inherencia que es consustancial a la biometría. Aporta una garantía de identidad real que no se pueden obtener de los factores de posesión o conocimiento, los cuales pueden ser cedidos o sustraídos por otras personas. (Fuente: Guía del CCN).

Menor eficacia de la verificación manual

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Guía de la AEPD de 2023	Actualidad
La guía de 2023 no analiza esta característica.	La acreditación de identidad de forma manual consiste en la revisión manual por parte de una persona de la autenticidad del documento de identidad del portador, así como de la correspondencia del documento con la persona que lo porta. (Fuente: Guía del CCN).
	Esta forma de acreditación tiene un nivel de equivalencia similar al biométrico. (Fuente: Guía del CCN). En el plano teórico es similar, pero en la práctica la eficacia de la acreditación manual es muy inferior, debido a su alta tasa de error y falsos positivos y negativos.
	La eficacia de la acreditación automática con datos biométricos es superior, ya que es más rápida y tiene un margen de error muy inferior.
	El error humano, que se ha convertido en la primera causa de los incidentes de seguridad, también puede producirse en la verificación manual de la identidad. A pesar de todas las medidas aplicadas para su predicción (Técnica THERP) y reducción (Técnica SHERPA), siempre existe un riesgo residual insalvable, tal como indica el Ministerio de Trabajo en su nota técnica sobre los métodos de análisis de la fiabilidad humana.
	La capacidad del ser humano de verificar la identidad de una persona está sujeta a múltiples errores, como veremos en la siguiente página.

Errores del ser humano en la autenticación manual

Tipo de error	Ejemplos
1. Errores de percepción y comparación	1. Similitud con otra persona. 2. Similitud de rasgos entre familiares. 3. Similitud de rasgos raciales. Este error es relevante en las empresas con trabajadores extranjeros. 4. Cambios físicos: barba, maquillaje, cambios en el peso, envejecimiento. 5. Fatiga visual, estrés, cansancio, alta frecuencia o excesiva velocidad de los reconocimientos.
2. Errores por falta de atención	1. No revisar con detenimiento los rasgos faciales por prisa o rutina. 2. Pasar por alto pequeños detalles (cicatrices, lunares, asimetrías). 3. No comparar con suficiente tiempo la foto con el rostro real. 4. Distraerse con otros elementos del documento (fecha de nacimiento, nombre) y no centrarse en la imagen.
3. Errores debido a sesgos cognitivos	1. Sesgo de comparación: confianza excesiva en una característica facial. 2. Sesgo de confirmación: Si el verificador cree que la persona es legítima, puede pasar por alto discrepancias. 3. Efecto de familiaridad: Si el individuo parece "confiable", el agente puede no revisar con la misma rigurosidad. 4. Discriminación inconsciente: Algunas personas pueden recibir más escrutinio que otras según su apariencia.

Alternativa a los sistemas basados en una presunción de identidad

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Guía de la AEPD de 2023	Actualidad
En relación con el requisito de la posible “equivalencia de los tratamientos” hay que tener en cuenta que, si existen alternativas disponibles al tratamiento de datos biométricos que impliquen menor riesgo para los derechos y libertades de las personas cuyos datos personales se van a tratar, que permitan que en un momento dado todos los trabajadores opten por otras alternativas, el procesamiento de datos biométricos deja de ser necesario para la implementación del tratamiento. Debe demostrarse la necesidad objetiva (requisito para tratamientos de alto riesgo) y las posibles alternativas, de tal manera que para poder tratar esos datos biométricos no exista otra alternativa que sirva para satisfacer la necesidad identificada y que implique un riesgo menor en los derechos y libertades de las personas físicas.	El uso de tecnologías biométricas aporta garantías de inherencia, a diferencia de otros medios basados en contraseñas o el uso de dispositivos físicos, cuyo uso sólo puede dar lugar a una identidad presunta (dado que pueden ser cedidas o robadas).
	El uso de contraseñas genera una presunción de identidad en relación con su titular, ya que la contraseña puede ser cedida a un tercero o robada.
	El uso de dispositivos físicos genera una presunción de identidad en relación con su titular, ya que el dispositivo puede ser cedido a un tercero o robado.
	Los sistemas biométricos son el único mecanismo automático que permite acreditar la identidad real. (Fuente: Guía del CCN).

Único sistema de autenticación eficaz

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Guía de la AEPD de 2023	Actualidad
En relación con el requisito de la posible “equivalencia de los tratamientos” hay que tener en cuenta que, si existen alternativas disponibles al tratamiento de datos biométricos que impliquen menor riesgo para los derechos y libertades de las personas cuyos datos personales se van a tratar, que permitan que en un momento dado todos los trabajadores opten por otras alternativas, el procesamiento de datos biométricos deja de ser necesario para la implementación del tratamiento. Debe demostrarse la necesidad objetiva (requisito para tratamientos de alto riesgo) y las posibles alternativas, de tal manera que para poder tratar esos datos biométricos no exista otra alternativa que sirva para satisfacer la necesidad identificada y que implique un riesgo menor en los derechos y libertades de las personas físicas.	Los sistemas biométricos son el único mecanismo automático que permite acreditar la identidad real. (Fuente: Guía del CCN).
	Los sistemas basados en contraseñas (“algo que sabes”) o basados en la tenencia de un dispositivo (“algo que tienes”) no permiten acreditar que la persona que lleva a cabo el proceso de autenticación es realmente quien dice ser. Se trata de sistemas basados en la presunción de que la persona que conoce una contraseña o tiene un dispositivo es quien dice ser. (Fuente: Guía del CCN y ENS).
	Sin embargo, el factor de inherencia (“algo que eres”) está recogido como un factor que, combinado con los anteriores, aporta una capa más de seguridad y puede ser empleado en entornos con mayores exigencias. (Fuente: Guía del CCN y ENS).

Falsos positivos y falsos negativos

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Guía de la AEPD de 2023	Actualidad
Para que un tratamiento se pueda considerar idóneo, ha de permitir cumplir con la finalidad última del tratamiento con unos niveles adecuados de calidad, teniendo en cuenta que no hay tratamiento que esté libre de errores ni de posibilidad de fraude.	Tasas de falsos positivos por debajo de 0.000001 (Fuente: CCN) Es decir, sólo un 0.0001% de las veces el sistema biométrico confunde a dos personas diferentes indicando que son la misma persona. (Fuente: CCN)
	Tasas de falsos negativos inferiores a 0.005. (Fuente: CCN) Es decir, sólo el 0,5% de las personas legítimas son rechazadas de forma incorrecta. (Fuente: CCN)
	El error humano, que se ha convertido en la primera causa de los incidentes de seguridad, también puede producirse en la verificación manual de la identidad. A pesar de todas las medidas aplicadas para su predicción (Técnica THERP) y reducción (Técnica SHERPA), siempre existe un riesgo residual insalvable, tal como indica el Ministerio de Trabajo en su nota técnica sobre los métodos de análisis de la fiabilidad humana.

La aplicación de un sistema alternativo genera un riesgo para la seguridad

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Guía de la AEPD de 2023	Actualidad
Deben ofrecerse sistemas alternativos equivalentes y menos intrusivos	Cualquier otro sistema diferente al biométrico no ofrece una seguridad equivalente en el control de acceso. (Fuente: CCN)
	La aplicación de sistemas alternativos genera un riesgo para la seguridad.

**Medidas que reducen más si cabe el riesgo bajo, según el RIA, de
afectación de derechos fundamentales en el uso de los datos
biométricos y en el caso de brecha de seguridad**

Las plantillas biométricas han sido superadas por los modelos biométricos

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Guía de la AEPD de 2023	Actualidad
La guía de la AEPD indica que una plantilla biométrica es una forma de escritura de una característica biométrica humana , como un rostro o una huella dactilar, de manera que sea interpretable por una máquina de forma eficiente y eficaz para un propósito o propósitos determinados.	La guía del CCN indica que en la actualidad se utilizan métodos de aprendizaje automático (Machine Learning) o incluso aprendizaje profundo (Deep Learning). En este caso la plantilla no es un conjunto de características, sino los parámetros generados por una red neuronal y se le denomina modelo biométrico.
	La norma ISO 24745 estandariza protecciones adicionales de seguridad a las plantillas biométricas creando las denominadas “Renewables Biometric References (RBR)” o “plantillas biométricas RBRs”

Múltiples plantillas de un mismo rostro o huella

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Guía de la AEPD de 2023	Actualidad
La guía de 2023 no analiza esta característica.	Sobre cada rostro, iris o huella dactilar de una persona pueden obtenerse una cantidad casi infinita de plantillas "RBRs" distintas. (Fuente: Guía del CCN y norma ISO 24745)
	Ello ofrece la posibilidad de revocar plantillar y sustituirlas por otras nuevas todas las veces que se quiera.

Irreversibilidad

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Guía de la AEPD de 2023	Actualidad
El hecho de que, a partir de una plantilla biométrica, por ejemplo, de reconocimiento facial, no se pueda reconstruir el rostro original carece de relevancia, pues es un identificador único que lo singulariza unívocamente, al menos, en el marco de un tratamiento automatizado. De igual forma, a partir de únicamente del número de DNI no se puede reconstruir un nombre o un rostro. A ambos identificadores únicos, plantilla biométrica o número del DNI, se les puede asociar datos personales y atributos adicionales en un fichero.	Es imposible obtener, a partir de una plantilla RBR, los rasgos biométricos de una persona. (Fuente: Guía del CCN y norma ISO 24745)
	Las personas con escasos conocimientos en la materia tienen la creencia falsa y el temor injustificado de que una plantilla biométrica permite reconstruir la cara o la huella dactilar a partir de la que ha sido obtenida. Tal como indica el CCN, es imposible obtener, a partir de una plantilla RBR, los rasgos biométricos de una persona. Ello es así gracias a tecnología utilizada y al escaso número de referencias seleccionado.
	Un identificador único no es un dato sensible en sí mismo. No está incluido en la lista de categorías especiales de datos del artículo 9.1 del RGPD. En el control de acceso es posible utilizar plantillas anónimas, desvinculadas de una persona concreta, que no actúen como identificador único.

Minimización de datos

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Guía de la AEPD de 2023	Actualidad
La guía recomienda aplicar la minimización de los datos biométricos recogidos, con una evaluación objetiva de que no ha posibilidad de revelar categorías especiales de datos adicionales.	En la actualidad se aplica el principio de minimización extrema, consistente en recoger únicamente los datos de referencia estrictamente necesarios para asegurar las finalidades de la creación de la plantilla.

Minimización extrema en el tratamiento de datos biométricos de trabajadores

Los cálculos de Roxburgh para el número mínimo de detalles necesarios para declarar una coincidencia positiva, con un margen de error de 1 en 50 000.¹

Población o Numero en clase ²	Character of Print				
	(i) Ideal	(ii) En promedio buena	(iii) En promedio mala	(iv) Deficiente	(v) Muy mala
10 ¹	2	3	3	3	8
10 ²	3	3	4	4	9
10 ³	4	4	5	6	10
10 ⁴	4/5	5	6	7	11
10 ⁵	5	6	6/7	8	12
10 ⁶	6	7	7/8	9	13
10 ⁷	7	8	8	10	14
10 ⁸	7	8	9	11	15/16
10 ⁹	8	9	10	12	16/17
1.6 x 10 ⁹ (mundo)	8	9	10/11	12/13	17
1.6 x 10 ¹⁰ (dedo descono- cido)	9	10	11	13	18

Cómo funciona la minimización extrema

Esta tabla proviene de “El libro de referencia de la huella dactilar” publicado en 2017 por el Departamento de Justicia de los EEUU.

En este libro se explican los diferentes métodos de identificación de una persona a través de datos biométricos y la probabilidad de tener éxito en esta identificación en función del número de minucias y el número de personas que forman la población.

La aplicación de esta escala ha permitido hasta ahora seguir una de las recomendaciones de la AEPD en su guía sobre tratamientos de control de presencia mediante sistemas biométricos. Esta recomendación, prevista en la página 8 de la guía, consiste en configurar el sistema para adecuarlo a las necesidades concretas del tratamiento, y conseguir una evaluación objetiva cuyo resultado sea que no hay recogida de datos innecesarios para cumplir el propósito del tratamiento, de acuerdo con el artículo 35 del RGPD.

La minimización extrema sería más exigente que este criterio y limitaría el número de minucias utilizadas en función del número de interesados autenticados.

Características adicionales del tratamiento que refuerzan los efectos de la minimización extrema

Múltiples plantillas

La minimización extrema permite obtener múltiples plantillas de una única muestra.

Revocabilidad

Al existir la posibilidad de obtener múltiples plantillas, también es posible revocarlas.

Sistemas incompatibles

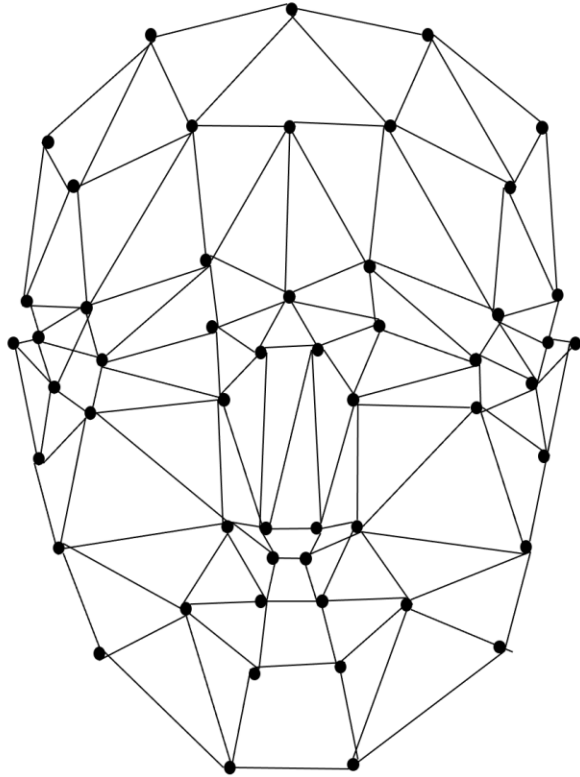
El formato de los datos tratados en un sistema es incompatible con los datos tratados en otro sistema, lo cual impide la suplantación de identidad.

Irreversibilidad

Un acceso no autorizado o una exfiltración de datos no permitiría utilizar recuperar las características biométricas a las que hace referencia..

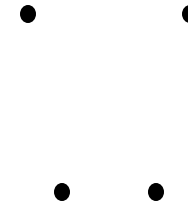
Efectos de la minimización extrema

Los puntos de referencia de una plantilla biométrica se limitan a los necesarios para conseguir verificar la identidad del interesado



Lo que muchas personas piensan

Los datos biométricos han sido demonizados a causa de la creencia en riesgos asociados a la suplantación de la personalidad y a la obtención de datos de salud o las emociones



Lo que las empresas tratan

Las empresas únicamente tratan el número mínimo de puntos de referencia para verificar la identidad de una persona en una comunidad pequeña de usuarios. Por ejemplo, 4 puntos para un grupo de 1000 personas.

Renovación

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Guía de la AEPD de 2023	Actualidad
La guía de 2023 no analiza esta característica.	Las características biométricas de una persona son inmutables, pero las plantillas biométricas RBR obtenidas a partir de dichas características no lo son. La obtención de la plantilla depende del algoritmo biométrico utilizado y de los mecanismos utilizados en su protección, que siempre puede parametrizarse, modificarse y/o renovarse. Dos algoritmos distintos producirán dos plantillas biométricas distintas a partir de los mismos datos biométricos. (Fuente: Guía del CCN)

No interoperabilidad

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Guía de la AEPD de 2023	Actualidad
Una de las medidas recomendadas una vez superados todos los requisitos de cumplimiento de los principios generales del RGPD, consiste en implementar medios técnicos para asegurar la imposibilidad de utilizar las plantillas para cualquier otro propósito. También recomienda utilizar formatos de datos o tecnologías específicas que imposibiliten la interconexión de bases de datos biométricos y la divulgación de datos no comprobada.	Para cada caso de uso se crea una plantilla “RBR” específica partiendo de los mismos rasgos, pero utilizando factores de ordenación distintos. (Fuente: Guía del CCN y norma ISO 24745)
	No es posible emplear la plantilla biométrica RBR generada para un propósito distinto al establecido cuando se generó. Cada plantilla biométrica RBR se genera de forma única y asociada al caso de uso o aplicativo específico. (Fuente: Guía del CCN y norma ISO 24745)
	Otro de los falsos mitos de los datos biométricos es que podrían ser utilizados por otras personas para suplantar la identidad del interesado. Sin embargo, la tecnología actual hace imposible el uso de una plantilla biométrica en otro sistema o para propósitos distintos a los establecidos inicialmente.

Incompatibilidad

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Guía de la AEPD de 2023	Actualidad
La guía de 2023 no analiza esta característica.	Dos algoritmos distintos producirán dos plantillas biométricas distintas a partir de los mismos datos biométricos. (Fuente: Guía del CCN)
	Ello significa que una plantilla biométrica generada en una aplicación con un algoritmo determinado no será compatible con otra aplicación que utilice otro algoritmo, y por lo tanto la plantilla biométrica no podrá ser utilizada fuera del sistema que la creó.
	La importante consecuencia de esta incompatibilidad es que no es posible suplantar la identidad del interesado con una plantilla biométrica actual.

Control del interesado

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Guía de la AEPD de 2023	Actualidad
Entre las medidas recomendables para minimizar el riesgo se encuentra la utilización de tecnologías biométricas debería basarse en utilizar dispositivos bajo el control exclusivo de los usuarios.	Como consecuencia de la falta de interoperabilidad, las plantillas biométricas RBR son datos con una usabilidad limitada, y sólo pueden ser utilizadas eficazmente por el individuo al que pertenecen. Incluso en caso de posible robo, el impacto sobre el usuario es mínimo. La plantilla por sí sola no da acceso a ningún sistema. (Fuente: Guía del CCN)

Revocabilidad

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Guía de la AEPD de 2023	Actualidad
La revocabilidad es una medida a aplicar una vez superados todos los requisitos de cumplimiento de los principios generales del RGPD, y consiste en implementar en el sistema biométrico la posibilidad de revocar el vínculo de identidad entre la plantilla biométrica y la persona física.	En caso de compromiso de un sistema, las plantillas RBR pueden ser revocadas y sustituidas por otras. (Fuente: Guía del CCN y norma ISO 24745)
	Si una plantilla es revocada y eliminada de la lista de plantillas válidas del sistema, no será reconocida como válida a partir del momento de la revocación y no se autorizará el acceso.
	En el caso de plantillas anónimas no es necesaria la medida de la revocabilidad, ya que no existe vínculo de identidad entre la plantilla biométrica y el interesado, sino entre la plantilla biométrica y los derechos de acceso.
	En el control de acceso la comparación se produce entre una plantilla anónima incluida en la lista de plantillas con derecho de acceso del sistema, y la plantilla generada por el interesado en el momento de la autenticación con el fin de acreditar su derecho de acceso.

No permanencia

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Guía de la AEPD de 2023	Actualidad
La guía de 2023 no analiza esta característica.	La expresión numérica concreta de una plantilla “RBRs” se puede modificar mediante cambios en el sistema. (Fuente: Guía del CCN y norma ISO 24745)

Datos anónimos

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Guía de la AEPD de 2023	Actualidad
La guía de 2023 no analiza esta característica.	La plantilla biométrica RBR no contiene ningún tipo de característica biométrica concreta (no representa la distancia entre ojos, el color de piel, el sexo, etc.), sino únicamente datos derivados de las mismas. (Fuente: Guía del CCN)
	No es posible conocer de qué persona se trata simplemente teniendo acceso a la plantilla biométrica RBR. (Fuente: Guía del CCN)

Cifrado en origen

Diferencias entre la guía sobre la utilización de datos biométricos para el control de presencia y acceso de la AEPD de 2023 y la actualidad

Guía de la AEPD de 2023	Actualidad
La guía recomienda utilizar cifrado para proteger la confidencialidad, disponibilidad e integridad de la plantilla biométrica.	Los sistemas biométricos que incluyen la generación de plantillas RBR, además de obtener la plantilla biométrica, suele incorporar mecanismos de cifrado, añadiendo una capa adicional de protección. La plantilla biométrica cifrada sólo puede ser descifrada por los propios mecanismos que la generaron. (Fuente: Guía del CCN).

Copia del DNI vs. plantilla biométrica RBR

Diferencias entre la copia del DNI y el tratamiento de datos biométricos

Copia del DNI	Plantilla biométrica RBR
A través de la foto del DNI se pueden obtener todos los datos relacionados en la tabla comparativa entre la foto y el dato biométrico.	A través de la plantilla biométrica únicamente se puede obtener el dato de que el interesado es o no es quien dice ser.
En caso de brecha de seguridad, el atacante puede acceder a la copia íntegra del DNI.	En caso de brecha de seguridad, el atacante accedería a datos cifrados, minimizados, seudonimizados y en un formato incompatible e interoperable.
	Los datos biométricos seudonimizados son anónimos para terceros
Identifica plenamente a la persona	No permiten identificar a la persona si no son comparados con los datos generados en el momento de la verificación.
Los datos se muestran en abierto	No se puede acceder a los datos de origen.

Comparativa entre las plantillas biométricas previas a 2022 y las actuales

Diferencias entre las características de las plantillas biométricas previas a la ISO 24745 de 2022 y las actuales

	Plantillas biométricas previas al formato de la ISO 24745 de 2022	Plantillas biométricas actuales con las características de la ISO 24745
Número de plantillas biométricas que se pueden obtener	Una única plantilla biométrica	Múltiples plantillas biométricas
Irreversibilidad	Plantillas biométricas reversibles	Plantillas biométricas irreversibles
Minimización de datos	Número de referencias alto	Número de referencias limitado al mínimo necesario para la finalidad
Renovación	Imposibilidad de renovación de la plantilla biométrica	Posibilidad de renovación de la plantilla biométrica
No interoperabilidad	Plantillas biométricas interoperables y compatibles	Plantillas biométricas no interoperables e incompatibles
Control del interesado	Control limitado	Control más amplio
Revocabilidad	Plantillas irrevocables	Plantillas revocables
Permanencia	Imposibilidad de modificar la expresión numérica de la plantilla	Posibilidad de modificar la expresión numérica de la plantilla
Datos anónimos	Datos seudonimizados	Datos seudonimizados y datos anonimizados

Conclusiones

Conclusiones obtenidas a través del análisis de la información reflejada en este documento

La plantilla biométrica RBR es el único sistema que permite acreditar la identidad real del interesado
El Reglamento de inteligencia artificial, que clasifica las aplicaciones de los sistemas de reconocimiento biométrico según el riesgo que puedan representar, califica las soluciones de uso de la biometría para el acceso con la participación voluntaria del interesado y habitualmente en proximidad, como de riesgo bajo o inexistente para los derechos fundamentales de las personas.
La aplicación de las medidas previstas la ISO 24745
La acumulación de avances tecnológicos en los sistemas de control biométrico es tan significativa que convierte en obsoletos los criterios aplicados hasta el momento por la Agencia Española de Protección de Datos y hace que las resoluciones sancionadoras basadas en estos criterios sean manifiestamente injustas.

Datos de contacto

Nombre del despacho	Ribas
Domicilio	Diagonal 640 1C - 08017 Barcelona
Persona de contacto	Xavier Ribas
Correo electrónico	xavier.ribas@ribastic.com
Teléfono fijo	934940748
Teléfono móvil	639108413
LinkedIn	https://www.linkedin.com/in/javierribas/
Web	http://ribas.legal
Blog	http://xribas.com