



# Universidad Politécnica de Madrid

Escuela Técnica Superior de Ingenieros de  
Telecomunicación

## Grado en Ingeniería Biomédica

Trabajo Fin de Grado

DISEÑO Y DESARROLLO DE UN SISTEMA DE RECONOCIMIENTO  
BIOMÉTRICO A TRAVÉS DEL ECG BASADO EN REDES  
NEURONALES CONVOLUCIONALES

Madrid 2020

Tutora

Carmen Sánchez Ávila

Autora

Irene Marín Radoszynski



# Diseño y desarrollo de un sistema de reconocimiento biométrico a través del ECG basado en Redes Neuronales Convolucionales

**Autora:** Irene Marín Radoszynski

**Tutora:** Carmen Sánchez Ávila

**Departamento:** Matemática Aplicada a las Tecnologías de la Información y las Comunicaciones

## **Tribunal**

**Presidente/a:**

**Vocal:**

**Secretario/a:**

Realizado el acto de defensa y lectura del Trabajo Fin de Grado el  
día ..... de ..... de 2020 en .....

**Calificación:** .....

PRESIDENTE/A

VOCAL

SECRETARIO/A





# Universidad Politécnica de Madrid

Escuela Técnica Superior de Ingenieros de  
Telecomunicación

## Grado en Ingeniería Biomédica

Trabajo Fin de Grado

DISEÑO Y DESARROLLO DE UN SISTEMA DE RECONOCIMIENTO  
BIOMÉTRICO A TRAVÉS DEL ECG BASADO EN REDES  
NEURONALES CONVOLUCIONALES

Madrid 2020

Tutora

Carmen Sánchez Ávila

Autora

Irene Marín Radoszynski



# Resumen

## Resumen

En el mundo en el que vivimos, el reconocimiento biométrico está cada vez más presente en nuestras vidas; por ejemplo, hacemos uso de la autenticación biométrica cada vez que desbloqueamos nuestros smartphones con escáneres de huellas dactilares o entramos en otros países mediante puertas de control de acceso fronterizo automatizadas con tecnología de reconocimiento facial. En este proyecto se estudia un novedoso enfoque en este campo, que está atrayendo cada vez más la atención de la comunidad científica: el uso del electrocardiograma (ECG) como característica biométrica. Esta tecnología todavía inmadura para esta aplicación, presenta grandes ventajas de cara al futuro, permitiendo la identificación y autenticación de personas a través de la actividad eléctrica del corazón, una señal muy difícil de falsificar y que, además, sirve como indicador de vida a la hora de detectar determinado tipo de ataques, en especial aquellos relacionados con la suplantación del usuario.

En esta dirección, hemos diseñado y desarrollado un sistema biométrico a través del ECG basado en el *Deep Learning*, y más concretamente, haciendo uso de redes neuronales convolucionales. Para llevarlo a cabo, hemos utilizado una base de datos de 105 personas sanas, cuyas señales de ECG se han sometido a una fase de preprocesamiento para, a continuación, realizar una extracción de sus características empleando una red neuronal convolucional y, finalmente, su clasificación biométrica. Este sistema se ha evaluado tanto en la modalidad de identificación de usuarios como en la verificación de la identidad, obteniendo resultados muy prometedores que nos permiten apoyar la afirmación de que el ECG posee importantes características para el reconocimiento biométrico. No obstante, es necesario seguir investigando en esta área tan novedosa y prometedora, para mejorar el rendimiento a largo plazo de estos sistemas biométricos basados en el ECG.

## Palabras clave

ECG, electrocardiograma, biometría, identificación, autenticación, verificación de la identidad, *Deep Learning*, redes neuronales convolucionales.

## Summary

In the world we live nowadays, biometric recognition has become a key element in our lives; for example, we are authenticated with biometric traits every time we unlock our smartphones with our fingerprints or when we go through a facial recognition scan at the border checkpoints. In this project, we investigate a new approach in the field of biometric recognition that has captured the attention of the scientific community: the use of the electrocardiogram (ECG) as a biometric trait. This technology is still in a development phase, yet it offers great opportunities to identify and authenticate people by their heart electrical activity. Those signals are difficult to falsify and can be used to prove user's life to detect impersonation attacks.

In this line, we have designed and developed a biometric system that uses ECG based on Deep Learning, and more specifically based on Convolutional Neural Networks. We have used a database that contains data of 105 healthy people. The ECG of those people has been preprocessed to be later used in a feature extraction process by the CNN and finally been classified. This method has been used to identify users as well as to verify their identity. In both cases the results are promising and shows that the ECG can be used to perform biometric recognition. Nonetheless, it is still necessary to continue this line of research in order to improve the performance of these biometric systems based on the ECG.

## Keywords

ECG, electrocardiogram, biometrics, identification, authentication, identity verification, Deep Learning, Convolutional Neural Networks.

## **Agradecimientos**

---



# Índice general

<b>Resumen</b>	<b>VII</b>
<b>Agradecimientos</b>	<b>IX</b>
<b>Índice general</b>	<b>XI</b>
<b>Índice de figuras</b>	<b>XIV</b>
<b>Índice de tablas</b>	<b>XVI</b>
<b>1. Introducción y objetivos</b>	<b>1</b>
1.1. Motivación . . . . .	1
1.2. Biometría . . . . .	2
1.2.1. Etapas en un sistema de reconocimiento biométrico . . . . .	3
1.2.2. Identificación y autenticación . . . . .	4
1.3. Fisiología del corazón . . . . .	5
1.4. ECG como modalidad biométrica . . . . .	6
1.5. Objetivos . . . . .	7
<b>2. Estado del arte</b>	<b>9</b>
2.1. Adquisición de datos . . . . .	9
2.2. Procesamiento de la señal . . . . .	10

2.3. Comparación de patrones . . . . .	10
<b>3. Desarrollo del sistema propuesto</b>	<b>13</b>
3.1. Contexto y planteamiento del problema . . . . .	13
3.2. Base de datos . . . . .	14
3.3. Preprocesado de la señal de ECG . . . . .	16
3.3.1. Filtrado de la señal . . . . .	16
3.3.2. Segmentación de la señal y obtención del vector V . . . . .	18
3.4. Extracción de características . . . . .	21
3.4.1. Arquitectura de la CNN . . . . .	21
3.4.2. Selección de hiperparámetros y entrenamiento de la red . . . . .	24
3.4.3. Comparación de patrones . . . . .	26
<b>4. Evaluación del sistema: resultados experimentales</b>	<b>28</b>
4.1. Identificación . . . . .	28
4.1.1. Primera base de datos . . . . .	28
4.1.2. Segunda base de datos . . . . .	31
4.1.3. Base de datos completa . . . . .	33
4.1.4. Variabilidad intra-clase . . . . .	35
4.2. Autenticación . . . . .	35
<b>5. Conclusiones</b>	<b>43</b>
5.1. Conclusiones . . . . .	43
5.2. Líneas futuras . . . . .	45
<b>A. Anexo I: Calidad de las clasificaciones obtenidas en identificación</b>	<b>I</b>
A.1. Base de datos 1 . . . . .	I
A.2. Base de datos 2 . . . . .	II
A.3. Base de datos completa . . . . .	III
<b>B. Anexo II: Visualización de los vectores de características con la herramienta PCA</b>	<b>IV</b>
<b>C. Anexo III: Aspectos éticos, económicos, sociales y ambientales</b>	<b>v</b>

---



# Índice de figuras

---

1.1.	Bloques en un sistema de reconocimiento biométrico. . . . .	4
1.2.	Esquema General de una señal de ECG. Fuente [1]. . . . .	5
3.1.	Flujo de Trabajo. . . . .	13
3.2.	Examen visual de la variabilidad entre los casos capturados. . . . .	15
3.3.	Resultado de aplicar un filtro paso-banda Butterworth. . . . .	17
3.4.	Espectro en frecuencia de la señal de ECG antes y después de aplicar un filtro paso-banda Butterworth. . . . .	17
3.5.	Detección de QRS con el algoritmo de Pan-Tompkins. . . . .	18
3.6.	Detección de picos R. . . . .	19
3.7.	Proceso de la segmentación de la señal hasta la obtención del vector V. . .	20
3.8.	Ejemplo de un vector V, compuesto por 8 QRS y tiene 1 segundo de duración. El vector V es la entrada de la CNN. . . . .	20
3.9.	Esquema de la arquitectura de la CNN. La capa densamente conectada solo se utiliza para el entrenamiento de la red y para identificación. . . . .	21
3.10.	Resumen del modelo empleado con los tamaños de las salidas de cada capa. .	23
3.11.	Optimización del tamaño de <i>batch</i> y el número de <i>epochs</i> mediante un muestreo de cuadrícula. . . . .	25
3.12.	Evolución del rendimiento y de la pérdida de entrenamiento y de validación durante la fase de entrenamiento de la red. . . . .	26
4.1.	Matriz de confusión obtenida para la base de datos 1. . . . .	29

---

4.2.	Curva CMC obtenida para los datos de prueba de la base de datos 1 . . . . .	30
4.3.	Matriz de confusión obtenida para la base de datos 2. . . . .	31
4.4.	Curva CMC obtenida para la base de datos 2. . . . .	32
4.5.	Matriz de confusión obtenida para los datos de prueba de la base de datos completa. . . . .	33
4.6.	Comparación de las CMC obtenidas para las bases de datos 1 y 2, así como la base de datos al completo. . . . .	34
4.7.	Variación de la tasa de identificación en el rank(1) en función del número de sujetos. . . . .	34
4.8.	Esquema de la división de usuarios y de sus muestras para las distintas fases en cada modelo. . . . .	36
4.9.	Comparativa de la distribución de los vectores de características obtenidos durante la fase de reclutamiento para cada modelo, empleando la herramienta de visualización TSNE para reducir a tres dimensiones el espacio. .	37
4.10.	Esquema de la fase de consulta. . . . .	38
4.11.	Distribución de usuarios genuinos e impostores mediante la distancia euclídea. .	38
4.12.	Curvas FAR y FRR. El EER es el punto de intersección entre ambas curvas. .	39
4.13.	Comparación del EER obtenido en función del porcentaje de usuarios utilizado para el entrenamiento de la red. . . . .	40
4.14.	Variabilidad del resultado de error obtenido en función de las muestras utilizadas. . . . .	41
4.15.	Variación del EER en función del número de muestras. . . . .	41
4.16.	Comparación del rendimiento de los tres modelos con la curva ROC. . . . .	42
A.1.	Calidad de las clasificaciones obtenidas para cada usuario de la base de datos completa. . . . .	III
B.1.	Comparativa de la distribución de los vectores de características obtenidos durante la fase de reclutamiento para cada modelo, empleando la herramienta de visualización PCA para reducir a tres dimensiones el espacio. .	IV

---

# Índice de tablas

---

2.1. Comparativa de estudios existentes basados en redes neuronales para la identificación y autenticación biométrica a través del ECG. . . . .	11
3.1. Comparativa de los resultados del rendimiento de la red durante la fase de prueba para diferentes modelos. . . . .	24
4.1. Calidad de las clasificaciones obtenidas para la base de datos 1. . . . .	30
4.2. Calidad de las clasificaciones obtenidas para la base de datos 2. . . . .	32
4.3. Comparación de los resultados de rendimiento y pérdida obtenidos con variabilidad intra-clase. . . . .	35
5.1. Comparativa de estudios existentes basados en redes neuronales para la identificación y autenticación biométrica a través del ECG. . . . .	44
A.1. Calidad de las clasificaciones obtenidas para cada usuario de la primera base de datos. . . . .	I
A.2. Calidad de las clasificaciones obtenidas para cada usuario de la segunda base de datos. . . . .	II
A.3. Calidad de las clasificaciones obtenidas para la base de datos completa. . .	III
C.1. Presupuesto económico. . . . .	VI



# 1. Introducción y objetivos

---

## 1.1. Motivación

En el mundo en el que vivimos, la mayoría de áreas de nuestras vidas, sufren cada día una creciente digitalización. Todos los días, utilizamos servicios en línea, como aplicaciones de nuestro banco para el móvil o las simples comunicaciones vía mail tan presentes en nuestras rutinas, y no dudamos en mantener nuestra información personal en nuestros dispositivos o en almacenamientos en la nube. Sin embargo, esta era digital también ha allanado el camino a una serie de nuevos ataques, que incluyen el acceso no autorizado a nuestros datos y dispositivos personales.

Es curioso como, en general, los usuarios seguimos necesitando una infinidad de contraseñas, un sistema rudimentario que se lleva utilizando para el control de acceso desde los primeros días de la informática. Es por esto que recientemente se ha producido un cambio de enfoque hacia el campo de la autenticación biométrica, que verifica la identidad del usuario utilizando sus características biológicas.

Una de sus aplicaciones más comunes la vemos en el uso de escáneres de huellas dactilares, como el que poseen muchos smartphones y portátiles. Aunque esto supone un gran avance, todavía quedan problemas sin solucionar relacionados con su usabilidad y fiabilidad.

Siguiendo con este enfoque novedoso, nos encontramos con el uso de señales fisiológicas unidimensionales, como el electrocardiograma (ECG), a modo de características biométricas, que está atrayendo cada vez más la atención de la comunidad científica. Algunas de las principales ventajas que presentan estas señales son:

- Son difíciles de falsificar.
- Están presentes en todos los seres vivos.
- Contienen información sobre el estado clínico o psicológico, que puede ser utilizada para otras aplicaciones.

- Su adquisición por largos periodos de tiempo no requiere una acción explícita del usuario.
- Presentan características típicas para la identificación biométrica.

Además, entre las técnicas de análisis de señales fisiológicas en el ámbito de la Medicina, el ECG destaca por su madurez y difusión, y estudios recientes demuestran que su aplicación para la biometría puede llegar a obtener una precisión muy elevada. No obstante, esta modalidad biométrica tiene que hacer frente a una serie de problemas, que incluyen:

- La alta variabilidad de las muestras causada por el ritmo cardíaco, la realización de actividades y los escenarios en los que han sido tomadas.
- La falta de estudios que demuestren la representatividad entre usuarios con bases de datos a gran escala.
- Los cambios a largo plazo en los rasgos de las personas.
- La protección frente a nuevos ataques.
- La adecuada extracción de características de las señales y el diseño de modelos precisos para el reconocimiento de patrones.

## 1.2. Biometría

El término Biometría, dentro del ámbito de la identificación de personas, hace referencia al reconocimiento de personas basado en las características únicas de cada individuo. Estas características pueden ser fisiológicas, permitiendo identificar a una persona mediante su huella dactilar o sus rasgos faciales por ejemplo, o de comportamiento, como su voz o su forma de caminar.

Esta capacidad de reconocimiento biométrico es innata para los seres vivos, que podemos reconocer a nuestros semejantes. Pero la Biometría como la ciencia que estudia la individualidad de las personas, no nace hasta finales del siglo XIX. A día de hoy, está cada vez más presente en el mundo que nos rodea, y es utilizada en diversas aplicaciones, como sistemas de control de acceso y la autenticación o identificación de usuarios.

La mayoría de los sistemas de control de acceso existentes, requieren el uso de algo que la persona conoce (p. ej una contraseña) o que tiene (p. ej tokens de seguridad). Sin embargo, mediante la Biometría, esto se puede sustituir por algo que la persona *es*, es decir, sus rasgos, permitiendo así mejorar la usabilidad del sistema, puesto que los usuarios ya no necesitan recordar claves secretas o llevar algo consigo. Además, estas nuevas modalidades no tienen por qué sustituir a las tradicionales, y ambas se pueden combinar, incrementando la seguridad todavía más y actuando como mecanismos de detección de ataques [1].

A la hora de juzgar si un sistema biométrico es válido o no, hay muchos parámetros a tener en cuenta. Algunos de ellos son:

- Universalidad: las características están presentes y se pueden extraer de cualquier persona.
-

- Unicidad: las características son suficientemente diferentes de persona a persona.
- Estabilidad: las características se mantienen invariantes a lo largo de la vida de la persona, independientemente del tiempo, la edad, posibles enfermedades, etc.
- Facilidad de captura: las características pueden ser extraídas del sujeto de manera sencilla.
- Rendimiento: el sistema es fiable y fácil de analizar cuando se utiliza para la identificación personal.
- Aceptación: la recolección y el uso de datos es socialmente aceptable.
- Robustez frente a ataques: las características biométricas no son fácilmente imitables y suplantables por otro individuo.
- Coste.

Por tanto, la modalidad óptima para el reconocimiento biométrico depende de cada situación y entorno, con diferentes requisitos de seguridad, y no se puede afirmar que exista una única técnica, perfecta e ideal, que se pueda utilizar siempre.

Algunas de las modalidades biométricas ya cuentan con una implantación muy elevada. Por ejemplo, el uso de la huella dactilar en los móviles o el reconocimiento facial en controles automáticos de fronteras, son, sin duda, aplicaciones muy conocidas. Sin embargo, cualquier otra característica biológica o de comportamiento de la persona puede ser usada para realizar su reconocimiento, siempre que sea propia y única de ella. Entre las más conocidas podemos citar las siguientes: iris, voz, andadura, dinámica de teclado, ADN, firma manuscrita, etc.

Si bien la Biometría ofrece muchas ventajas sobre las técnicas tradicionales de control de acceso, todavía existen serias preocupaciones sobre la seguridad y la privacidad de esta modalidad, al emplear características visibles externamente del individuo, que son susceptibles de ser copiadas o falsificadas. Por ejemplo, los rasgos faciales de una persona pueden ser fácilmente obtenidos de sus fotos en redes sociales, permitiendo este hecho un ataque que daría acceso ilegítimo del atacante a la información y servicios de la persona en cuestión. Es por ello, que se busca el uso de características no visibles, internas, que sean difíciles de copiar. Además, esto permite al sistema tener una "*fe de vida*" del usuario, es decir, detectar que el usuario en cuestión está vivo.

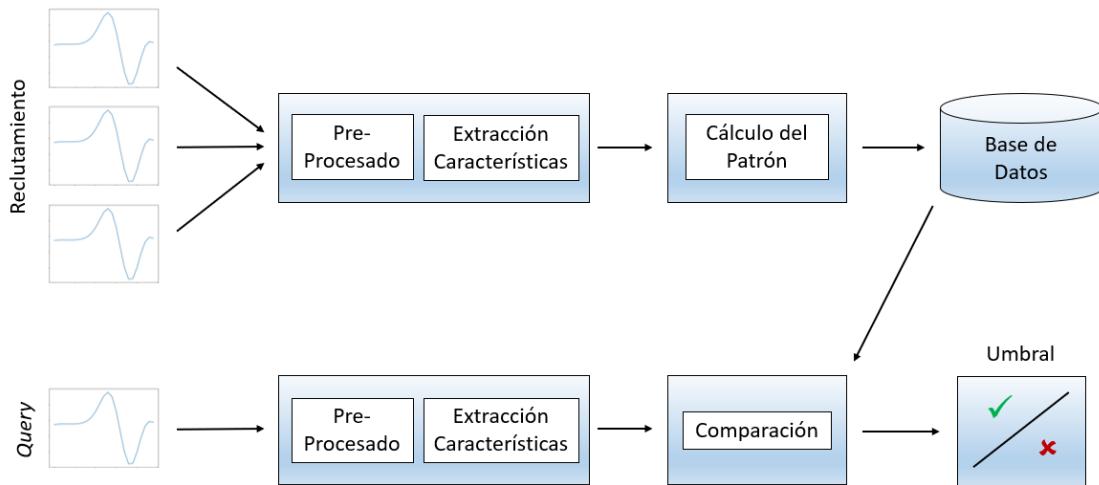
### **1.2.1. Etapas en un sistema de reconocimiento biométrico**

Como ya hemos visto, existen multitud de técnicas de reconocimiento biométrico, basadas en las diferentes características de las personas. A pesar de esta diversidad, podemos establecer un esquema común a todas ellas a la hora de implementar un sistema de identificación biométrica. Así, nos encontramos con dos fases totalmente diferenciadas, e independientes de la técnica empleada, como podemos ver en la Figura 1.1:

- La primera fase es la de reclutamiento o registro. En esta fase, se toman muestras del usuario y se procesan, de forma que se obtiene un patrón de este usuario, que le caracteriza, y este patrón se almacena. Generalmente, se toman varias muestras
-

durante el proceso, para poder extraer más características del usuario, analizar la repetitividad de las muestras, enseñar al usuario a usar el sistema... y suele ser un proceso supervisado, es decir, hay una persona encargada de la toma de datos y de asegurar la identidad del sujeto.

- La segunda fase es la de consulta o *query*. En esta fase, cada vez que se requiere reconocer a un usuario o verificar su identidad, se toma una nueva muestra y se compara con su referencia almacenada. En el caso de verificación del usuario, resultado de la comparación se establece en base a un umbral.



**Figura 1.1.** Bloques en un sistema de reconocimiento biométrico.

En cuanto a la elección del umbral en el caso de autenticación, es interesante destacar que si éste aumenta, el sistema se relaja, permitiendo una mayor probabilidad de accesos de personas no autorizadas (Tasa de Falsa Aceptación, o FAR), mientras que si disminuye, el sistema se vuelve más restrictivo, de manera que aumenta la probabilidad de rechazo para personas autorizadas (Tasa de Falso Rechazo, o FRR). Por tanto, su elección dependerá del grado de seguridad que requiera cada sistema.

Además, como se ve en la Figura 1.1, cada una de estas fases está compuesta por diferentes bloques, que permiten caracterizar a la persona a partir de sus rasgos biológicos o de comportamiento. Estas fases son: captura de los datos, pre-procesado de los mismos para facilitar su tratamiento, extracción de características (bloque en el que se fundamenta la capacidad del sistema de distinguir entre sujetos) y comparación de las características con las previamente almacenadas. Esta comparación puede estar basada en las distintas técnicas de reconocimiento de patrones, como por ejemplo, técnicas basadas en modelado de problemas, como las redes neuronales.

### 1.2.2. Identificación y autenticación

Hasta el momento se ha hecho referencia al reconocimiento biométrico como algo genérico. Sin embargo, cabe diferenciar entre identificación y autenticación.

- Identificación: consiste en determinar la identidad de un usuario registrado en el sistema. Para ello, se comparan las características extraídas con los patrones de todos

los usuarios. El principal inconveniente de esta funcionalidad es la necesidad de una base de datos para los patrones, lo que implica una capacidad de almacenamiento elevada y una seguridad apropiada en la custodia de los datos. Como posibles aplicaciones podemos encontrar la identificación de delincuentes a partir de imágenes de videovigilancia o el reconocimiento forense.

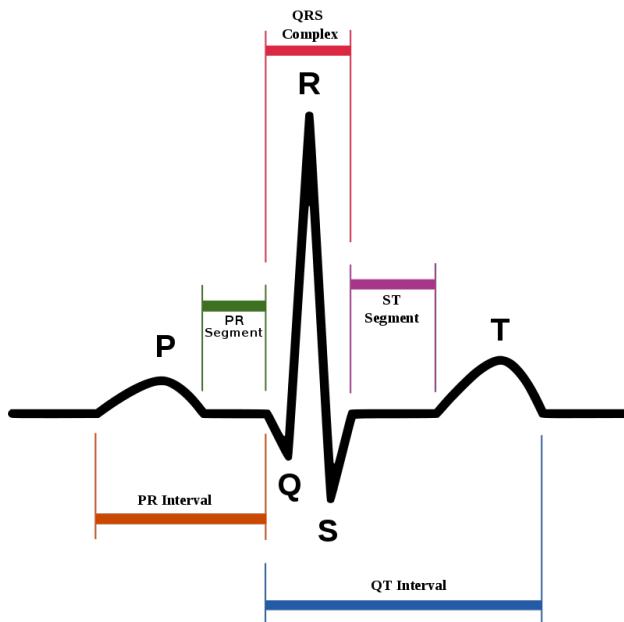
- Autenticación o verificación: consiste en determinar si el usuario es realmente quien dice ser. Para ello, además de las características del usuario, éste tiene que comunicar su identidad. El sistema compara estas características con el patrón del usuario indicado, que puede estar almacenado en una base de datos o en un sistema portátil de información, y decide si la petición es válida o no. Por ejemplo, presentar el pasaporte en una frontera es una aplicación de autenticación de usuarios.

En este trabajo se va a diseñar tanto un sistema para la identificación biométrica como uno para la autenticación.

### 1.3. Fisiología del corazón

Antes de analizar la utilidad del electrocardiograma como modalidad biométrica, esta sección presenta un resumen de la fisiología del corazón.

El corazón es el músculo que bombea la sangre en nuestro cuerpo y para ello, se contrae gracias a impulsos eléctricos. Estos impulsos eléctricos pueden ser detectados en la superficie del cuerpo mediante el uso de electrodos. Así, el ECG es la representación gráfica de la actividad eléctrica del corazón, como una señal en función del tiempo, dando como resultado una curva que representa cada ciclo cardíaco y que de forma teórica se puede ver en la Figura 1.2. Habitualmente, en electrocardiografía se utilizan 12 derivaciones para su obtención.



**Figura 1.2.** Esquema General de una señal de ECG. Fuente [1].

---

Como se puede comprobar, dicha señal se compone de varias partes diferenciadas, que corresponden a la despolarización y repolarización de las cámaras del corazón, provocando la contracción y relajación de las mismas. Las distintas fases del funcionamiento del corazón son:

- Onda P: representa la despolarización de las aurículas.
- Segmento PR: es el tiempo entre la despolarización de la aurícula y el inicio de la despolarización de los ventrículos.
- Complejo QRS: representa la despolarización de los ventrículos. Es la parte más característica de la señal del ECG.
- Segmento ST: corresponde al tiempo antes de que los ventrículos se vuelvan a polarizar.
- Onda T: representa la repolarización ventricular.

Cada uno de estos componentes podría variar tanto en amplitud como en duración, atendiendo a la derivación que se está tomando, el ritmo cardíaco, el estado de estrés, la posición del cuerpo, etc. Evidentemente también varían cuando el usuario sufre alguna patología cardíaca, tal como arritmias, reflujo ventricular, etc. Todas estas variaciones, además de las propias del sujeto, hacen que utilizar esta información como modalidad biométrica, resulte un reto considerable [2].

#### 1.4. ECG como modalidad biométrica

Tras analizar brevemente la fisiología del corazón, en esta sección pasamos a considerar si el ECG podría ser un elemento biométrico viable.

Como ya se ha mencionado en la sección 1.2, para que un sistema biométrico sea válido debe ser universal, único y estable, entre otros aspectos.

En cuanto a la universalidad, es evidente que se cumple en el caso del ECG, pues la actividad eléctrica del corazón está presente en todos los seres vivos, siendo la falta de esta actividad incompatible con la vida.

Por otro lado, la validación de la unicidad del ECG para su uso como método biométrico no es tan fácil de demostrar, debido principalmente a la falta de datos y de estudios que lo prueben. La mayoría de los trabajos que exploran el uso ECG para la identificación de personas no evalúan el rendimiento del sistema para grandes bases de datos, como se ha hecho en otras modalidades biométricas.

Una excepción notable es un estudio de Carreiras *et al.* [3], que se centra en la unicidad de las señales de ECG. Los autores de este artículo científico evaluaron el rendimiento de su sistema biométrico con una base de datos de registros de ECG recogidos de 618 sujetos y obtuvieron altas tasas de reconocimiento.

Autores como Sufi *et al.*[4] afirman la unicidad de la composición, el mecanismo y la actividad eléctrica del corazón humano basándose en el dogma central de la Biología

---

molecular, que establece que la información fluye desde el ADN al ARN y de este a las proteínas.

En el caso de la estabilidad del ECG nos encontramos con todavía menos estudios que la investiguen. Si bien, es posible demostrar la unicidad utilizando datos registrados en un único momento temporal, para demostrar la estabilidad es necesario reunir datos del mismo individuo durante un período de tiempo lo suficientemente largo. La creación de estas grandes bases de datos, para estos estudios longitudinales, es costosa e implica una importante inversión de tiempo, lo que explica el reducido número de estudios que examinan la estabilidad del ECG.

En un estudio de Silva *et al.* [5] se recogieron datos de ECG de 63 sujetos, con dos sesiones de adquisición de datos separadas por un intervalo de 4 meses. Sus resultados indican que aunque la autenticación biométrica funciona peor para los datos de ECG longitudinales, siguen siendo viables para aplicaciones en el mundo real.

En resumen, el ECG sigue siendo un fuerte candidato a ser usado para el reconocimiento biométrico. Varios estudios han demostrado la unicidad y la estabilidad del ECG, aunque a pequeña escala. Además, la aparición de sensores de ECG de bajo costo proporcionaría una buena oportunidad para que estos fueran incorporados en los sistemas de control de acceso existentes. En contraposición, todavía no hay suficiente investigación sobre la extracción de características de las señales del ECG, que permitan prevenir los ataques de falsificación y garantizar que los sistemas biométricos basados en ECG sean aceptados por el público en general [1].

## 1.5. Objetivos

El objetivo principal de este trabajo consiste en el diseño, desarrollo y evaluación de un novedoso sistema de reconocimiento biométrico a través del ECG basado en *Deep Learning*. Con este sistema se consigue un avance en el uso de esta modalidad biométrica interna de las personas, característica que no solo hace que sea difícil de copiar, sino que también sirve como indicador de vida en la detección de ataques.

Como se puede ver en el siguiente capítulo (2), esta modalidad cuenta todavía con muy pocos estudios concluyentes, situándola en un estado muy preliminar. Por ello, este estudio pretende contribuir a la superación de algunas de las limitaciones de las investigaciones existentes, relacionadas con el uso de esta señal, para el reconocimiento biométrico.

Para ello, hemos diseñado y desarrollado un sistema basado en el uso de una red neuronal convolucional, con la que se puede llevar a cabo una extracción de características que permite la identificación de un conjunto cerrado (*closed set*) y la autenticación de usuarios. Además, la evaluación de este sistema se ha realizado con señales de ECG registradas en varias sesiones, incluyendo tomas después de que el sujeto haya realizado ejercicio, probando que el ECG puede utilizarse característica biométrica.

El desarrollo de este proyecto se ha basado en los algoritmos propuestos por Labati *et al.* en el artículo científico *Deep ECG: Convolutional Neural Networks for ECG biometric recognition* [6].

En el capítulo 2 de este estudio, se revisan las contribuciones más importantes en el ámbito del reconocimiento biométrico basado en el ECG existentes hasta el momento.

---

Posteriormente, en el capítulo 3 se realiza una descripción detallada del desarrollo del sistema propuesto, empezando por una contextualización del problema y una descripción de la base de datos utilizada, y describiendo a continuación, en profundidad, los procesos de preprocesado de la señal y de extracción de características que se han llevado a cabo. En el capítulo 4 se expone una extensa evaluación del sistema, tanto para la identificación de usuarios como para la verificación de la identidad. Y finalmente, este proyecto concluye en el capítulo 5, donde además se presentan posibles líneas futuras de trabajo.

## 2. Estado del arte

---

Si bien el uso del ECG como modalidad biométrica no es una idea nueva, siendo pioneros en esta técnica trabajos como el de Biel *et al.* [7] y el de Kyoso *et al.* [8] (2001), esta modalidad todavía se encuentra en un estado muy inmaduro, no tanto debido al número de estudios existentes, sino a la falta casi absoluta de consenso en las metodologías apropiadas para su aplicación.

Odinaka *et al.* presenta en [9] una extensa y detallada comparativa del estado de la técnica hasta el año 2012. En este capítulo se ofrece una breve descripción de la literatura científica de los últimos años sobre esta modalidad.

A la hora de diseñar un sistema biométrico basado en el ECG, hay que tener muy en cuenta una serie de aspectos que van a influir notablemente en su rendimiento. Por esta razón, el estado de la técnica puede diferenciarse en función de cómo se han llevado a cabo las etapas de adquisición de datos, procesamiento de la señal y comparación de características.

### 2.1. Adquisición de datos

La mayoría de técnicas actuales utilizan bases de datos ya existentes y solo unas pocas investigan la estabilidad y usabilidad del ECG como método biométrico.

Si nos fijamos en la posición de los electrodos, mientras que la mayoría de estudios utilizan bases de datos capturadas con electrodos localizados directamente en el cuerpo de la persona [3, 10, 11, 12], en biometría basada en ECG un escenario más realista es aquél en el que la adquisición se realiza con sensores de ECG móviles. Por ejemplo, Falconi *et al.* [13] incluyó sensores en fundas de smartphones y Silva *et al.* [5] en reposamuñecas de ordenador.

Por otro lado, si nos atenemos al tipo de autenticación requerida por el sistema, ésta suele ser una verificación única en un instante dado, es decir, en el momento en el que se realiza la petición del recurso (para acceder a un edificio o a un servicio bancario, por ejemplo). Sin embargo, también puede resultar interesante una autenticación continua, en

la que la identidad del usuario se verifica en todo momento mientras el recurso esté en uso (conduciendo un coche, por ejemplo) [6, 14, 15].

Otro factor a tener en cuenta a la hora de la adquisición de las muestras de ECG, es el periodo de tiempo en las que éstas han sido registradas. Así, la estabilidad de los estudios basados en registros tomados en una única sesión, no pueden considerarse como concluyente. Samarin *et al.* [1] aborda esta limitación, teniendo como componente central la confección de una base de datos de ECG propia para la autenticación de usuarios, con dos sesiones diferentes para la toma de datos. Reíllo *et al.* [2] también basa su trabajo sobre una base de datos propia, con una representatividad aceptable tanto para la autenticación intra-clase, como para la inter-clase, registrando muestras en dos días diferentes de 105 usuarios.

Por último, la mayoría de bases de datos ya existentes tienen un propósito médico, y no de reconocimiento de usuarios. Esto supone una gran limitación a la hora de usarlas para identificación de personas, pues no son representativas para una realidad en la que la mayoría de usuarios del sistema biométrico no tendrían afecciones cardíacas.

## 2.2. Procesamiento de la señal

La elección de características utilizadas para el procesamiento de la señal de ECG también deja clara una falta absoluta de línea directriz común en las investigaciones existentes.

El procesamiento de la señal puede estar basado en el uso de características locales (fiduciales), parcialmente fiduciales o características globales (no-fiduciales).

Los métodos fiduciales son aquellos que se basan en obtener, para cada ciclo cardíaco, los puntos característicos (por ejemplo, máximo de la onda P, puntos Q, R, S, etc), y obtener de ellos los vectores de características (que constituyen los *templates* o patrones). Estos métodos se han utilizado con éxito en varios estudios [11, 12, 13], pero requieren algoritmos específicos para localizar los puntos de referencia de la señal.

Los métodos parcialmente fiduciales localizan sólo los picos R (en el complejo QRS), y a partir de ellos se segmentan los ciclos cardíacos de la señal. Tras el preprocesado, estos segmentos son adoptados por el sistema biométrico como patrones [3, 5, 6].

Por último, los métodos basados en las características globales utilizan mecanismos de procesado tales como la transformada discreta del coseno (DCT), wavelets, redes neuronales, etc. En casi todos estos casos, se parte de la premisa de que un ciclo cardíaco va a ser prácticamente igual al anterior y al siguiente y no es necesario extraer puntos de referencia de la señal [14, 15].

## 2.3. Comparación de patrones

*Template matching*, o comparación de patrones, hace referencia al proceso de verificación de la consulta biométrica con respecto a los patrones almacenados. Igual que pasa con el procesado, para la comparación de patrones tampoco se puede ver una trayectoria única a la hora de determinar qué algoritmos se deben utilizar.

---

En [2] se presenta una detallada comparación de las diferentes técnicas utilizadas, así como de los resultados obtenidos.

En este trabajo, resulta de especial interés la aplicación del *Deep Learning*, y en concreto, el uso de redes neuronales convolucionales. La literatura existente presenta numerosos estudios basados en este tipo de aprendizaje aplicado a la Biometría, especialmente en reconocimiento facial y de iris, e incluso con señales unidimensionales como es el caso del reconocimiento por voz. Sin embargo, la aplicación de las CNNs a la señal del ECG es considerada por muy pocos estudios hasta la fecha, y la mayoría se centran en la clasificación de arritmias y no en aplicaciones biométricas [16, 17].

Así, el uso de CNNs para el reconocimiento biométrico basado en ECG es muy novedoso y cuenta con muy pocos estudios llevados a cabo hasta el momento.

En 2017, Song-Kyoo *et al.* presentó un posible marco de trabajo para la aplicación de las CNNs en la autenticación biométrica con ECG en [18].

También en 2017, Zhang *et al.* presentó en [19] un algoritmo basado en CNNs para identificar usuarios, utilizando segmentos aleatorios de sus señales ECG sin una gran ingeniería de extracción de características y consiguiendo una independencia respecto a los datos utilizados con una gran capacidad de generalización. Además, unos meses después, propuso en [20] un novedoso sistema de ECG corporal, con electrodos colocados en el brazo o detrás de las orejas, para identificar individuos utilizando estos registros débiles de los latidos del corazón gracias a la aplicación de una red neuronal convolucional, obteniendo resultados prometedores para las “aplicaciones de salud inteligentes” (del inglés *smart health applications*).

*Deep-ECG: Convolutional Neural Networks for ECG biometric recognition* [6], publicado en 2019 y utilizado como estudio de referencia en este trabajo, utiliza las CNNs para extraer características de usuarios durante la fase de entrenamiento de la red y a continuación realiza una fase de identificación *closed set*, y otra de verificación de la identidad y re-autenticación periódica, con usuarios diferentes a los utilizados para entrenar la red.

Y finalmente, también en 2019, Pinto *et al.* presentó otras dos aplicaciones de las CNNs para el reconocimiento biométrico basado en ECG en [21] y [22]. Ambos estudios presentan novedosos métodos que permiten llevar a cabo tanto la identificación como la autenticación de usuarios sin la necesidad de preprocesar las señales ECG, obteniendo resultados muy prometedores para ambas modalidades tras una evaluación de los métodos propuestos sobre varias bases de datos.

La siguiente Tabla 2.1 muestra una comparativa de los resultados obtenidos en estos últimos trabajos citados.

Autor	Usuarios	Preprocesado	Método	Tasa de Identificación	EER de autenticación
Labati <i>et al.</i> [6]	52	Parcialmente-local	CNN	100 %	1,05
Zhang <i>et al.</i> [19]	18 a 47	Sin preprocesar	CNN	93,5 %	-
Zhang <i>et al.</i> [20]	18 a 47	Parcialmente-local	CNN	95 %	-
Pinto <i>et al.</i> [21]	1019	Sin preprocesar	CNN	-	7,86 %
Pinto <i>et al.</i> [22]	1019	Sin preprocesar	CNN	96,1 %	-
Salloum <i>et al.</i> [23]	47	Parcialmente-local	RNN	100 %	0 %

**Tabla 2.1.** Comparativa de estudios existentes basados en redes neuronales para la identificación y autenticación biométrica a través del ECG.

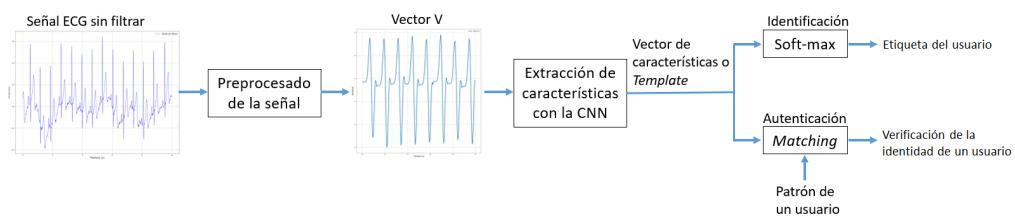
Como conclusión, es muy difícil poder comparar los resultados obtenidos en los diversos trabajos previos debido a la falta de consenso casi absoluta existente en esta técnica biométrica, llegándonos incluso a encontrar discrepancias sobre qué métricas usar a la hora de evaluar los sistemas diseñados. Por tanto, el ECG como modalidad biométrica es una técnica novedosa muy prometedora, pero hasta el momento en un estado muy preliminar.

### 3. Desarrollo del sistema propuesto

#### 3.1. Contexto y planteamiento del problema

Como ya se ha comentado, este trabajo implementa y evalúa un sistema de reconocimiento biométrico a través del ECG basado en redes neuronales convolucionales (CNN), con el que se puede realizar tanto la modalidad de identificación de usuarios como la de autenticación. Para ello, el desarrollo se ha basado en los algoritmos propuestos en el artículo científico *Deep-ECG: Convolutional Neural Networks for ECG biometric recognition* [6].

Para ambas modalidades, el novedoso enfoque presentado en [6] que se ha utilizado en este estudio consiste en extraer un conjunto de  $m$  complejos QRS de registros de ECG de corta duración y concatenarlos, obteniendo una nueva señal  $\mathbf{V}$ . En la identificación *closed set*, una CNN procesa  $\mathbf{V}$  e indica quién es el usuario registrado más cercano. En la verificación de la identidad, la CNN procesa  $\mathbf{V}$  para obtener un patrón biométrico  $\mathbf{T}$  y, mediante la técnica de comparación de patrones (o *template matching*), da una respuesta a la autenticación en base a la medida de la distancia euclídea.



**Figura 3.1.** Flujo de Trabajo.

El flujo de trabajo está dividido en las siguientes etapas (Figura 3.1):

- Preprocesamiento de la señal.
- Extracción de características con la CNN.
- Reconocimiento biométrico.
  1. Identificación basada en *Soft-max*.
  2. Autenticación basada en comparación de patrones.

Además, con este estudio se ha querido analizar la estabilidad del ECG como característica biométrica, utilizando registros de la señal obtenidos en dos sesiones diferentes y utilizando experimentos diferentes según la toma de datos.

Todo el desarrollo de este proyecto ha sido implementado con el lenguaje de programación Python [24], que es el lenguaje más utilizado hoy en día para construir y entrenar redes neuronales y, en particular, redes neuronales convolucionales. La sintaxis de Python se caracteriza por su sencillez, que hace que sea fácil de usar y rápido de aprender. Además, este lenguaje tiene licencia de código abierto y cuenta con una amplia cantidad de bibliotecas disponibles para el *Deep Learning*, incluyendo NumPy [25], scikit-learn [26], así como con todas las plataformas más populares y poderosas de este campo. Una de ellas es Keras [27], que se ha utilizado en este proyecto para la implementación de todas las CNNs. Keras es una biblioteca de *Deep Learning* de alto nivel, que se ejecuta típicamente sobre TensorFlow [28]. Esta biblioteca permite una rápida experimentación y se caracteriza por su modularidad y extensibilidad, que permiten combinar y añadir capas neuronales, funciones de activación, hiperparámetros y otros elementos con facilidad.

### 3.2. Base de datos

Como se ha podido ver en el capítulo 2, no existe un consenso sobre qué requisitos deben cumplir las bases de datos utilizadas para el diseño de sistemas biométricos basados en ECG, haciendo muy difícil una posible comparativa entre métodos. Las técnicas de adquisición de datos utilizadas actualmente varían en parámetros tan importantes como la configuración de los electrodos, el tiempo de adquisición, el número de sujetos o el número de sesiones, entre muchos otros. Además, existen diferencias entre si la autenticación es continua o si la verificación de la identidad del usuario es requerida para un instante dado.

Afortunadamente, para la realización de este trabajo se ha podido contar con una base de datos ya existente y diseñada especialmente para aplicaciones de identificación y autenticación.

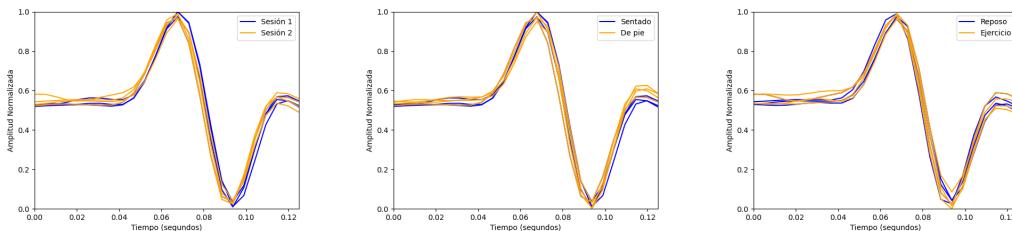
La captura de las muestras se llevó a cabo utilizando BioPac MP100, un equipo comercial de ECG, y los usuarios participantes fueron 105 personas sanas, con edades comprendidas entre los 19 y los 60 años, siendo 54 mujeres y 51 hombres.

Esta base de datos, a su vez puede ser dividida en dos, según el tipo de experimento realizado para la toma de los datos. Así, la captura de los mismos se rige de la siguiente manera:

---

- Para obtener variabilidad intra-clase, se llevaron a cabo 2 sesiones de captura por cada usuario, separadas entre sí un mínimo de una semana.
- Para la **primera base de datos, constituida por los 50 primeros sujetos**, ambas sesiones son iguales:
  - En la primera toma, el usuario se encuentra sentado, en actitud relajada y con los ojos abiertos.
  - En la segunda toma, el usuario se encuentra también sentado y en actitud relajada, pero esta vez con los ojos cerrados.
- Para la **segunda base de datos, constituida por los siguientes 55 sujetos**, las sesiones varían:
  - Para la primera sesión:
    - La primera toma es igual que para la primera base de datos.
    - En la segunda toma, el usuario se encuentra de pie, con los ojos abiertos y en actitud relajada.
  - Para la segunda sesión:
    - La primera toma se mantiene.
    - En la segunda toma, el usuario está sentado, y se realiza después de haberse ejercitado en un *stepper* durante 5 minutos hasta llegar a los 130 latidos por minuto.
- Cada toma de datos se repitió 5 veces y cada una tiene una duración de 60 segundos. Cada usuario tiene 20 tomas.
- La señal ECG fue capturada en las muñecas de los usuarios.
- La frecuencia de muestreo se fijó a 1 KHz.
- Además, como la base de datos completa la forman 105 usuarios, se consiguió una representatividad aceptable de la distribución inter-clase.

La Figura 3.2 muestra visualmente las posibles diferencias que existen, para un mismo usuario, entre las dos sesiones de captura, entre estar sentado y de pie, y entre estar en reposo o después de hacer ejercicio.



**Figura 3.2.** Examen visual de la variabilidad entre los casos capturados.

Como se puede ver, no existe una gran variabilidad entre la primera sesión y la segunda sesión. Sí que se aprecia una pequeña variación (especialmente en la onda T) entre estar

sentado y estar de pie. La variación es algo más significativa entre las muestras obtenidas tras haber hecho ejercicio.

### 3.3. Preprocesado de la señal de ECG

En esta sección se describe la etapa de preprocesado de las señales del ECG, que tiene como objetivo mejorar su calidad y extraer de ellas los complejos QRS más discriminantes. Para ello, nos hemos basado en los algoritmos presentados en el artículo de referencia [6].

#### 3.3.1. Filtrado de la señal

Antes de llevar a cabo el filtrado de las señales, para obtener las muestras biométricas que se van a emplear en el entrenamiento y en la evaluación del sistema, la frecuencia de muestreo de cada toma se ha reducido de 1000 Hz a 200 Hz. Además, cada señal de 60 segundos se ha dividido en intervalos de 10 segundos, periodo que se utiliza típicamente para el análisis médico [6]. Por tanto, para cada usuario ahora hay 120 tomas registradas.

Realizar un filtrado adecuado para las señales del ECG requiere tener en cuenta las componentes de ruido que puedan estar presentes, y las componentes de frecuencia de las diferentes ondas que describe el corazón (descritas en la sección 1.3), especialmente del complejo QRS.

Típicamente, el electrocardiograma tiene dos fuentes de ruido principales [18, 29, 30]:

- Variaciones de baja frecuencia de la línea base (o en inglés *Baseline Wander*) causadas por el uso de electrodos inapropiados, movimientos del sujeto y la propia respiración. Esto genera un "desplazamiento" de la línea base arriba y abajo que se encuentran en el rango de 0,5 Hz, aunque un mayor movimiento del sujeto al realizar ejercicio o pruebas de estrés pueden aumentar su frecuencia. Para eliminar esta fuente de ruido, bastaría con aplicar un filtro de respuesta finita al impulso (*FIR*) de paso alto con una frecuencia de corte de 0,5 Hz.
- Interferencias de red, presentes en cualquier señal bio-eléctrica registrada desde la superficie del cuerpo de una persona. Este ruido se caracteriza por ser una interferencia sinusoidal de 50-60 Hz, posiblemente acompañada de una serie de armónicos. Para eliminarlo, puede utilizarse un filtro notch de respuesta infinita al impulso (*IIR*).

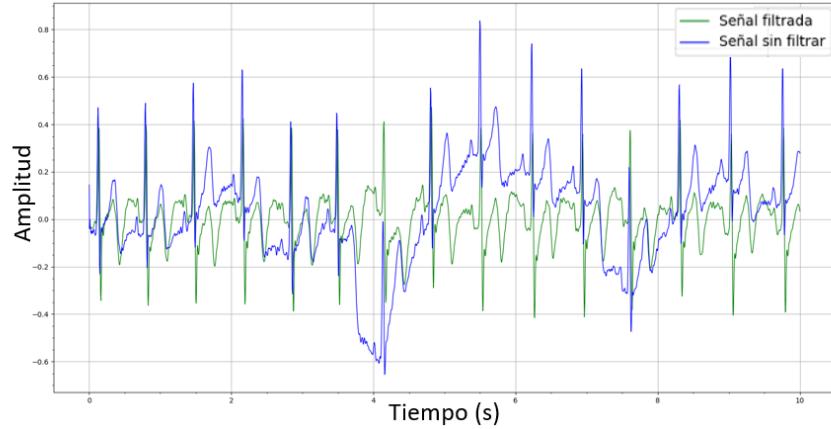
Teniendo esto en cuenta, para reducir el ruido global de la señal del ECG, también podría utilizarse un filtro paso-banda, como puede ser el filtro paso banda de *Butterworth*, que se caracteriza por una respuesta muy uniforme a las frecuencias dentro de la banda de paso [1, 2, 22].

Respecto a qué componentes de frecuencia son más útiles para analizar las diferentes ondas presentes en el ECG, no existe un consenso absoluto, y diferentes investigadores muestran distintas respuestas, considerándose incluso que el ancho de banda útil para analizar el complejo QRS varía en función de la persona e incluso en función del tiempo para una misma persona [31, 32, 33].

Con el fin de mejorar la calidad de las señales de nuestra base de datos, se han probado los diferentes filtros citados, experimentando con diferentes frecuencias de corte

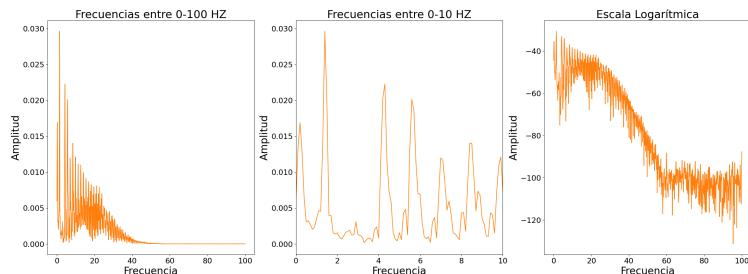
---

y con distintos valores de orden, y finalmente se ha utilizado un filtro *Butterworth* paso banda entre 1 y 35 Hz de orden 5. El resultado de aplicar este filtro sobre la señal sin procesar se puede ver en la Figura 3.3

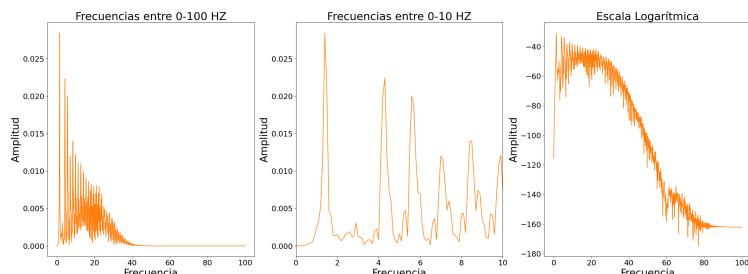


**Figura 3.3.** Resultado de aplicar un filtro paso-banda Butterworth.

Además, la Figura 3.4, muestra el espectro en frecuencia de la señal de ECG antes y después de aplicar el filtro, donde se puede apreciar claramente como se ha eliminado el ruido de baja frecuencia correspondiente a la *Baseline Wander*. El ruido debido a las interferencias de red, sin embargo, solo es apreciable en la escala logarítmica.



**(a)** Espectro en frecuencia de la señal sin filtrar.



**(b)** Espectro en frecuencia de la señal filtrada.

**Figura 3.4.** Espectro en frecuencia de la señal de ECG antes y después de aplicar un filtro paso-banda Butterworth.

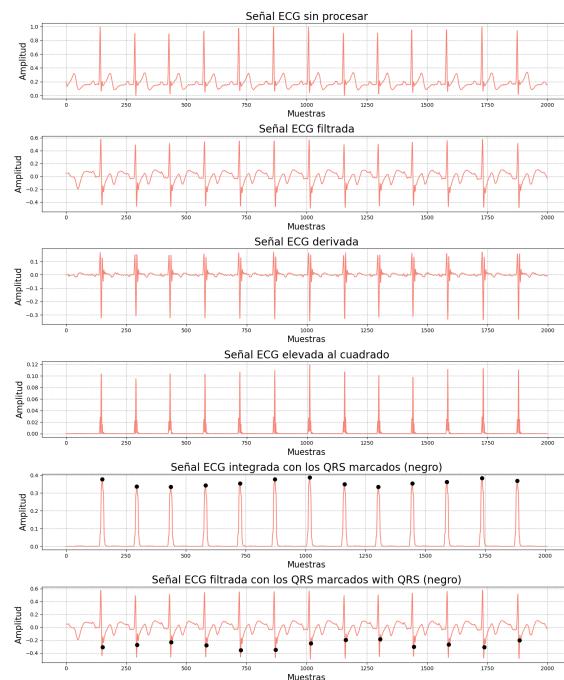
También se realizó un filtrado mucho más agresivo sobre la señal, con un filtro *Butterworth* paso banda entre 5 y 20 Hz, como se utilizó en el estudio realizado por Carreiras *et al.* [3]. Si bien este filtrado permitía mejorar la precisión en la detección de picos R, los resultados obtenidos para la identificación de personas fueron notablemente peores (84 % frente a 97 %). Esto demuestra que la selección de un filtrado adecuado influye de forma significativa en el funcionamiento de la red, y que si se eliminan demasiadas componentes de frecuencia del complejo QRS, la red no es capaz de distinguir entre los diferentes sujetos con tanta precisión.

### 3.3.2. Segmentación de la señal y obtención del vector V

El siguiente paso, una vez mejorada la calidad de la señal de ECG, es la extracción de los complejos QRS. El uso de este complejo para propósitos biométricos puede ser muy beneficioso, al ser la parte del ECG menos sensible a las variaciones debidas al esfuerzo físico o al estado emocional de la persona. Así, el QRS puede utilizarse para extraer los rasgos que componen los patrones biométricos de cada individuo.

Como se ha explicado anteriormente (capítulo 2), los sistemas biométricos basados en el ECG se pueden clasificar en función de si su procesamiento se basa en el uso de características locales (o sea, fiduciales) o características globales (no-fiduciales). En este caso, el enfoque es parcialmente-fiducial, es decir, mediante la localización de los picos R se extraen las características de las ondas de los latidos del corazón, concretamente del complejo QRS.

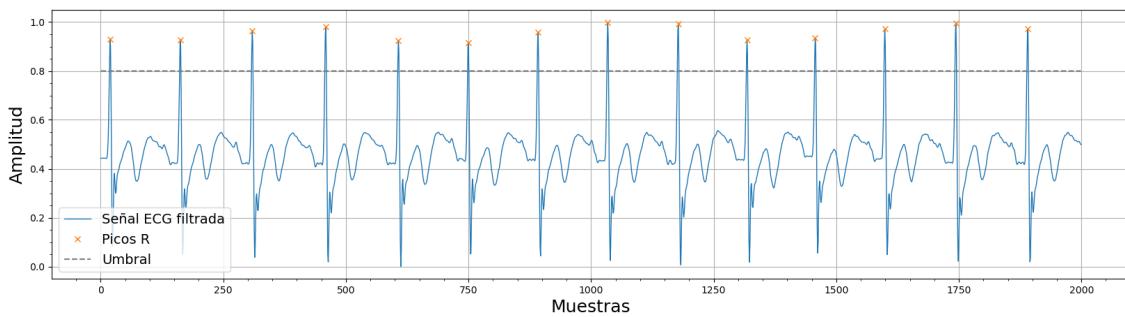
Por tanto, el primer paso es la detección del pico R de cada latido. La búsqueda de este punto es generalmente más sencilla que la búsqueda de otros puntos de referencia, porque es el pico más alto y más agudo en un latido.



**Figura 3.5.** Detección de QRS con el algoritmo de Pan-Tompkins.

En un inicio, se utilizó una implementación del algoritmo de Pan-Tompkins para la detección de los complejos QRS [34]. Este algoritmo se basa en la derivación, la elevación al cuadrado y la integración de la señal, para la detección de picos basada en umbrales adaptativos, como se puede ver en la Figura 3.5.

Sin embargo, para detectar los picos R con mayor precisión, se ha utilizado una herramienta de detección de picos de *SciPy.org* [35], definiendo un umbral sobre las señales normalizadas y fijando una distancia mínima entre picos, que se corresponde con el intervalo R-R, y que varía en función de si la persona ha hecho ejercicio o no. Este valor se ha establecido de manera fija pero, habiendo obtenido previamente el número de complejos QRS mediante el algoritmo de Pan-Tompkins, se podría hacer dinámico en función del número de latidos, mejorando así la detección.



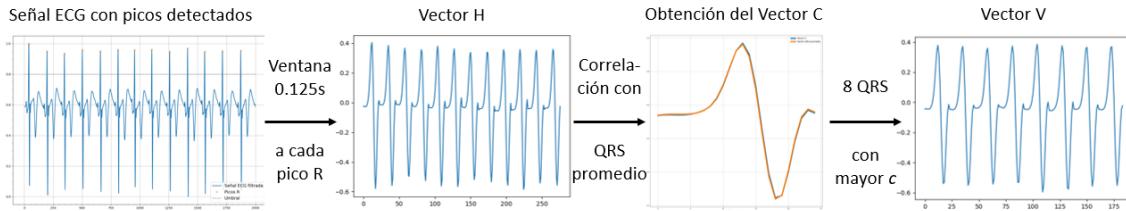
**Figura 3.6.** Detección de picos R.

Esta tarea ha sido especialmente complicada, pues en muchas de las señales la presencia de ruido aún después del filtrado o la propia morfología de la señal de ciertas personas, hace que el pico R no siempre sea fácil de distinguir, confundiéndose en muchas ocasiones con la onda T. Una posible mejora es la aplicación de un umbral dinámico basado en la media móvil de la señal. Por otro lado, como medida preventiva, aquellas señales en las que no se ha detectado un mínimo de 3 picos R han sido descartadas, considerando que la detección no se ha realizado correctamente.

Una vez localizados los picos R, se ha llevado a cabo la segmentación de la señal en los diferentes complejos QRS. Para ello:

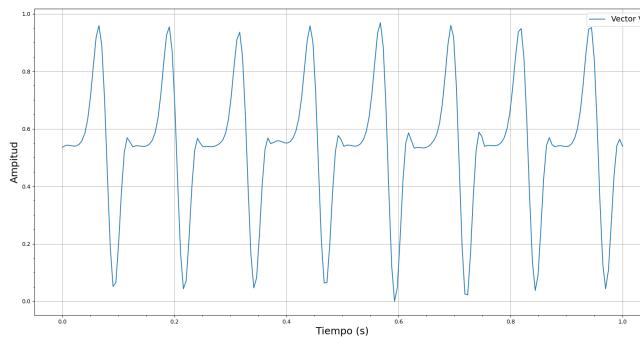
- Se aplica una ventana de 0,125 segundos a cada punto detectado, obteniendo así un vector H de  $n$  complejos QRS, y el resto de la señal se desecha. Este valor es constante, pues como se ha podido ver en la Figura 3.2 la duración del QRS no varía para una misma persona aún habiendo realizado ejercicio, aunque el ritmo cardíaco sea mayor.
- De estos  $n$  QRS, se extraen los  $m$  QRS más discriminatorios, obteniendo así el **vector V**, que es el vector que va a caracterizar a cada sujeto junto con su correspondiente etiqueta:
  - Para valorar la calidad de los complejos QRS y obtener dichos  $m$  QRS más discriminatorios que forman el vector **V**, se extrae del vector H el QRS promedio,  $\overline{QRS}$ , y se calculan los coeficientes de correlación de Pearson. Es decir, se calcula la correlación entre cada complejo QRS del vector H y el  $\overline{QRS}$ , obteniendo el vector C.

- Los  $m$  complejos QRS que tengan mayor valor de  $C$  se concatenan, dando como resultado el vector  $\mathbf{V}$ .
- Si el número  $i$  de QRS presentes en el vector  $H$  es menor que  $m$ , se completa el vector  $\mathbf{V}$  replicando el complejo que tenga mayor valor de  $C$ .
- Si el valor del coeficiente de correlación de Pearson es menor de 0,5, se considera que el complejo QRS no está correlado con el  $\overline{QRS}$ , y por tanto se descarta considerando que es ruidoso, o un complejo mal detectado.



**Figura 3.7.** Proceso de la segmentación de la señal hasta la obtención del vector  $V$ .

Para cada muestra que, recordamos, tiene una duración de 10 segundos y un número de QRS variable, sobre todo, según la persona y en función de si ha realizado ejercicio o no, se extrae el vector  $\mathbf{V}$  de características fijando  $m = 8QRS$ , es decir, un vector de 1 sg compuesto por 8 QRS concatenados y una dimensión de  $200 \times 1$ , teniendo en cuenta la frecuencia de muestreo (200 Hz). Este valor para  $m$  se ha fijado teniendo en cuenta el artículo de referencia [6], que basa su decisión en estudios previos que demuestran que 8 latidos mantienen un buen equilibrio entre rendimiento y usabilidad [9]. Además, el estudio de Salloum *et al.* [23], también ha demostrado que un mayor número de latidos concatenados da lugar a un mejor rendimiento de la red neuronal.



**Figura 3.8.** Ejemplo de un vector  $V$ , compuesto por 8 QRS y tiene 1 segundo de duración. El vector  $V$  es la entrada de la CNN.

A partir de este momento, cada vez que se haga referencia al uso de muestras de un usuario, éstas equivalen al  $\mathbf{V}$ . Este vector está compuesto por 200 elementos (1 segundo).

### 3.4. Extracción de características

Una vez realizado el preprocessamiento de la señal y obtenido el vector V, que se va a emplear para caracterizar a los sujetos, el siguiente paso es la extracción de características, es decir, la búsqueda de patrones. Como ya se ha comentado anteriormente, para realizar tanto la función de identificación como de autenticación, la extracción de características se basa en una red neuronal convolucional (CNN).

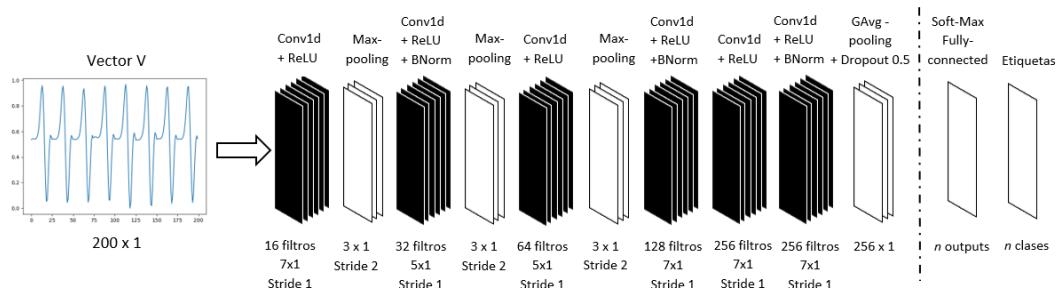
Aunque el uso más generalizado de las CNNs es la clasificación de imágenes 2D, su aplicación para señales unidimensionales es también muy efectiva cuando se espera extraer rasgos de pequeñas ventanas del conjunto de datos, y cuando la ubicación de estas características dentro de la ventana no es de gran relevancia. Así, mientras que una capa densamente conectada (*fully connected*) aprende patrones globales en su espacio global de entrada, las capas convolucionales lo hacen de manera local [36].

Como se va a detallar a lo largo de esta sección, para la identificación de usuarios y el entrenamiento de la red, el reconocimiento de los patrones obtenidos por la CNN se lleva a cabo mediante una capa de salida con la función de activación *Soft-max*, que devuelve la identidad del sujeto, mientras que para la autenticación, se realiza una comparación de estos patrones obtenidos por la CNN, determinando la verificación de la identidad en función de un umbral.

Los pasos que se han seguido para ello son: el diseño de la arquitectura de la CNN, la selección de hiperparámetros y el entrenamiento de la red y, en autenticación, la comparación de patrones.

#### 3.4.1. Arquitectura de la CNN

La Figura 3.9 muestra la arquitectura de la red utilizada. Como se puede comprobar, las primeras capas son convolucionales, intercaladas con capas de reagrupamiento *pooling* y de normalización, seguidas por una capa de *dropout* y finalmente, para el entrenamiento y la identificación, una capa densamente conectada (*fully connected*) con activación *Soft-max* (que se elimina en la configuración de red para autenticación de usuarios).



**Figura 3.9.** Esquema de la arquitectura de la CNN. La capa densamente conectada solo se utiliza para el entrenamiento de la red y para identificación.

A continuación, vamos a analizar brevemente las diferentes capas y su comportamiento:

- Primera capa convolucional 1D: esta capa es la que recibe los datos de entrada, es decir, el vector V obtenido tras el preprocesado de las señales. Este vector tiene una dimensión de  $200 \times 1$ , y por tanto, la capa estará compuesta por 200 neuronas. Esta capa define 16 filtros de dimensión  $7 \times 1$ , conocida como *kernel size*, es decir, la red aplica 16 filtros diferentes sobre el vector de entrada. Como resultado de la convolución con cada filtro, la salida de esta capa va a ser una matriz de características de  $194 \times 16$ . Cada columna de esta matriz contiene los pesos (*weights*) de un único filtro, es decir, 194 pesos. Estos pesos se van optimizando conforme se va entrenando la red.
- *Max-pooling*: esta capa se utiliza después de una capa convolucional con el fin de simplificar la información recogida por ésta y crear una versión condensada de la información que contiene. De esta manera, se reduce la complejidad de la salida de la capa anterior y ayuda a prevenir el sobreajuste *overfitting* de los datos. En concreto, la capa *Max-pooling* se queda con el valor máximo de los que había en la ventana de entrada. En este caso, tiene un tamaño de 3, por lo cual el tamaño de la matriz de salida de esta capa será solo una tercera parte de la de entrada.
- *Batch Normalization*: esta capa normaliza las funciones de activación de la capa anterior para cada *batch*, es decir, aplica una transformación para mantener su media próxima a 0 y su desviación estándar próxima a 1. Esta capa ayuda a prevenir la realentización del entrenamiento, reduciendo el cambio de covariante interno (del inglés *internal covariate shift*). El tamaño de la salida de esta capa es el mismo que el de la entrada.
- *Global Average Pooling*: esta capa es otro tipo de reagrupamiento, donde cada grupo de puntos de entrada se transforma en el valor promedio de los mismos, en vez del valor máximo. Por tanto, por cada filtro, solo permanece en la red un peso, reduciéndose así a una sola dimensión la salida.
- *Dropout*: esta capa asignará aleatoriamente un 0 a los pesos de las neuronas de la red. En este caso, el 50% de las neuronas recibirán un peso igual a cero. Gracias a esta capa, la red es menos sensible a pequeñas variaciones en los datos, y por tanto, aumentará su rendimiento cuando se utilice para datos desconocidos, es decir, mejorará su capacidad de generalizar. La dimensión de la salida de esta capa es la misma que la de entrada.

Para todas las capas convolucionales se usa la función de activación ReLU (*Rectified Linear Units*) para introducir la no linealidad a la red. La función de activación ReLU activa un solo nodo si la entrada está por encima de cierto umbral. Si la entrada está por debajo de cero la salida será cero, y cuando está por encima, la salida es una relación lineal con la variable de entrada de la forma  $f(x) = x$ . Además, en todas las capas *Max-pooling* se especifica una longitud de paso de avance (*stride*) de 2. Este parámetro controla cómo convoluciona el filtro sobre el volumen de entrada, es decir, define el número de pasos en que se mueve la ventana de los filtros, reduciendo todavía más el tamaño de la matriz de salida de las capas.

---

Las capas convolucionales y de reagrupamiento se van intercalando, como ya se ha visto en la Figura 3.9, de forma que la información obtenida como resultado de la convolución de los diferentes filtros con la señal de entrada se condensa, hasta que se obtiene un único **vector de características** de 256 elementos. Este vector representa el patrón de cada usuario. La Figura 3.10 muestra la arquitectura de la red con los tamaños de salida de cada capa.

Layer (type)	Output Shape	Param #
<hr/>		
conv1d_1 (Conv1D)	(None, 194, 16)	128
<hr/>		
max_pooling1d_1 (MaxPooling1)	(None, 96, 16)	0
<hr/>		
conv1d_2 (Conv1D)	(None, 92, 32)	2592
<hr/>		
batch_normalization_1 (Batch Normalization)	(None, 92, 32)	368
<hr/>		
max_pooling1d_2 (MaxPooling1)	(None, 45, 32)	0
<hr/>		
conv1d_3 (Conv1D)	(None, 41, 64)	10304
<hr/>		
max_pooling1d_3 (MaxPooling1)	(None, 20, 64)	0
<hr/>		
conv1d_4 (Conv1D)	(None, 14, 128)	57472
<hr/>		
batch_normalization_2 (Batch Normalization)	(None, 14, 128)	56
<hr/>		
conv1d_5 (Conv1D)	(None, 8, 256)	229632
<hr/>		
conv1d_6 (Conv1D)	(None, 2, 256)	459008
<hr/>		
batch_normalization_3 (Batch Normalization)	(None, 2, 256)	8
<hr/>		
global_average_pooling1d_1 (Global Average Pooling1D)	(None, 256)	0
<hr/>		
dropout_1 (Dropout)	(None, 256)	0
<hr/>		
dense_1 (Dense)	(None, 50)	12850
<hr/>		
Total params:	772,418	
Trainable params:	772,202	
Non-trainable params:	216	

**Figura 3.10.** Resumen del modelo empleado con los tamaños de las salidas de cada capa.

Los parámetros que no son entrenables provienen de las capas de *Batch Normalization*, pues sus vectores de media y varianza no se actualizan por propagación hacia atrás (*backpropagation*) [37].

En el caso de la arquitectura de la red para el entrenamiento y para realizar identificación, se utiliza una última capa de salida densamente conectada con función de activación *Soft-max*. Esta capa recibe como entrada el vector de características o patrón, de 256 elementos, y lo clasifica, de forma que devuelve como salida un vector de dimensión igual al número de clases posibles en la clasificación. Por tanto, para la primera base de datos que tiene 50 usuarios registrados, el vector tendrá 50 elementos, y para la segunda que tiene 55, 55. En esta capa *Soft-max*, cada neurona depende de las salidas de todas las demás neuronas de la capa, puesto que la suma de la salida de todas ellas debe ser 1. Por tanto, el valor de salida de cada neurona representa la probabilidad que tiene de pertenecer a la clase que representa.

Por otro lado, en autenticación, el vector de características se utiliza para realizar *template matching*, como se explica en la sección 3.4.3.

### 3.4.2. Selección de hiperparámetros y entrenamiento de la red

Los hiperparámetros difieren de los parámetros del modelo de una red, en que estos no pueden ser aprendidos explícitamente de los datos durante la fase de entrenamiento. Por tanto, los hiperparámetros se definen antes de entrenar un modelo y rigen el propio proceso de entrenamiento, influyendo de manera muy significativa en el resultado final. El número de hiperparámetros que se puede tener en cuenta a la hora de diseñar una red es muy extenso, y existen muchas posibles combinaciones. Además, también hay muchas formas de llevar a cabo la optimización de dichos hiperparámetros. Esto hace que su proceso de selección y optimización sea muy laborioso.

Para llevar a cabo esta optimización, los datos de entrenamiento han sido a su vez divididos en dos subconjuntos (*datasets*): el de entrenamiento y el de validación. De esta forma, los datos de validación, que la red no ha analizado durante el entrenamiento, se utilizan para ajustar los hiperparámetros. Así, para ambas bases de datos, las muestras se han dividido desde el principio en tres *datasets*: entrenamiento, validación y prueba. De esta manera, el modelo siempre se entrena sobre los datos de entrenamiento, los hiperparámetros se optimizan usando los datos de validación y el resultado final del modelo se evalúa sobre los de prueba, conocido como método de retención (*holdout method*). La desventaja que presenta este método es que la evaluación de resultados se ve condicionada por los datos elegidos para la validación. Por ello, para la primera base de datos, también se ha probado una validación cruzada de  $K$  iteraciones ( *$k$ -fold cross-validation*). En ella, los datos de entrenamiento se dividen en  $k$  subconjuntos (*folds*), y el proceso de validación cruzada se repite  $k$  veces. En cada iteración, uno de los  $k$  subconjuntos se usa como set de validación y el resto  $k - 1$  subconjuntos son utilizados como set de entrenamiento. Finalmente se realiza la media aritmética de los resultados de cada iteración para obtener un único resultado. Sin embargo, aunque este método es más preciso, es muy lento desde el punto de vista computacional, y no se ha aplicado para la segunda base de datos.

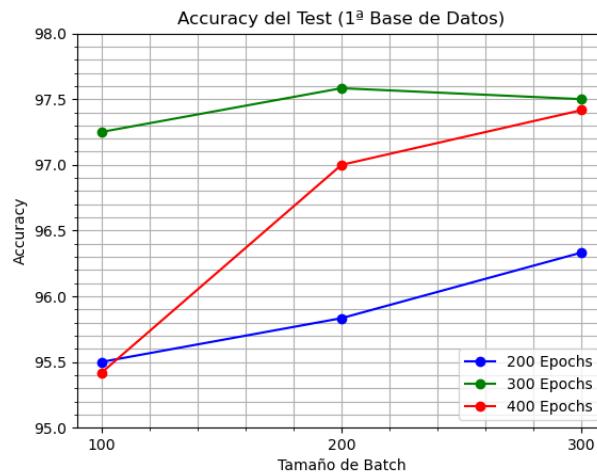
El método de muestreo que se ha utilizado durante la optimización ha sido el muestreo de cuadrícula (*grid search*), que consiste en una búsqueda exhaustiva sobre determinados conjuntos de hiperparámetros del modelo. La red es entrenada para cada valor de los hiperparámetros, y el resultado de cada modelo es comparado, eligiendo finalmente el que que haya obtenido un resultado mejor. La métrica que se ha utilizado para comparar los modelos es el rendimiento (*accuracy*).

Optimizador	BatchNormalization Layers	Global Avg-Pooling	Accuracy
SGD	Si	Si	95,6%
		No	94,75%
	No	Si	-
		No	71%
Adam	Si	Si	97,75%
		No	97,5%
	No	Si	-
		No	95,7%

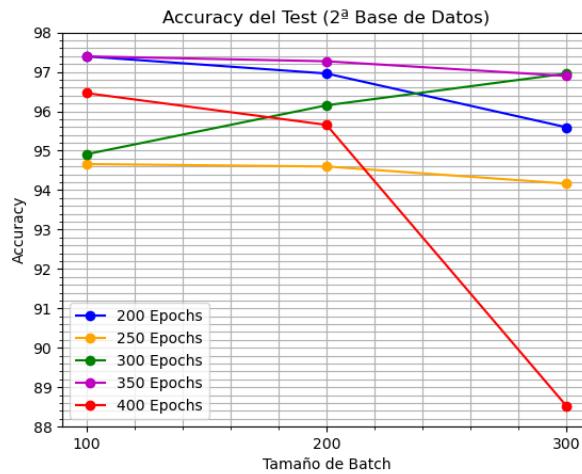
**Tabla 3.1.** Comparativa de los resultados del rendimiento de la red durante la fase de prueba para diferentes modelos.

Algunos de los hiperparámetros, como el número de capas ocultas de la red, el uso de *strides*, el tamaño y número de filtros y las funciones de activación, entre otros, ya se han comentado en la sección anterior. Estos han sido ajustados basándose en el artículo de referencia [6] y de manera empírica. La Tabla 3.1 muestra una comparativa de los resultados de rendimiento sobre los datos de prueba de diferentes modelos que se han evaluado para la primera base de datos.

Otros hiperparámetros que se han tenido en cuenta son el tamaño de *batch* y el número de *epochs*. Para ambas bases de datos, se ha realizado un muestreo en cuadrícula para diferentes valores. Los resultados de rendimiento obtenidos para cada base de datos sobre las muestras de prueba en las diferentes combinaciones se pueden ver en la Figura 3.11.



(a) Base de datos 1

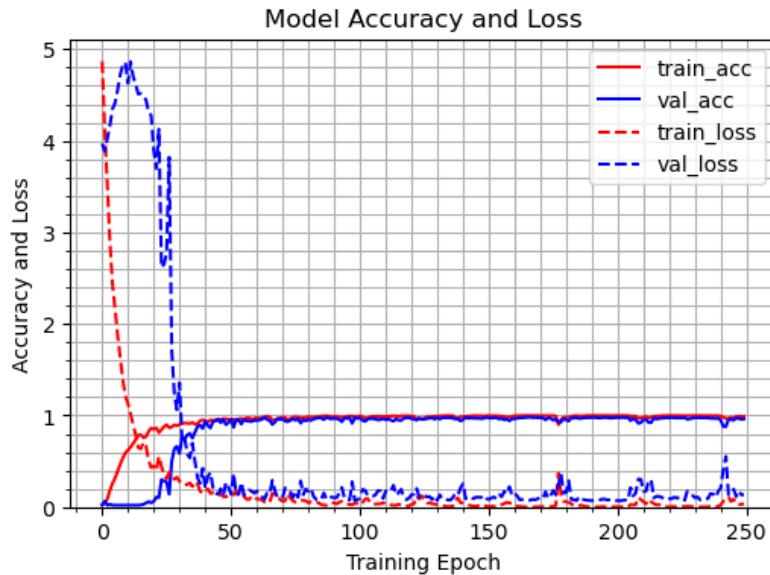


(b) Base de datos 2

**Figura 3.11.** Optimización del tamaño de *batch* y el número de *epochs* mediante un muestreo de cuadrícula.

Para la fase de entrenamiento la función de pérdida (*loss*) que se ha utilizado es *categorical\_crossentropy*, que ajusta los parámetros del modelo (los pesos  $w_i$  y el sesgo  $b$ ) de tal manera que el resultado de la pérdida tenga el mínimo valor posible. Finalmente, el optimizador usado ha sido el *adam* con una tasa de aprendizaje (*learning rate*) de 0.001.

La Figura 3.12 muestra la evolución del rendimiento y de la pérdida durante el entrenamiento de uno de los modelos. Como se puede ver, tanto para el set de entrenamiento como para el de validación, el rendimiento se acerca a 1 y la pérdida a 0, obteniéndose por tanto buenos resultados en cuanto al entrenamiento de la red.



**Figura 3.12.** Evolución del rendimiento y de la pérdida de entrenamiento y de validación durante la fase de entrenamiento de la red.

### 3.4.3. Comparación de patrones

La autenticación biométrica se ha llevado a cabo mediante la comparación de patrones o *template matching*. Más específicamente, un **patrón** o **template** es una instancia registrada de las características biométricas de una persona. El patrón se registra durante la fase de reclutamiento del usuario en el sistema y se almacena en una base de datos. Posteriormente, cuando el usuario realiza una consulta (*query*), se registra una nueva muestra y se compara con su patrón específico, en oposición a la identificación, en la que se compara con todos los patrones registrados, tal y como se ha explicado en la sección 1.2.2.

Para implementar la configuración de red utilizada en autenticación, se ha retirado la última capa (*Soft-max*) de un modelo entrenado con los usuarios de la primera base de datos, y esta nueva arquitectura de red se ha utilizado para verificar la identidad de los usuarios de la segunda base de datos, y viceversa. De esta manera, la red siempre ha sido entrenada con usuarios diferentes a los usuarios que se quiere autenticar.

Durante la fase de reclutamiento, la red se utiliza para obtener el patrón específico de cada usuario. La nueva salida (*output*) de la red es el vector de características de 256 elementos para cada muestra, como ya comentábamos en 3.4.1. De todos los vectores de

características obtenidos para un mismo usuario, se extrae un único vector promedio, de la misma dimensión, y éste se almacena como **patrón** del usuario.

Durante la fase de consulta, se obtiene el vector de características para una nueva muestra del usuario que realiza dicha consulta, y este vector de características se compara con el patrón almacenado de este usuario. Para realizar esta comparación, en el espacio de dimensión  $k = 256$ , se ha utilizado la distancia euclídea:

$$D(P, Q) = \sqrt{\sum_{i=1}^n (p_i - q_i)^2}$$

Donde  $P$  es el vector **patrón** y  $Q$  es el vector de la **consulta (query)**. Si la distancia obtenida es menor que un umbral establecido, la consulta se considera válida, el usuario es quien dice ser, mientras que si supera el umbral la consulta es rechazada, pues el usuario no es quien dice ser sino un impostor.

---

## **4. Evaluación del sistema: resultados experimentales**

---

En este capítulo se va a describir la evaluación de la red neuronal convolucional propuesta en el capítulo anterior con las bases de datos, también ya descritas. Los resultados están divididos en dos secciones: Identificación y Autenticación. Además, los resultados de identificación están a su vez divididos según las diferentes bases de datos.

### **4.1. Identificación**

La arquitectura de identificación se ha probado tanto para la primera base de datos como para la segunda y, además, se ha realizado una prueba sobre la base de datos completa (los 105 sujetos). En todos los casos, se ha realizado una identificación sobre un conjunto cerrado (*closed set*), es decir, todos los sujetos que se pretende identificar han tenido que ser previamente registrados (todas las muestras de test pertenecen a usuarios cuyas muestras se han utilizado para el entrenamiento de la red).

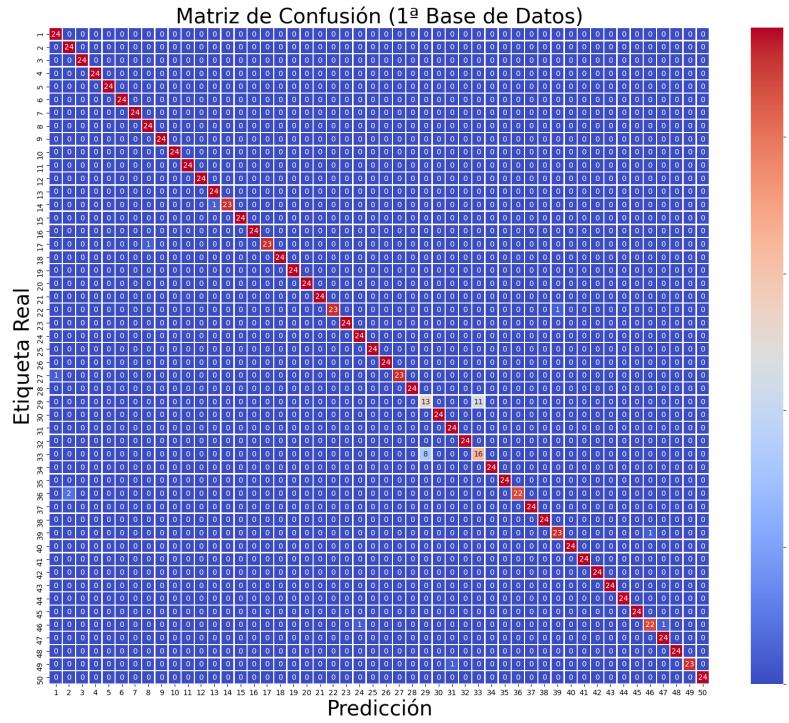
Las muestras se han dividido siempre en un 80 % para entrenamiento y 20 % para test. A su vez, el set de entrenamiento se ha dividido en un 90 % entrenamiento y 10 % validación.

Al evaluar el rendimiento del clasificador con ambas bases de datos, se ha querido comprobar que, efectivamente, ni el estado físico de la persona ni el día en que han sido tomadas las muestras afectan al proceso de su identificación.

#### **4.1.1. Primera base de datos**

Para los primeros 50 usuarios, se han utilizado muestras tanto de la primera sesión como de la segunda de cada uno. Además, se han incluido muestras tanto con los ojos abiertos como con los ojos cerrados. Como resultado, se ha conseguido un rendimiento de prueba del 97,58 %, con una pérdida de 0,08.

Para llevar a cabo una evaluación más exhaustiva del clasificador, la matriz de confusión con las identidades reales y las predichas se puede ver en la Figura 4.1.



**Figura 4.1.** Matriz de confusión obtenida para la base de datos 1.

Como se puede ver, es evidente que el sistema no es capaz de distinguir con tanta precisión solo entre los sujetos 29 y 33. Una hipótesis que cabría plantearse es si estas dos personas podrían tener una relación paterno-filial o fraternal, poniendo en duda la unicidad de la señal cardíaca en ese caso.

La Tabla 4.1 muestra una medición de la calidad de las clasificaciones basada en las siguientes métricas:

- Precisión: indica si una predicción positiva lo era realmente.

$$precision = \frac{VP}{VP+FP}$$

- *Recall* o exhaustividad: indica cuántos positivos ha identificado el modelo de todos los posibles positivos.

$$recall = \frac{VP}{VP+FN}$$

- *F1-score* o valor F: es la media armónica entre precisión y *recall*.

$$F1 = 2 \times \frac{precision \times recall}{precision + recall}$$

Siendo  $VP$  verdaderos positivos,  $FP$  falsos positivos y  $FN$  falsos negativos.

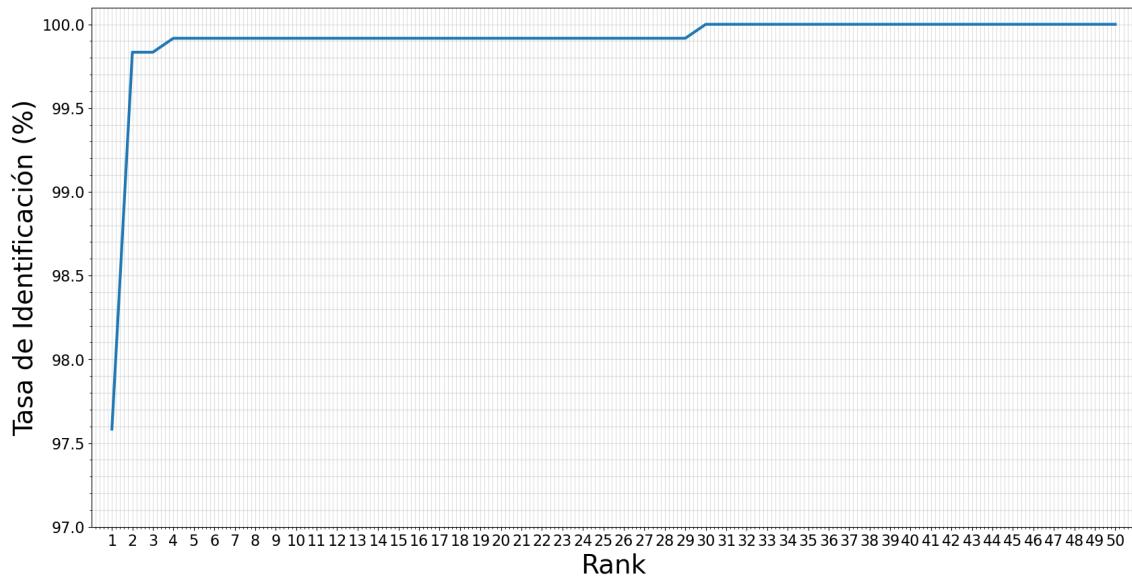
Donde *macro avg* es el resultado de calcular las métricas de cada etiqueta y obtener su media no ponderada, sin tener en cuenta el desequilibrio entre etiquetas, mientras que en *weighted avg* se obtiene la media ponderada [26].

	Precisión	Exhaustividad	Valor F1	N.º de Muestras
<i>accuracy</i>			0,98	1200
<i>macro avg</i>	0,98	0,98	0,98	1200
<i>weighted avg</i>	0,98	0,98	0,98	1200

**Tabla 4.1.** Calidad de las clasificaciones obtenidas para la base de datos 1.

En este caso, para cada usuario se ha utilizado el mismo número de muestras en la evaluación, y estos valores próximos a 1 para las diferentes métricas muestran una buena calidad de los resultados. Los valores de cada métrica para la identificación de cada usuario pueden verse en A.1. Si nos fijamos en los valores obtenidos para los usuarios 29 y 33 nos damos cuenta que, efectivamente, estos son notablemente inferiores que para el resto de usuarios, con un Valor de F1 igual a 0,68 y 0,58 respectivamente.

Atendiendo a la norma *ISO/IEC JTC 1/SC 37* [38] y a *Biometrics Evaluation and Testing (BEAT)* [39, 40], la métrica para evaluar un sistema de identificación *closed set* es la curva CMC (*Cumulative Match Characteristic*). En identificación,  $rank(k)$  es el menor valor de  $k$  para el cual un identificador correcto de un usuario está entre los principales  $k$  identificadores devueltos por el sistema, y su valor varía entre 1 y el número de sujetos (en este caso 50). La curva CMC representa gráficamente los resultados de test, representando en el eje  $x$  los valores de  $rank(k)$ , frente a la probabilidad de que la identificación sea correcta en ese  $rank$ , en el eje  $y$  [41].



**Figura 4.2.** Curva CMC obtenida para los datos de prueba de la base de datos 1.

Como se puede ver, para este modelo hay un primer fallo de identificación en el  $rank = 30$ , lo que indica que el identificador correcto tenía por delante 30 identifica-

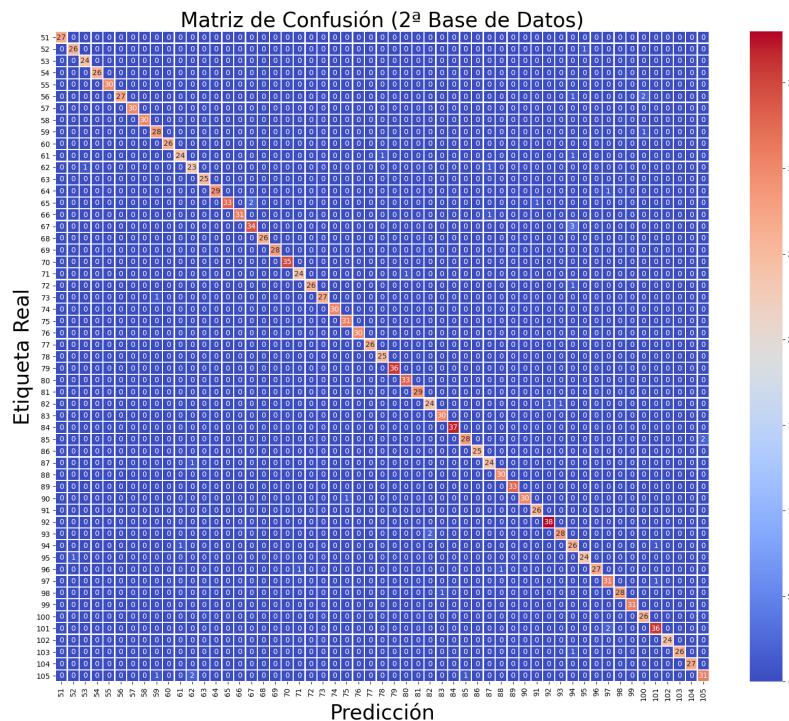
dores con una mayor probabilidad. Los demás fallos en la predicción de identidades los encontramos a partir del  $rank = 4$ , dando lugar a una curva muy próxima a la esquina superior izquierda. Teniendo en cuenta que un sistema es mejor cuanto más se acerca a la esquina superior izquierda [40], podemos asegurar que el rendimiento de este sistema es muy prometedor.

#### **4.1.2. Segunda base de datos**

Para la segunda base de datos se ha seguido el mismo procedimiento que para la primera, obteniendo resultados de 96,98 % de rendimiento y 0,13 de pérdida. Estos resultados se han obtenido utilizando las muestras de ambas sesiones, es decir, incluyendo tomas en reposo y tras realizar ejercicio.

Además, como las tomas en las que el usuario ha realizado ejercicio son solo un cuarto del total de las tomas, estas han sido a su vez divididas durante el preprocesado en dos nuevas tomas, atendiendo al incremento en el número de QRS presentes en ellas. Con esta modificación de la base de datos se ha vuelto a entrenar una CNN, consiguiendo mejorar el resultado a un 97,39 % de rendimiento y 0,12 de pérdida. Estos valores permiten demostrar que la red es capaz de identificar usuarios aún cuando las muestras incluyen tomas después de haber realizado deporte.

Las siguientes Figuras y Tablas muestran la matriz de confusión, la medición de la calidad del clasificador y la curva CMC de este modelo, tal y como se ha hecho para la primera base de datos.



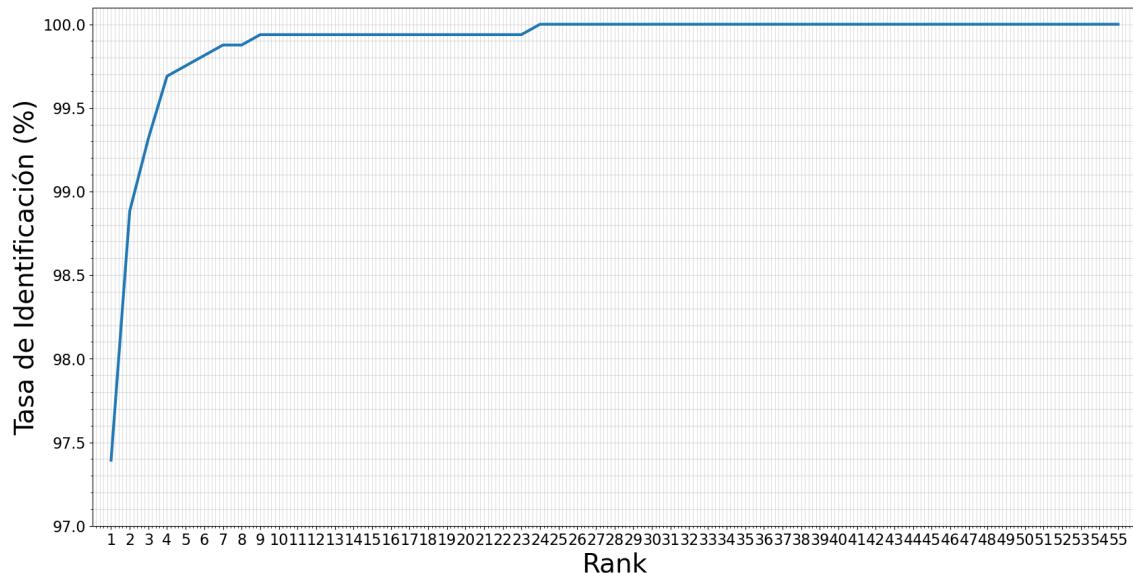
**Figura 4.3.** Matriz de confusión obtenida para la base de datos 2.

Esta matriz de confusión muestra unos muy buenos resultados de predicción para todos los usuarios por igual. En este caso, como se puede observar, no se ha utilizado el mismo número de muestras para cada usuario.

	Precisión	Exhaustividad	Valor F1	N.º de Muestras
<i>accuracy</i>			0,97	1611
<i>macro avg</i>	0,97	0,97	0,97	1611
<i>weighted avg</i>	0,98	0,97	0,97	1611

**Tabla 4.2.** Calidad de las clasificaciones obtenidas para la base de datos 2.

Los resultados de las métricas de la identificación de cada usuario por separado se pueden ver en A.2. Como se puede apreciar, en este caso sí hay una ligera diferencia entre la media ponderada y sin ponderar de la precisión debido al desequilibrio entre el número de muestras de cada usuario utilizado.



**Figura 4.4.** Curva CMC obtenida para la base de datos 2.

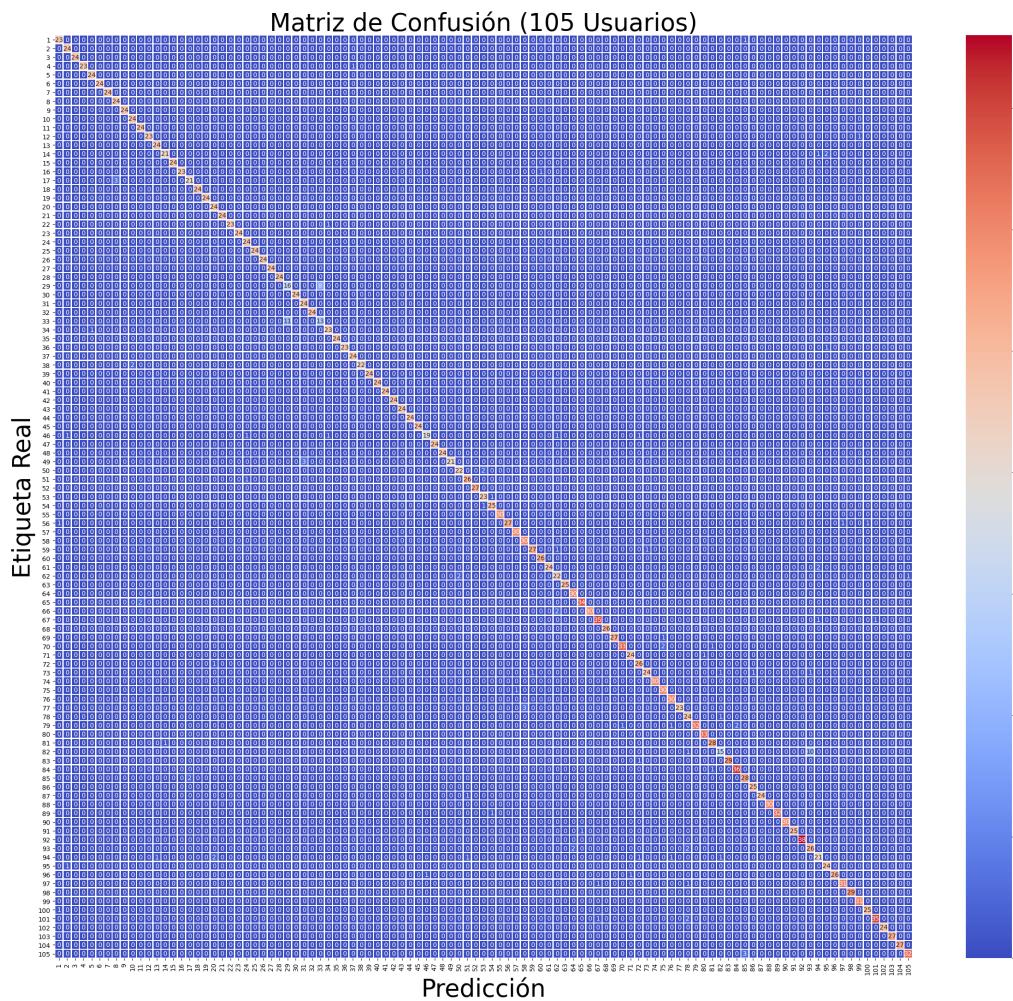
Para este modelo, la curva CMC muestra un primer fallo de identificación en el  $rank = 24$ . Comparando las dos curvas CMC obtenidas (Figura 4.6), podemos ver cómo a partir del  $rank = 9$  el rendimiento de este sistema es algo peor que el del primero. Aún así, se puede considerar que se ha obtenido una buena curva CMC.

Como se puede ver, los resultados obtenidos son muy parecidos para ambas bases de datos, lo que demuestra que el ECG se puede utilizar para la identificación de usuarios aún cuando se incluyen muestras registradas después de haber realizado ejercicio, con un incremento notable del ritmo cardíaco.

#### 4.1.3. Base de datos completa

También se ha entrenado una red para toda la base de datos, incluyendo los 105 usuarios, obteniendo un rendimiento de 95,59 % y una pérdida de 0,18.

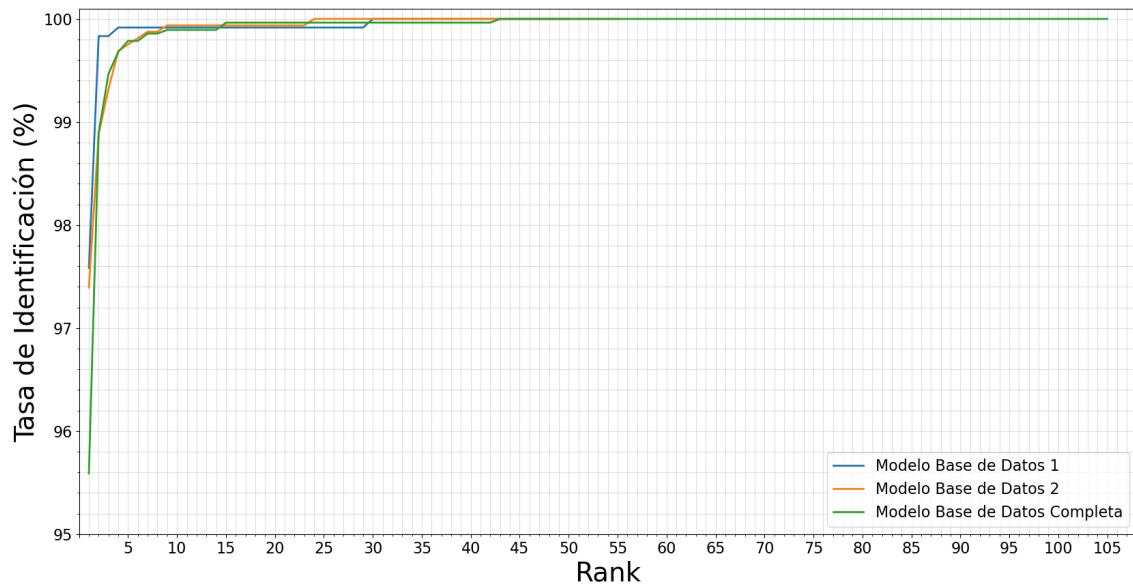
La matriz de confusión de este modelo se puede ver en la Figura 4.5. Si nos fijamos bien, es posible observar como este modelo sigue sin ser capaz de distinguir con precisión entre los usuarios 29 y 33. Por otro lado, a diferencia del modelo anterior, este nuevo modelo no es capaz de identificar con tanta precisión las muestras del usuario 82, confundiéndolo a menudo su identidad con la del usuario 93, pero no del revés.



**Figura 4.5.** Matriz de confusión obtenida para los datos de prueba de la base de datos completa.

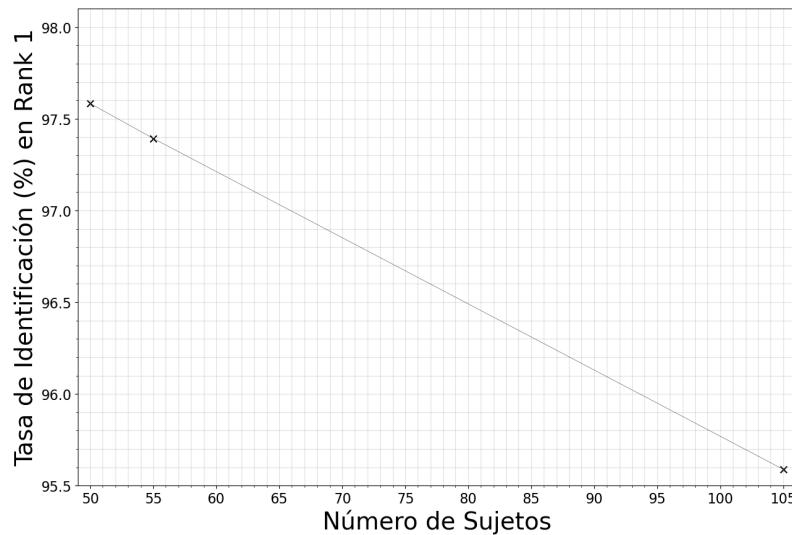
La métricas obtenidas en la evaluación de la calidad del sistema se pueden ver en A.3.

La curva CMC obtenida para esta base de datos, comparada con las curvas obtenidas para las otras dos bases de datos, puede verse en la Figura 4.6. Aunque el rendimiento de este modelo sea algo peor, se puede apreciar una buena curva CMC, próxima a la obtenida para el modelo que identifica solo a la segunda base de datos.



**Figura 4.6.** Comparación de las CMC obtenidas para las bases de datos 1 y 2, así como la base de datos al completo.

Además, la siguiente Figura (4.7) muestra una comparativa de la tasa de identificación para el  $\text{rank}(1)$  en función del número de usuarios registrados en el sistema. Cabe recordar que ninguno de los usuarios utilizados para los valores de 50 y 55 son los mismos, mientras que el valor 105 corresponde a la unión de ambos.



**Figura 4.7.** Variación de la tasa de identificación en el  $\text{rank}(1)$  en función del número de sujetos.

Como se puede ver, en este caso la identificación ha empeorado cuando ha aumentado el número de usuarios registrados. Sin embargo, ajustando los hiperparámetros de red de este último modelo, probablemente se podrían llegar a conseguir mejores resultados.

#### 4.1.4. Variabilidad intra-clase

Por último, se ha querido comprobar la estabilidad del ECG como característica biométrica. Para ello, se ha utilizado solo la primera base de datos, entrenando una red con los registros de la primera sesión y evaluando el sistema con los registros de la segunda sesión, y viceversa. Por tanto, la división de muestras en esta configuración ha sido 50 % de entrenamiento y 50 % de test. Para poder comparar los resultados con los obtenidos cuando las muestras de ambas sesiones están mezcladas, se ha entrenado también otra red con una división 50 – 50 %. Los resultados obtenidos han sido los siguientes (Tabla 4.3):

Muestras de Test	Accuracy	Loss
Sesión 1 y 2	95,0%	0,18
Sesión 1	65,1%	3,01
Sesión 2	67,8%	3,42

**Tabla 4.3.** Comparación de los resultados de rendimiento y pérdida obtenidos con variabilidad intra-clase.

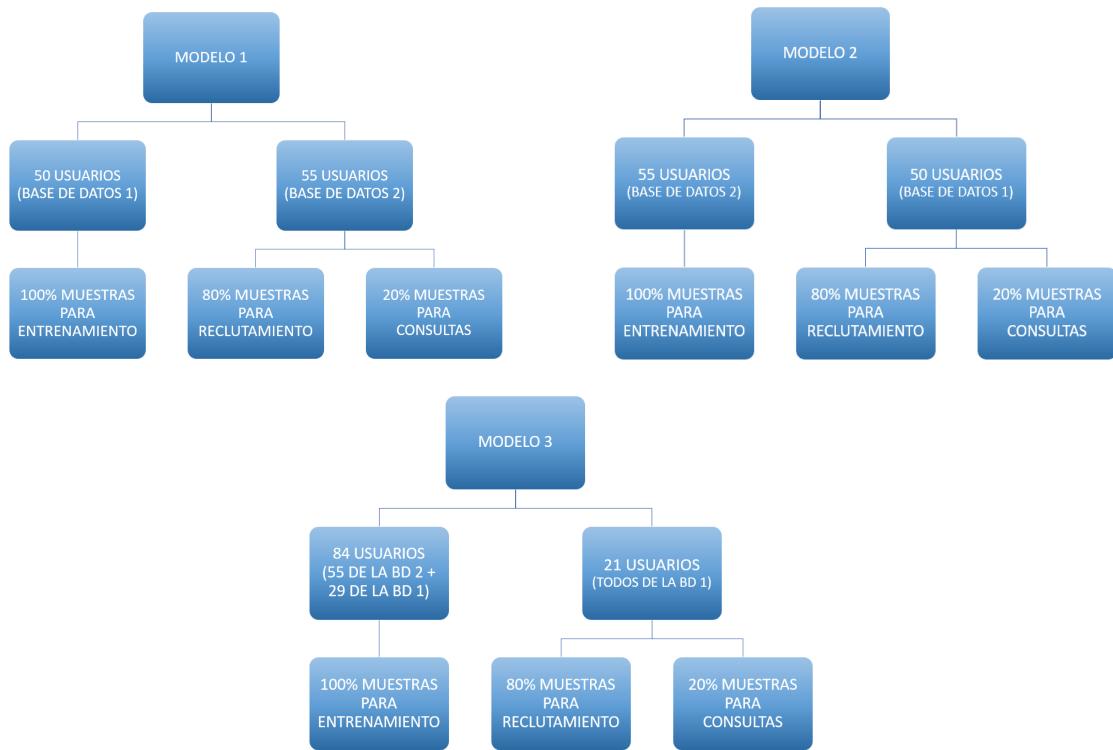
Se puede apreciar que la identificación de usuarios es notablemente peor cuando la evaluación del sistema se realiza con muestras registradas en un día diferente al de las muestras utilizadas para el entrenamiento de la red. Por tanto, no podemos demostrar la estabilidad del ECG como característica biométrica con este estudio.

#### 4.2. Autenticación

El proceso de autenticación se divide (como ya hemos visto) en dos fases: reclutamiento y consulta. Para el reclutamiento se ha utilizado el 80 % de las muestras de cada usuario del cual se quiere verificar la identidad, y el 20 % restantes se han reservado para realizar las consultas. Por tanto, las muestras de verificación nunca se han utilizado en el reclutamiento, ni viceversa.

Para evaluar el sistema se han realizado pruebas sobre 3 modelos diferentes:

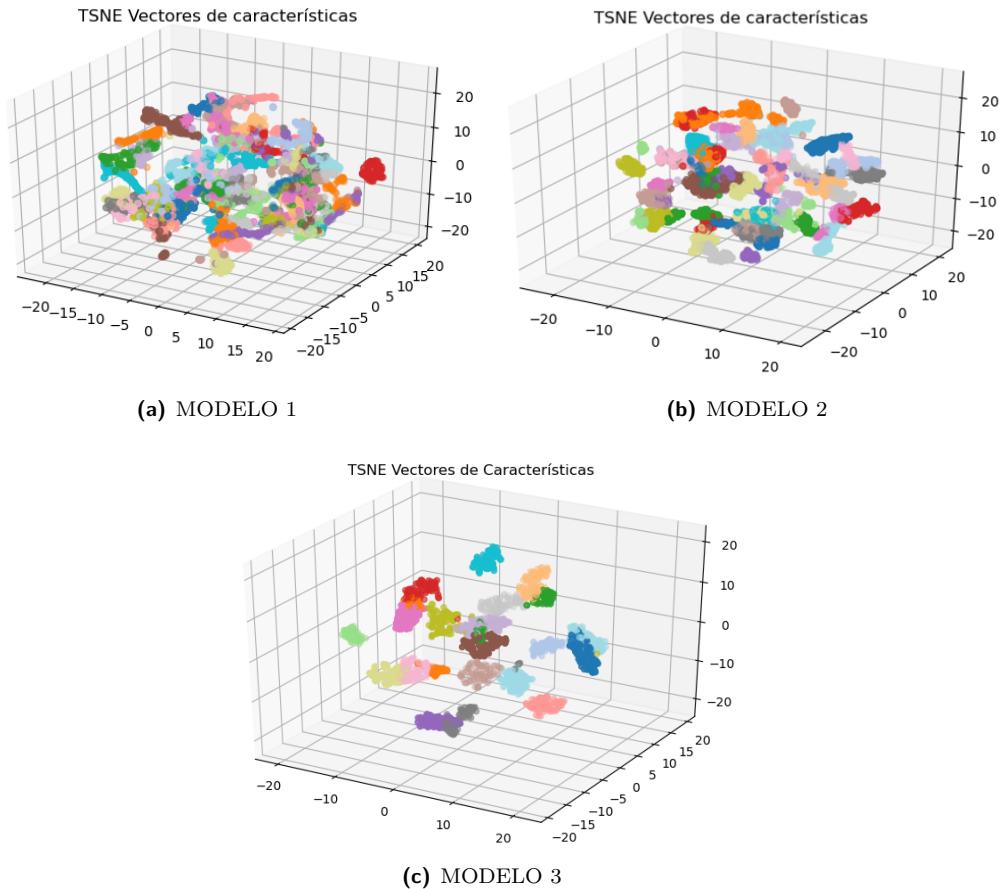
- Modelo 1: se verifica la identidad de los 55 usuarios de la segunda base de datos (que recordamos, incluye tomas registradas después de haber realizado ejercicio). Para ello, se utiliza una red entrenada con los 50 usuarios de la primera base de datos, es decir, el porcentaje de usuarios utilizado para el entrenamiento es del 47 %.
- Modelo 2: se verifica la identidad de los 50 usuarios de la primera base de datos, utilizando una red entrenada con los 55 de la segunda (54 %).
- Modelo 3: para comprobar la influencia del porcentaje de usuarios utilizados para el entrenamiento, se ha entrenado una nueva red con el 80 % de los usuarios totales (84 usuarios) y se ha verificado la identidad del 20 % de usuarios restantes.



**Figura 4.8.** Esquema de la división de usuarios y de sus muestras para las distintas fases en cada modelo.

Para visualizar los vectores de características obtenidos durante la fase de reclutamiento, se han utilizado las herramientas PCA y TSNE [26]. Estas herramientas permiten la visualización de datos de grandes dimensiones, mediante la reducción de su dimensionalidad.

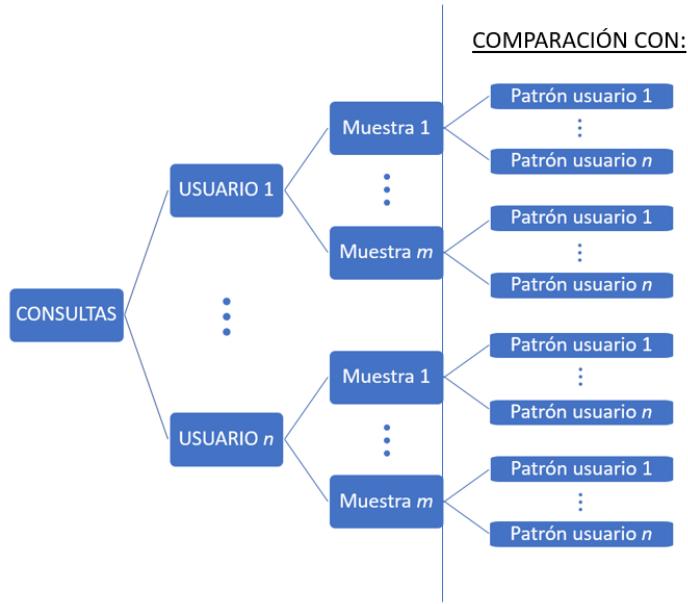
Como se puede ver en la Figura 4.9, los vectores de características se encuentran bastante agrupados en el espacio en función del usuario al que corresponden. Estas agrupaciones por usuarios son más evidentes en el Modelo 3, pero esto puede deberse a que solo hay 21 usuarios registrados en el sistema y por eso la visualización es mejor. Entre el Modelo 1 y el 2, cabría esperar obtener mejores resultados para el segundo, donde estas agrupaciones están más definidas. Visualizando de esta manera los vectores de características de cada usuario, es bastante evidente que sí se puede distinguir a las personas a través de su señal de ECG. En B.1 se puede ver la visualización de los mismos vectores con la herramienta PCA.



**Figura 4.9.** Comparativa de la distribución de los vectores de características obtenidos durante la fase de reclutamiento para cada modelo, empleando la herramienta de visualización TSNE para reducir a tres dimensiones el espacio.

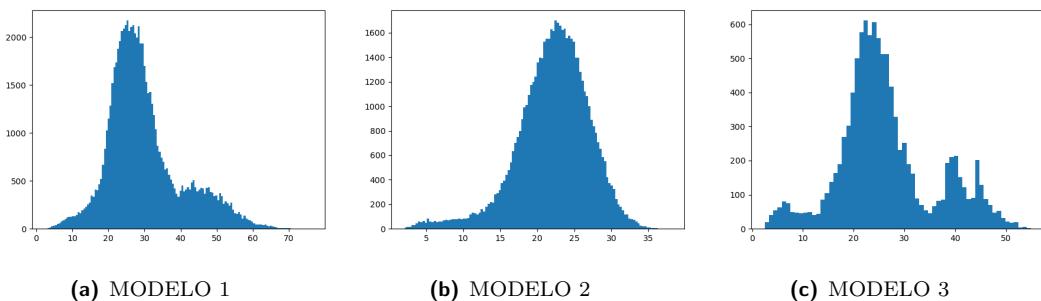
Para evaluar el sistema, con cada muestra de cada usuario se han realizado consultas genuinas, en las que se compara la muestra con su patrón registrado, pero también consultas de “impostores”, donde se compara la muestra de ese usuario con los patrones registrados de todos los demás usuarios. Cada consulta, ya sea genuina o no, se considera independiente, luego para una única muestra hay tantas consultas como usuarios ( $n$ ) registrados en el sistema, de las cuales solo 1 es genuina y el resto ( $n - 1$ ) de impostores. Aunque en un escenario más realista para un sistema de autenticación se espera que el número de consultas genuinas sea mayor que el de consultas de impostores, en este estudio se ha utilizado esta metodología para poder evaluar más a fondo el rendimiento del sistema con los datos disponibles.

Como el número de consultas depende del número de usuarios registrados en cada modelo, para llevar a cabo una comparativa entre los mismos se va a hablar siempre del número de muestras  $m$  por usuario que se ha utilizado para realizar las consultas  $q$ , con  $q = n \times (m \times n)$ .



**Figura 4.10.** Esquema de la fase de consulta.

La distribución de las distancias euclídeas obtenidas al utilizar todas las muestras del set de consulta para realizar con ellas todas las consultas posibles, se puede observar en la Figura 4.11. Como la mayoría de las consultas son de impostores, esta visualización de las distancias permite hacerse una idea de dónde debería establecerse el umbral. Además, se ve claramente como la mayoría de distancias se encuentran dentro de un rango de valores, y solo unas pocas (las correspondientes a las consultas genuinas) tienen una distancia menor. Aunque en el modelo en el que mejor se aprecia es en el 3, esto se debe a que al haber menos usuarios registrados el número de consultas realizadas también es menor (aproximadamente un sexto de las consultas realizadas en los otros 2 modelos). Por otro lado, es notable la diferencia del rango de valores obtenidos para las distancias entre los modelos, estando todas las distancias bastante más concentradas en el Modelo 2 (entre 2,5 y 37).



**Figura 4.11.** Distribución de usuarios genuinos e impostores mediante la distancia euclídea.

Atendiendo a la norma *ISO/IEC JTC 1/SC 37* [38] y a *Biometrics Evaluation and Testing (BEAT)* [39, 40], las métricas utilizadas para evaluar un sistema de autenticación son:

- *Failure-to-enrollment rate*: proporción de los usuarios para los que el sistema no ha completado la fase de reclutamiento.
- *Failure-to-acquire rate*: proporción de intentos de verificación o identificación en los que el sistema no logra captar o localizar una imagen o señal de calidad suficiente.
- Tasa de Falsa Aceptación o FAR (de sus siglas en inglés): proporción de intentos de acceso no autorizados aceptados incorrectamente por el sistema.
- Tasa de Falso Reconocimiento o FRR (de sus siglas en inglés): proporción de intentos de acceso autorizados denegados incorrectamente por el sistema.

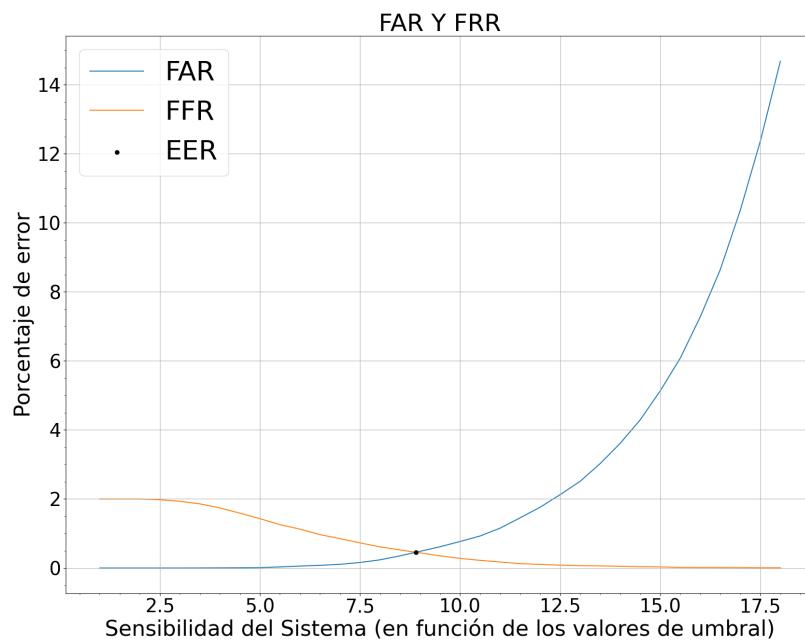
En este trabajo, la tasa de adquisición se desconoce y la tasa de error de enrolamiento no se ha tenido en cuenta, por lo que se considera también como desconocida.

El FAR y el FRR han sido calculados de la siguiente manera:

$$FAR = \frac{\text{Falsos Positivos}}{\text{Nº Total de Consultas}}$$

$$FRR = \frac{\text{Falsos Negativos}}{\text{Nº Total de Consultas}}$$

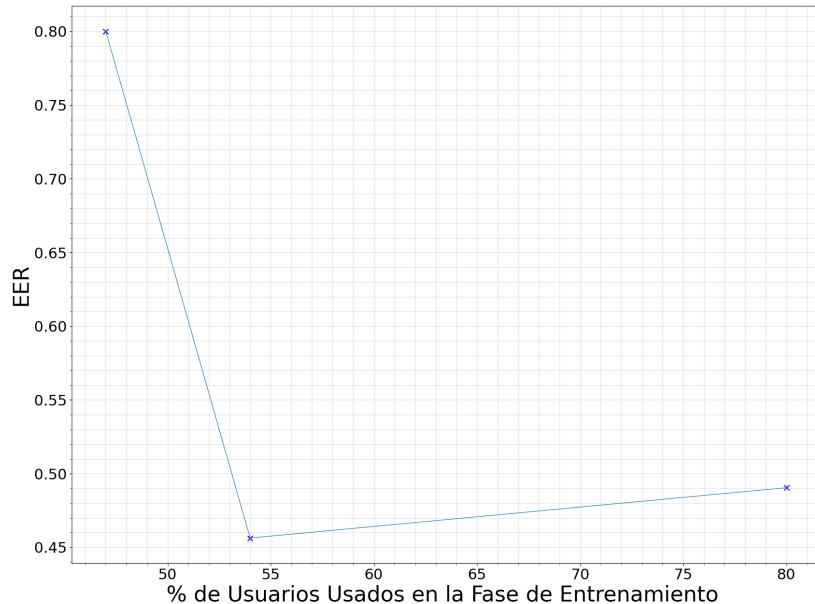
Además, la métrica empleada para comparar el rendimiento de los diferentes modelos ha sido el *Equal Error Rate* (EER), que se obtiene variando el umbral y representando gráficamente las curvas FAR y FRR obtenidas, siendo el EER el punto de intersección entre ambas.



**Figura 4.12.** Curvas FAR y FRR. El EER es el punto de intersección entre ambas curvas.

El con el que se ha obtenido mejor EER ha sido el 2, con un error de tan solo:  $EER_2 = 0,46\%$ . La Figura 4.12 muestra su EER obtenido haciendo uso de todas las muestras disponibles en el set de consulta.

Si comparamos el EER obtenido para los 3 modelos (Figura 4.13), nos encontramos con un peor valor para el primero ( $EER_1 = 0,81\%$ ). Aún así, este valor de error sigue siendo significativamente bueno y, más aún, si tenemos en cuenta que estamos utilizando una red que no ha sido entrenada con ninguna toma registrada después de hacer ejercicio, para verificar la identidad de usuarios después de haberlo realizado. Si nos fijamos en los resultados obtenidos para el 2º y el 3º modelo, observamos que son prácticamente iguales ( $EER_3 = 0,49\%$ ), por lo que a primera vista parece que aumentar el porcentaje de sujetos con los que se ha realizado la fase de entrenamiento no ha supuesto una mejora.

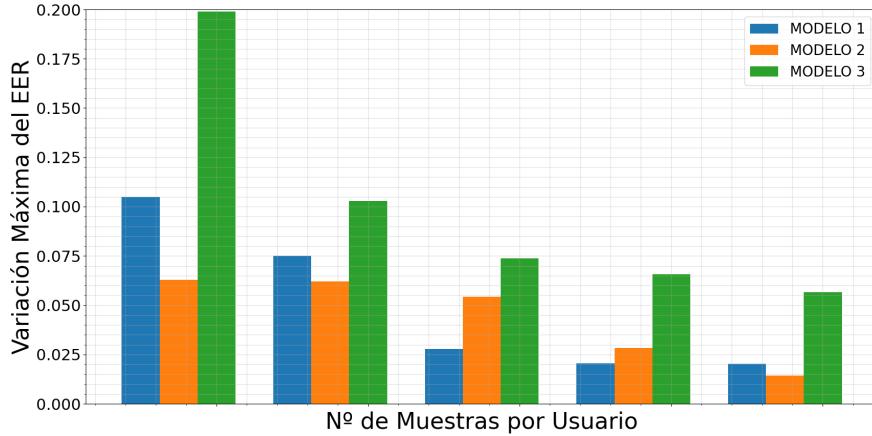


**Figura 4.13.** Comparación del EER obtenido en función del porcentaje de usuarios utilizado para el entrenamiento de la red.

Para analizar más detalladamente el comportamiento del EER, se ha analizado su variabilidad en función de las muestras de cada usuario que se utilizan para realizar las consultas. Para ello, se han ejecutado varias veces consultas con  $m$  muestras por usuario. Estas  $m$  muestras de cada usuario se seleccionan aleatoriamente de entre todas las disponibles cada vez que se realiza una ejecución con  $q = n \times (m \times n)$  consultas.

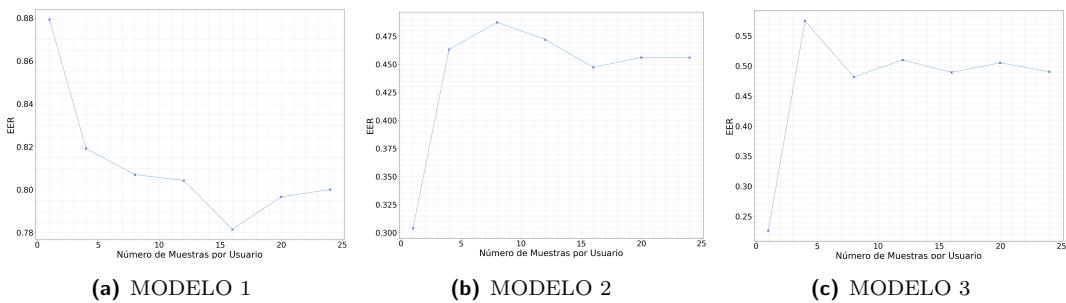
En la Figura 4.14 podemos ver la variación máxima del EER en función del número de muestras por usuario para cada modelo. Esta Figura muestra una clara tendencia en la que la variación máxima del EER disminuye a medida que aumenta el número de muestras utilizado, en todos los modelos. Por tanto, el rendimiento del sistema depende en cierta medida de las muestras con las que se han realizado las consultas, y cuantas más consultas se realizan más fiable es el resultado obtenido.

Además, es muy significativa la diferencia de magnitud entre el Modelo 3 y los demás, con una variación de más del doble en algunos de los casos. Este dato evidencia que el sistema es más fiable cuantas más consultas se realizan, pues en el Modelo 3 hay menos de la mitad de usuarios registrados y por tanto el número de consultas que se pueden realizar con  $m$  muestras es mucho menor. Así, cabría pensar que, si se pudiera hacer un mayor número de consultas para evaluar este modelo sí obtendríamos una mejora del rendimiento en función del número de usuarios utilizados para el entrenamiento, como se obtiene en [23].



**Figura 4.14.** Variabilidad del resultado de error obtenido en función de las muestras utilizadas.

En la siguiente Figura (4.15) podemos ver un ejemplo de los EER obtenidos utilizando  $m$  muestras aleatorias de cada usuario. Teniendo en cuenta la variación de este error que acabamos de comentar, podemos ver cómo aunque se haya obtenido un mejor error para un  $m$  menor, este resultado depende de las muestras que se hayan utilizado para ese caso concreto, mientras que si aumenta el número de muestras utilizado el resultado es más fiable.

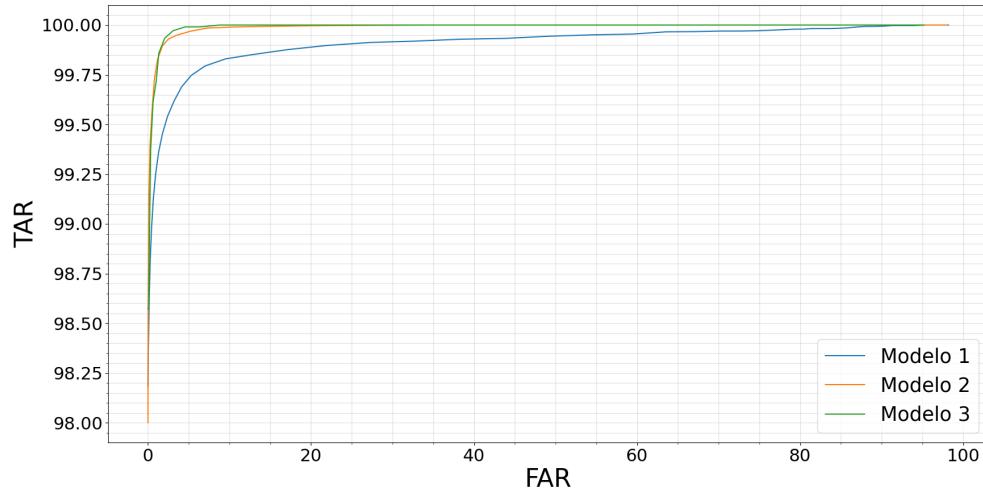


**Figura 4.15.** Variación del EER en función del número de muestras.

Por último, se ha comparado el rendimiento de los tres modelos mediante la curva ROC (*Receiver Operating Characteristic curve*). En ella se representa el FAR frente a TAR (*True Acceptance Rate*).

$$TAR = 1 - FRR$$

Esta curva es independiente del umbral y permite la comparación del rendimiento de diferentes sistemas bajo unas condiciones similares [38].



**Figura 4.16.** Comparación del rendimiento de los tres modelos con la curva ROC.

Como se puede apreciar en la Figura 4.16, el sistema con un peor rendimiento es el Modelo 1, en el que la curva no se acerca tanto a la esquina izquierda. Aún así, la curva obtenida para los tres modelos permite confirmar que puede realizarse la verificación de usuarios obteniendo buenos resultados con cualquiera de ellos.

## 5. Conclusiones

---

### 5.1. Conclusiones

Con este proyecto, se ha querido probar la fiabilidad que ofrece la actividad eléctrica del corazón registrada con el ECG como una característica biométrica, que permita tanto la identificación de usuarios, como su autenticación. Para ello, se ha diseñado un sistema basado en redes neuronales convolucionales (CNN), con las que se ha realizado una extracción de características, indicando quién es el usuario registrado más cercano, en el caso de la identificación, y obteniendo patrones biométricos, en el caso de la verificación de identidad.

Además, se ha evaluado el sistema implementado para ambas modalidades biométricas, haciendo uso de una base de datos especialmente diseñada para el reconocimiento de usuarios a través de su ECG. Esta base de datos incluye muestras de 105 usuarios registradas en dos sesiones diferentes para cada uno, separadas entre sí por un mínimo de una semana. En estas sesiones, se han llevado a cabo diferentes experimentos para el registro de la señal, incluyendo tomas en las que el usuario se encuentra sentado, de pie e, incluso, tomas realizadas después de someter al usuario a un ejercicio físico, acelerando el ritmo cardíaco hasta llegar a los 130 latidos por minuto. Con ello, hemos querido probar tanto la unicidad del ECG como característica biométrica, como su estabilidad.

En primer lugar, estas señales han sido sometidas a una fase de preprocesamiento, que incluye el filtrado de la señal, su segmentación basada en la detección de picos R, y la obtención de un vector formado por 8 complejos QRS concatenados. Este vector se ha utilizado como entrada (*input*) de una red neuronal, que ha permitido llevar a cabo el reconocimiento de usuarios.

En el caso de la identificación, se han realizado diferentes pruebas para un conjunto cerrado (*closed set*) de los usuarios de la base de datos. Por un lado, se ha demostrado que la identificación de 50 usuarios, cuyas tomas de ECG han sido registradas en dos sesiones diferentes, se puede conseguir con una exactitud del **97,58 %**. Además, si se evalúa el rendimiento del sistema con 55 usuarios cuyas tomas, además de haber sido registradas en dos sesiones diferentes, incluyen muestras en las que el usuario se encontraba tanto

sentado como de pie, y tanto en reposo como después de haber realizado deporte, la exactitud obtenida ha sido del **97,39 %**. Finalmente, la evaluación del sistema utilizando los 105 usuarios juntos, ha permitido demostrar la unicidad del ECG como característica biométrica, con un rendimiento del **95,59 %**. Esta disminución de la exactitud obtenida al aumentar el número de sujetos se ve condicionada, en parte, por una optimización de hiperparámetros menos que se ha realizado de manera menos exhaustiva que en el caso de los otros dos modelos.

En cuanto a la estabilidad del ECG para su uso en la identificación de usuarios, sí podemos confirmar que el rendimiento del sistema es muy elevado cuando ha sido entrenado con registros de diferentes días y bajo diferentes condiciones. Sin embargo, no hemos podido probar que el ECG sea una característica estable, pues el rendimiento del sistema ha disminuido notablemente cuando el entrenamiento se ha realizado con tomas registradas un día diferente al día de registro de las tomas utilizadas para su evaluación, siendo, además, el número de usuarios de la base de datos no excesivamente alto.

En el caso de la autenticación, la evaluación del sistema se ha realizado con usuarios diferentes a los utilizados para el entrenamiento de la red neuronal. De esta manera, ha sido posible verificar la identidad de 55 usuarios, cuyas muestras habían sido registradas incluyendo la condición del ejercicio, con un sistema entrenado sin este tipo de muestras, con un EER del **0,81 %**. Si además, el sistema sí es entrenado con muestras bajo esta condición, se consigue una mejora del rendimiento del sistema, obteniendo un EER de tan solo el **0,45 %**.

Estos resultados obtenidos para ambas modalidades, nos permiten confirmar que el ECG se puede utilizar para el reconocimiento biométrico con un rendimiento muy elevado, demostrando que esta novedosa técnica es potencialmente prometedora.

La comparación de los resultados obtenidos en este proyecto con otros estudios, basados también en redes neuronales, se puede observar en la siguiente Tabla 5.1.

Autor	Usuarios	Preprocesado	Método	Tasa de Identificación	EER de autenticación
Labati <i>et al.</i> [6]	52	Parcialmente-local	CNN	100 %	1,05
Zhang <i>et al.</i> [19]	18 a 47	Sin preprocesar	CNN	93,5 %	-
Zhang <i>et al.</i> [20]	18 a 47	Parcialmente-local	CNN	95 %	-
Pinto <i>et al.</i> [21]	1019	Sin preprocesar	CNN	-	7,86 %
Pinto <i>et al.</i> [22]	1019	Sin preprocesar	CNN	96,1 %	-
Salloum <i>et al.</i> [23]	47	Parcialmente-local	RNN	100 %	0 %
Sistema propuesto	105	Parcialmente-local	CNN	95,59 %	0,45 %

**Tabla 5.1.** Comparativa de estudios existentes basados en redes neuronales para la identificación y autenticación biométrica a través del ECG.

Por último, cabe destacar el bajo coste computacional que requiere tanto la fase de identificación como la fase de consulta de la verificación de la identidad. Para la implementación de este estudio, se ha utilizado un ordenador portátil con un procesador Intel(R) Core(TM) i7-8550U CPU de 1,8GHz, con una RAM de 12 GB. El tiempo de identificación de cada muestra ha sido de 0,478 ms y el tiempo para la comparación de patrones en autenticación ha sido de 0,609 ms para cada consulta. Estos valores tan bajos, permiten que estos sistemas se puedan llegar a emplear en escenarios reales para el reconocimiento biométrico.

## 5.2. Lineas futuras

En esta sección, presentamos posibles líneas futuras de trabajo que podemos introducir gracias a este proyecto:

- Mejorar el rendimiento del sistema de identificación cuando aumenta el número de usuarios registrados, llevando a cabo una búsqueda más exhaustiva de hiperparámetros del modelo.
- Diseñar y desarrollar un sistema de identificación de usuarios de un conjunto abierto (*open set*). Para ello, bastaría con determinar un umbral en el sistema implementado en este proyecto, que permitiera clasificar al usuario como no registrado, cuando la probabilidad de pertenecer a una de las clases registradas no sea en ningún caso superior a dicho umbral.
- Implementar un sistema basado en redes neuronales convolucionales con una fase de preprocessado menos compleja, que permita el reconocimiento de usuarios a partir de fragmentos de las señales de ECG, sin la necesidad de ser segmentadas en base a la detección de picos R.
- Demostrar la estabilidad del ECG como característica biométrica para ambas modalidades, consiguiendo una mejora del rendimiento del sistema cuando se trabaja con muestras registradas en diferentes sesiones y bajo diferentes condiciones. Para ello, se podría implementar una base de datos multisessión propia, que incluya tomas de diferentes días y horas, además de diferentes situaciones que generen alteraciones del ritmo cardíaco del usuario (actividades deportivas, pruebas de estrés, etc).



# Anexo I: Calidad de las clasificaciones obtenidas en identificación

## A.1. Base de datos 1

	precision	recall	f1-score	support		precision	recall	f1-score	support
1	0.96	1.00	0.98	24	26	1.00	1.00	1.00	24
2	0.92	1.00	0.96	24	27	1.00	0.96	0.98	24
3	1.00	1.00	1.00	24	28	1.00	1.00	1.00	24
4	1.00	1.00	1.00	24	29	0.62	0.54	0.58	24
5	1.00	1.00	1.00	24	30	1.00	1.00	1.00	24
6	1.00	1.00	1.00	24	31	0.96	1.00	0.98	24
7	1.00	1.00	1.00	24	32	1.00	1.00	1.00	24
8	0.96	1.00	0.98	24	33	0.59	0.67	0.63	24
9	1.00	1.00	1.00	24	34	1.00	1.00	1.00	24
10	1.00	1.00	1.00	24	35	1.00	1.00	1.00	24
11	1.00	1.00	1.00	24	36	1.00	0.92	0.96	24
12	1.00	1.00	1.00	24	37	1.00	1.00	1.00	24
13	0.96	1.00	0.98	24	38	1.00	1.00	1.00	24
14	1.00	0.96	0.98	24	39	0.96	0.96	0.96	24
15	1.00	1.00	1.00	24	40	1.00	1.00	1.00	24
16	1.00	1.00	1.00	24	41	1.00	1.00	1.00	24
17	1.00	0.96	0.98	24	42	1.00	1.00	1.00	24
18	1.00	1.00	1.00	24	43	1.00	1.00	1.00	24
19	1.00	1.00	1.00	24	44	1.00	1.00	1.00	24
20	1.00	1.00	1.00	24	45	1.00	1.00	1.00	24
21	1.00	1.00	1.00	24	46	0.96	0.92	0.94	24
22	1.00	0.96	0.98	24	47	0.96	1.00	0.98	24
23	1.00	1.00	1.00	24	48	1.00	1.00	1.00	24
24	0.96	1.00	0.98	24	49	1.00	0.96	0.98	24
25	1.00	1.00	1.00	24	50	1.00	1.00	1.00	24

**Tabla A.1.** Calidad de las clasificaciones obtenidas para cada usuario de la primera base de datos.

## A.2. Base de datos 2

	precision	recall	f1-score	support		precision	recall	f1-score	support
51	1.00	1.00	1.00	27	80	0.97	1.00	0.99	33
52	0.96	0.96	0.96	27	81	1.00	1.00	1.00	29
53	0.96	1.00	0.98	24	82	0.92	0.92	0.92	26
54	1.00	1.00	1.00	26	83	0.97	1.00	0.98	30
55	1.00	1.00	1.00	30	84	1.00	1.00	1.00	37
56	1.00	0.90	0.95	30	85	0.97	0.93	0.95	30
57	1.00	1.00	1.00	30	86	1.00	1.00	1.00	25
58	1.00	1.00	1.00	30	87	0.92	0.96	0.94	25
59	0.93	0.97	0.95	29	88	0.97	1.00	0.98	30
60	1.00	1.00	1.00	26	89	1.00	1.00	1.00	33
61	0.96	0.92	0.94	26	90	1.00	0.97	0.98	31
62	0.88	0.92	0.90	25	91	0.96	1.00	0.98	26
63	1.00	1.00	1.00	25	92	0.97	1.00	0.99	38
64	1.00	0.97	0.98	30	93	0.97	0.93	0.95	30
65	1.00	0.92	0.96	36	94	0.79	0.93	0.85	28
66	1.00	0.97	0.98	32	95	0.96	0.96	0.96	25
67	0.94	0.92	0.93	37	96	1.00	0.93	0.96	29
68	1.00	1.00	1.00	26	97	0.91	0.97	0.94	32
69	1.00	1.00	1.00	28	98	1.00	0.97	0.98	29
70	1.00	1.00	1.00	35	99	1.00	1.00	1.00	31
71	0.96	0.96	0.96	25	100	0.90	1.00	0.95	26
72	1.00	0.96	0.98	27	101	0.95	0.95	0.95	38
73	1.00	0.96	0.98	28	102	1.00	1.00	1.00	24
74	1.00	1.00	1.00	30	103	1.00	0.96	0.98	27
75	0.97	1.00	0.98	31	104	1.00	1.00	1.00	27
76	1.00	1.00	1.00	30	105	0.94	0.89	0.91	35
77	1.00	1.00	1.00	26					
78	0.96	1.00	0.98	25					
79	1.00	1.00	1.00	36					

**Tabla A.2.** Calidad de las clasificaciones obtenidas para cada usuario de la segunda base de datos.

### A.3. Base de datos completa

	Precisión	Exhaustividad	Valor F1	N.º de Muestras
<i>accuracy</i>			0,96	2811
<i>macro avg</i>	0,96	0,96	0,96	2811
<i>weighted avg</i>	0,96	0,96	0,96	2811

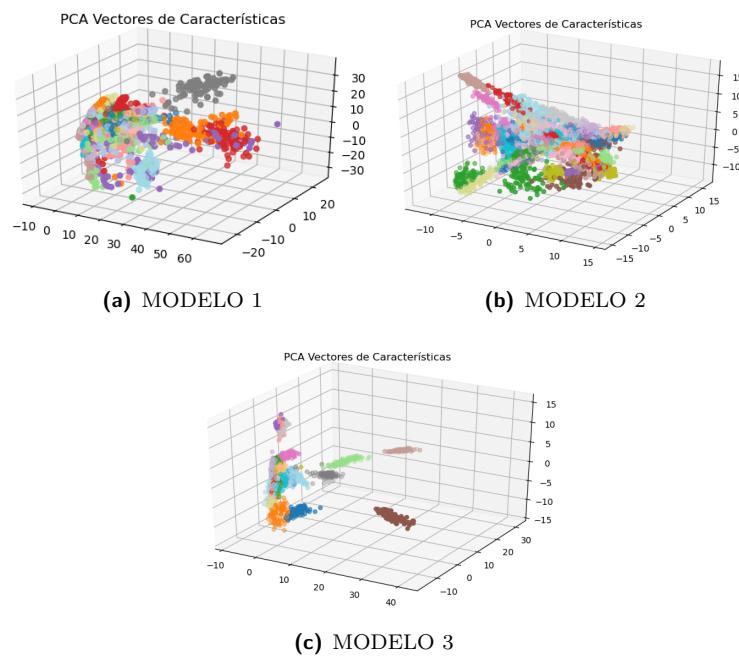
**Tabla A.3.** Calidad de las clasificaciones obtenidas para la base de datos completa.

	precision	recall	f1-score	support		precision	recall	f1-score	support		precision	recall	f1-score	support	
1	0.92	0.96	0.94	24		36	1.00	0.96	0.98	24	71	0.96	0.96	0.96	25
2	0.92	1.00	0.96	24		37	0.96	1.00	0.98	24	72	0.98	0.96	0.93	27
3	1.00	1.00	1.00	24		38	1.00	0.92	0.96	24	73	0.96	0.86	0.91	28
4	1.00	0.96	0.98	24		39	1.00	1.00	1.00	24	74	1.00	1.00	1.00	30
5	0.96	1.00	0.98	24		40	1.00	1.00	1.00	24	75	0.91	0.97	0.94	31
6	1.00	1.00	1.00	24		41	1.00	1.00	1.00	24	76	0.94	1.00	0.97	30
7	1.00	1.00	1.00	24		42	1.00	1.00	1.00	24	77	1.00	0.88	0.94	26
8	0.89	1.00	0.94	24		43	1.00	1.00	1.00	24	78	0.88	0.96	0.87	25
9	1.00	1.00	1.00	24		44	1.00	1.00	1.00	24	79	1.00	0.89	0.94	36
10	0.92	1.00	0.96	24		45	1.00	1.00	1.00	24	80	0.97	1.00	0.99	33
11	0.92	1.00	0.96	24		46	0.95	0.79	0.86	24	81	0.93	0.97	0.95	29
12	1.00	0.96	0.98	24		47	1.00	1.00	1.00	24	82	0.83	0.58	0.68	26
13	0.96	1.00	0.98	24		48	1.00	1.00	1.00	24	83	1.00	0.97	0.98	30
14	0.95	0.88	0.91	24		49	1.00	0.88	0.93	24	84	0.95	0.97	0.96	37
15	1.00	1.00	1.00	24		50	0.92	0.92	0.92	24	85	0.88	0.93	0.90	30
16	1.00	0.96	0.98	24		51	0.93	0.96	0.95	27	86	0.96	1.00	0.98	25
17	0.91	0.88	0.89	24		52	1.00	1.00	1.00	27	87	1.00	0.96	0.98	25
18	1.00	1.00	1.00	24		53	0.88	0.96	0.92	24	88	1.00	1.00	1.00	30
19	1.00	1.00	1.00	24		54	0.93	0.96	0.94	26	89	1.00	0.97	0.98	33
20	0.89	1.00	0.94	24		55	1.00	1.00	1.00	30	90	1.00	1.00	1.00	30
21	1.00	1.00	1.00	24		56	1.00	0.90	0.95	30	91	1.00	0.96	0.98	26
22	1.00	0.96	0.98	24		57	0.97	1.00	0.98	30	92	1.00	1.00	1.00	38
23	1.00	1.00	1.00	24		58	0.91	1.00	0.95	30	93	0.70	0.87	0.78	30
24	0.92	1.00	0.96	24		59	0.96	0.93	0.95	29	94	0.84	0.75	0.79	28
25	1.00	1.00	1.00	24		60	0.96	1.00	0.98	26	95	0.89	0.96	0.92	25
26	1.00	1.00	1.00	24		61	1.00	0.92	0.96	26	96	1.00	0.93	0.96	28
27	1.00	1.00	1.00	24		62	0.85	0.88	0.86	25	97	0.97	0.94	0.95	33
28	1.00	1.00	1.00	24		63	1.00	1.00	1.00	25	98	1.00	1.00	1.00	29
29	0.59	0.67	0.63	24		64	0.94	1.00	0.97	30	99	0.97	1.00	0.98	31
30	1.00	1.00	1.00	24		65	0.97	0.94	0.96	36	100	0.96	0.96	0.96	26
31	0.89	1.00	0.94	24		66	1.00	0.94	0.97	32	101	0.97	0.92	0.95	38
32	1.00	1.00	1.00	24		67	0.95	0.95	0.95	37	102	1.00	1.00	1.00	24
33	0.62	0.54	0.58	24		68	1.00	1.00	1.00	26	103	1.00	1.00	1.00	27
34	0.92	0.96	0.94	24		69	1.00	0.96	0.98	28	104	1.00	1.00	1.00	27
35	1.00	1.00	1.00	24		70	0.97	0.92	0.94	36	105	0.97	0.91	0.94	35

**Figura A.1.** Calidad de las clasificaciones obtenidas para cada usuario de la base de datos completa.

## Anexo II: Visualización de los vectores de características con la herramienta PCA

Si visualizamos los vectores de características obtenidos durante la fase de reclutamiento utilizando la herramienta PCA (análisis de componentes principales, ACP, en castellano), las agrupaciones por usuario, que veíamos bien definidas en el espacio con la herramienta TSNE, dejan de ser tan evidentes, y solo un reducido número de usuarios parece estar distanciado del resto.



**Figura B.1.** Comparativa de la distribución de los vectores de características obtenidos durante la fase de reclutamiento para cada modelo, empleando la herramienta de visualización PCA para reducir a tres dimensiones el espacio.

## **Anexo III: Aspectos éticos, económicos, sociales y ambientales**

---

En este proyecto se ha implementado un sistema biométrico a través del ECG. Los sistemas biométricos se aplican mayoritariamente en el ámbito de la seguridad y, actualmente, son utilizados en numerosas ocasiones para el control de acceso, al tratarse de características propias de cada persona, intransferibles y difíciles de falsificar. Por ejemplo, esta tecnología tiene un gran impacto en el control fronterizo, donde nuestra identidad es verificada, detectando posibles falsificaciones de documentos y contrastando nuestra información con las bases de datos disponibles en el control en relación a posibles antecedentes. En este sentido, ya se están implantando proyectos piloto en España donde el paso fronterizo se encuentra automatizado y se utilizan como rasgos para la verificación la cara y la huella dactilar (Automatic Border Crossing (ABC)) [42]; agilizando de esta manera los tiempos en los controles y aumentando su seguridad.

Otro ámbito en el que esta tecnología presenta un gran impacto es la banca, debido a la gran necesidad de aumentar la seguridad de sus operaciones, previniendo y evitando los fraudes en este sector. Hoy en día, la mayoría de las operaciones bancarias dependen de la autenticación de los usuarios basada en el uso de una gran cantidad de claves (contraseñas, firmas digitales, tockens...). Sin embargo, estos sistemas de autenticación son altamente vulnerable en comparación con los sistemas de autenticación biométrica. Por ejemplo, las transacciones a través de teléfonos móviles podrían beneficiarse de estos novedosos sistemas biométricos, verificando la identidad de los usuarios en todo momento a través de sus rasgos, difícilmente suplantables. La biometría junto a la tecnología NFC (Near Field Communication), presente en la gran parte de teléfonos móviles, es una de las aplicaciones con más futuro para garantizar la seguridad en las transacciones.

Si además tenemos en cuenta este nuevo enfoque del reconocimiento biométrico a través del ECG, nos encontramos con una mejora en el campo de la seguridad y el reconocimiento de usuarios, en comparación con la gran mayoría de modalidades existentes: la demostración de *la vida* de la persona en cuestión a través de la actividad eléctrica del corazón. De esta manera, haciendo uso de esta característica biométrica interna, frente a, por ejemplo, el uso del rostro o las huella dactilares, se dificulta todavía más la suplantación de la identidad, haciendo posible la detección de este tipo de ataques y mejorando significativamente la fiabilidad de los sistemas de seguridad.

En el aspecto medioambiental, este proyecto no presenta grandes impactos, aunque sí podría realizar pequeñas aportaciones en algunos sectores. Por ejemplo, los tockens y tarjetas identificativas de usuarios que encontramos en ciertas empresas, o incluso las tarjetas a modo de llaves en el sector hotelero, podrían verse suplantados por estos nuevos sistemas biométricos, eliminando un gasto asociados al uso de plásticos y su huella medioambiental.

Un aspecto muy destacable de los sistemas biométricos es su gran componente ético y social, debido al uso y almacenamiento de la información personal de los usuarios. En el mundo en el que vivimos, este uso de la información es considerado en muchas ocasiones, por las personas, una invasión a su privacidad, y observamos un miedo generalizado a ser etiquetados en todo momento, demandando cada vez más seguridad respecto al uso y custodia de los datos. Por ello, es muy necesario que se cumpla en todo momento con la regulación vigente y es muy necesario informar al usuario del sistema sobre la utilización de sus datos, realizándose siempre de manera legítima y en base a una buena política de seguridad a la hora del almacenamiento de los datos. Los datos biométricos se encuentran dentro de una categoría especial en el Reglamento de Protección de Datos en la Unión Europea (GDPR) y están sujetos a los mismos controles que aquellos datos personales que permiten revelar el origen étnico, las convicciones políticas, la orientación sexual, las opiniones políticas o el estado de la salud. Por ello, la identificación unívoca de un usuario sólo podrá realizarse cuando el usuario haya dado su consentimiento o por razones de interés público, siendo muy necesario combinar los desarrollos en estos sistemas con la regulación existente para poder aprovechar sus ventajas y a la vez asegurar a los ciudadanos la protección de su privacidad.

Por último, la siguiente Tabla C.1, muestra el presupuesto económico que ha supuesto el desarrollo de este trabajo.

<b>COSTE DE MANO DE OBRA (coste directo)</b>	<b>Horas</b>	<b>Precio/hora</b>	<b>Total</b>
	500	15 €	<b>7.500 €</b>
<b>COSTE DE RECURSOS MATERIALES (coste directo)</b>			
	<b>Precio de compra</b>	<b>Uso en meses</b>	<b>Amortización (en años)</b>
Ordenador portátil	1100,00 €	6	5
Licencia de código abierto Python	0,00 €	6	5
<b>COSTE TOTAL DE RECURSOS MATERIALES (CD)</b>			<b>7610€</b>
<b>GASTOS GENERALES (costes indirectos)</b>	13% sobre CD		<b>989,3 €</b>
<b>BENEFICIO INDUSTRIAL</b>	6% sobre CD+CI		<b>515,95€</b>
<b>SUBTOTAL PRESUPUESTO</b>			<b>9115,258 €</b>
<b>IVA APPLICABLE</b>	21%		<b>1914,20€</b>
<b>TOTAL PRESUPUESTO</b>			<b>11029,46 €</b>

**Tabla C.1.** Presupuesto económico.

## Bibliografía

---

- [1] N. Samarin and D. Sannella, “A Key to Your Heart: Biometric Authentication Based on ECG Signals,” 2019. [Online]. Available: <http://arxiv.org/abs/1906.09181>
- [2] R. Sanchez Reillo, “Uso del ECG para la autenticación de usuarios en transacciones remotas,” UC3M, Tech. Rep., 2018.
- [3] C. Carreiras, A. Lourenço, H. Silva, and A. Fred, “Evaluating Template Uniqueness in ECG Biometrics,” 2016.
- [4] F. Sufi, I. Khalil, and J. Hu, “ECG-Based Authentication,” *Handbook of Information and Communication Security*, pp. 309–331, 2010.
- [5] H. P. Da Silva, A. Fred, A. Lourenco, and A. K. Jain, “Finger ECG signal for user authentication: Usability and performance,” *IEEE 6th International Conference on Biometrics: Theory, Applications and Systems, BTAS 2013*, 2013.
- [6] R. Donida Labati, E. Muñoz, V. Piuri, R. Sassi, and F. Scotti, “Deep-ECG: Convolutional Neural Networks for ECG biometric recognition,” *Pattern Recognition Letters*, vol. 126, pp. 78–85, sep 2019.
- [7] L. Biel, O. Pettersson, L. Philipson, and P. Wide, “ECG analysis: A new approach in human identification,” *IEEE Transactions on Instrumentation and Measurement*, vol. 50, no. 3, pp. 808–812, 2001.
- [8] M. Kyoso and A. Uchiyama, “Development of an ECG identification system,” *Annual Reports of the Research Reactor Institute, Kyoto University*, vol. 4, no. December, pp. 3721–3723, 2001.
- [9] I. Odinaka, P. H. Lai, A. D. Kaplan, J. A. O’Sullivan, E. J. Sirevaag, and J. W. Rohrbaugh, “ECG biometric recognition: A comparative analysis,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1812–1824, 2012.
- [10] A. Eduardo, H. Aidos, and A. Fred, “ECG-based biometrics using a deep auto encoder for feature learning an empirical study on transferability,” *ICPRAM 2017 - Proceedings of the 6th International Conference on Pattern Recognition Applications and Methods*, vol. 2017-Janua, no. Icram, pp. 463–470, 2017.

- [11] S. A. Israel, J. M. Irvine, A. Cheng, M. D. Wiederhold, and B. K. Wiederhold, "ECG to identify individuals," *Pattern Recognition*, vol. 38, no. 1, pp. 133–142, 2005.
- [12] I. Jekova, V. Krasteva, and R. Schmid, "Human identification by cross-correlation and pattern matching of personalized heartbeat: Influence of ECG leads and reference database size," *Sensors (Switzerland)*, vol. 18, no. 2, 2018.
- [13] J. S. Arteaga-Falconi, H. Al Osman, and A. El Saddik, "ECG Authentication for Mobile Devices," *IEEE Transactions on Instrumentation and Measurement*, vol. 65, no. 3, pp. 591–600, 2016.
- [14] J. R. Pinto, J. S. Cardoso, A. Lourenço, and C. Carreiras, "Towards a continuous biometric system based on ECG signals acquired on the steering wheel," *Sensors (Switzerland)*, vol. 17, no. 10, pp. 1–14, 2017.
- [15] D. P. Coutinho, A. L. Fred, and M. A. Figueiredo, "ECG-based continuous authentication system using adaptive string matching," *BIOSIGNALS 2011 - Proceedings of the International Conference on Bio-Inspired Systems and Signal Processing*, no. January, pp. 354–359, 2011.
- [16] J. Li, Y. Si, T. Xu, and S. Jiang, "Deep Convolutional Neural Network Based ECG Classification System Using Information Fusion and One-Hot Encoding Techniques," *Mathematical Problems in Engineering*, vol. 2018, 2018.
- [17] B. Pyakillya, N. Kazachenko, and N. Mikhailovsky, "Deep Learning for ECG Classification," *Journal of Physics: Conference Series*, vol. 913, no. 1, 2017.
- [18] S. K. Kim, C. Y. Yeun, E. Damiani, and N. W. Lo, "A machine learning framework for biometric authentication using electrocardiogram," *IEEE Access*, vol. 7, pp. 94 858–94 868, 2019.
- [19] Q. Zhang, D. Zhou, and X. Zeng, "HeartID: A Multiresolution Convolutional Neural Network for ECG-Based Biometric Human Identification in Smart Health Applications," *IEEE Access*, vol. 5, pp. 11 805–11 816, 2017.
- [20] Q. Zhang and D. Zhou, "Deep Arm/Ear-ECG Image Learning for Highly Wearable Biometric Human Identification," *Annals of Biomedical Engineering*, vol. 46, no. 1, pp. 122–134, 2017.
- [21] R. Pinto and J. S. Cardoso, "An End-to-End Convolutional Neural Network for ECG-Based Biometric Authentication," *10th International Conference on Biometrics Theory, Applications and Systems (BTAS 2019)*, 2019.
- [22] R. S. Bhadoria, J. R. Pinto, J. S. Cardoso, and A. Lourenço, "Deep Neural Networks for Biometric Identification Based on Non-Intrusive ECG Acquisitions," *The Biometric Computing*, pp. 217–234, 2020.
- [23] R. Salloum and C.-C. J. Kuo, "ECG-BASED BIOMETRICS USING RECURRENT NEURAL NETWORKS Ronald Salloum and C . -C . Jay Kuo Ming Hsieh Department of Electrical Engineering University of Southern California , Los Angeles , CA," *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP) 2017*, pp. 2062–2066, 2017.
- [24] G. Van Rossum and F. L. Drake, *Python 3 Reference Manual*. CreateSpace, 2009. [Online]. Available: <https://www.python.org/>

- [25] T. E. Oliphant, *A guide to NumPy*. Trelgol Publishing USA, 2006, vol. 1. [Online]. Available: <https://numpy.org/>
- [26] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay, “Scikit-learn,” *Journal of Machine Learning Research*, vol. 12, no. 1, pp. 2825–2830, 2011.
- [27] F. Chollet and Others, “Keras,” 2015. [Online]. Available: <https://keras.io>
- [28] M. Abadi, A. Agarwal, P. Barham, E. Brevdo, Z. Chen, C. Citro, G. S. Corrado, A. Davis, J. Dean, M. Devin, S. Ghemawat, I. Goodfellow, A. Harp, G. Irving, M. Isard, Y. Jia, R. Jozefowicz, L. Kaiser, M. Kudlur, J. Levenberg, D. Mane, R. Monga, S. Moore, D. Murray, C. Olah, M. Schuster, J. Shlens, B. Steiner, I. Sutskever, K. Talwar, P. Tucker, V. Vanhoucke, V. Vasudevan, F. Viegas, O. Vinyals, P. Warden, M. Wattenberg, M. Wicke, Y. Yu, and X. Zheng, “TensorFlow: Large-Scale Machine Learning on Heterogeneous Distributed Systems,” 2016. [Online]. Available: <http://tensorflow.org/>
- [29] R. Kher, “Signal Processing Techniques for Removing Noise from ECG Signals,” *Jber*, vol. 3, pp. 1–9, 2019.
- [30] K. K. Patro and P. R. Kumar, “Machine learning classification approaches for biometric recognition system using ECG signals,” *Journal of Engineering Science and Technology Review*, vol. 10, no. 6, pp. 1–8, 2017.
- [31] Larisa G. Tereshchenko and Mark E. Josephson, “Frequency Content and Characteristics of Ventricular Conduction,” *Physiology & behavior*, vol. 176, no. 3, pp. 139–148, 2019.
- [32] N. M. Saad, A. R. Abdullah, and Y. F. Low, “Detection of heart blocks in ECG signals by spectrum and time-frequency analysis,” *SCORed 2006 - Proceedings of 2006 4th Student Conference on Research and Development Towards Enhancing Research Excellence in the Region*, no. February 2016, pp. 61–65, 2006.
- [33] D. Castells-Rufas and J. Carrabina, “Simple real-time QRS detector with the MaMe-Mi filter,” *Biomedical Signal Processing and Control*, vol. 21, pp. 137–145, 2015.
- [34] J. Pan and W. J. Tompkins, “A Real-Time QRS Detection Algorithm,” *IEEE Transactions on Biomedical Engineering*, vol. BME-32, no. 3, pp. 230–236, 1985.
- [35] The SciPy community, “scipy.signal.find\_peaks,” 2019. [Online]. Available: [https://docs.scipy.org/doc/scipy/reference/generated/scipy.signal.find\\_{\\_}peaks.html](https://docs.scipy.org/doc/scipy/reference/generated/scipy.signal.find_{_}peaks.html)
- [36] J. Torres, *Deep Learning Introducción Práctica con Keras*. Independently Published, 2018. [Online]. Available: <https://books.google.dk/books?id=E696uQEACAAJ>
- [37] L. Vandroux, “What are the non-trainable parameters of the model?” 2018. [Online]. Available: <https://github.com/experiencor/keras-yolo2/issues/167>
- [38] B. Tutorial and P. Editor, “ISO / IEC JTC 1 / SC 37,” *Biometrics*, 2007.
- [39] C. H. Javier Galbally, Julian Fierrez and J. K. Chan, Norman Poh, “Metrics for the evaluation of biometric performance,” BEAT, Tech. Rep., 2013.

- [40] N. Poh, C.-H. Chan, J. Kittler, J. Fierrez, and J. Galbally, “Description of Metrics For the Evaluation of Biometric Performance,” *Biometrics Evaluation and Testing (BEAT)*, pp. 1–22, 2012.
- [41] P. Jonathon Phillips, P. Grother, R. J. Michaelas, D. M. Blackburn, E. Tabassi, and M. Bone, “Face Recognition Vendor Test,” no. March, 2003.
- [42] European Cominision, “Automated Border Control (ABC).” [Online]. Available: <https://ec.europa.eu/home-affairs/what-we-do/networks/european{-}migration{-}network/glossary{-}search/automated-border-control-abc{-}en>