Universidad de las Américas Puebla

Escuela de Ingeniería

Departamento de Computación, Electrónica y Mecatrónica

Desarrollo de un sistema de autenticación basado en señales de electroencefalografía

Tesis que, para completar los requisitos del Programa de Honores, presenta el estudiante:

Diego Farias Castro

ID. 159918

Licenciatura en Ingeniería en Sistemas Computacionales

Directora de tesis: Dra. Rocío Salazar Varas

San Andrés Cholula, Puebla. Otoño, 2021

Agradecimientos y dedicatorias

Agradezco enormemente a mi directora de tesis: la Dra. Rocío Salazar Varas por otorgarme su confianza, comprensión, conocimiento e inigualable apoyo, tanto en realización de este proyecto, como en mi formación profesional. Sin su soporte y asistencia, las metas que hoy he alcanzado no serían más que simples aspiraciones.

De igual forma, agradezco a mis padres: Eugenio Farias Oropeza, María Guadalupe Castro Dávalos, y Justina Mora González, por incentivarme a la persecución de metas ambiciosas y gratificantes; por su respaldo incondicional, inagotable esfuerzo e incesante cariño.

Asimismo, agradezco a mis amigos y compañeros por su soporte y confidencia; a mis profesores, por su inefable paciencia y sabiduría, y a la Universidad de las Américas Puebla por otorgarme las oportunidades y herramientas necesarias para alcanzar mis objetivos.

Para concluir, agradezco infinitamente y dedico las labores desempeñadas en la realización de esta tesis a la memoria del Dr. Eugenio Farias Chávez, cuya última ilusión fuese vislumbrar la completitud de mi grado de Licenciatura.

Índice general

Índice de tablas

Fase I: Sistema de autenticación basado en una clase genérica

Fase II: Sistema de autenticación basado en fronteras

Índice de figuras

Lista de abreviaturas

BCI	Brain-Computer Interface
BOLD	Blood Oxygen Level Dependent
BSS	Blind Source Separation
CCD	Charge-Coupled Device
CMOS	Complementary Meta-Oxide Semiconductor
ECG	Electrocardiografía
EcoG	Electrocorticografía
EEG	Electroencefalografía
EMG	Electromiografía
ERBD	Esquema Relacional de Base de Datos
FA	False Accept
FAR	False-Acceptance Rate
fMRI	Functional Magnetic Resonance Imaging
fNIRS	Functional Near-Infrared Spectroscopy
FR	False Reject
FRR	False-Reject Rate
GDF	General Data Format for biomedical signals
GLDS-SVM	Generalized Linear Discriminant Sequence with kernel SVM
GMM-JFA	Gaussian Mixture Model with Join Factor Analysis
GMM-SVM	Gaussian Mixture Model with kernel Support Vector Machine
GMM-UBM	Gaussian Mixture Model with Universal Background Model
GUI	Graphical User Interface

ICA	Independent Component Analysis
ICASSP	International Conference on Acoustics, Speech and Signal Processing
ICC	Interfaz Cerebro-Computadora
ICE	Intracortical Electroencephalography
IFIPAICT	International Federation for Information Processing
IQR	Interquartile range
kNN	k-Nearest Neighbors
LDA	Linear Discriminant Analysis
MAD	Median Absolute Deviation
MEG	Magneto Encefalografía
MIT	Massachusetts Institute of Technology
MLP	Multi-Layer Perceptron
NIP	Número de Identificación Personal
PCA	Principal Component Analysis
SGBD	Sistema Gestor de Base de Datos
SVM	Support Vector Machine
TA	True Accept
TER	Total Error Rate
TGT	Ticket-Granting Ticket
TR	True Reject
TSR	Total Success Rate
UML	Unified Modeling Language
VQ-UBM	Vector Quantizer with Universal Background Model

Resumen

La autenticación biométrica, es un servicio de seguridad que permite constatar la identidad de un individuo con base en sus parámetros físicos o conductuales, para posteriormente brindar acceso a un recurso restringido. Esto, en contraposición con el tradicional uso de contraseñas o llaves físicas. Algunos ejemplos comúnes son el análisis de huella digital, el reconocimiento de voz, iris y retina. Dichas soluciones, destacan por su efectividad, que ronda entre 80.37% y 99.99%, así como su eficiencia i.e., requiriendo menos de 35 segundos para registrar y/o autenticar a un usuario. No obstante, pese a su desempeño, estas soluciones son vulnerables a intentos de suplantación e.g., el análisis de huella es suceptible a señuelos de silicona, el reconocimiento de voz a imitadores y el análisis de iris y retina a fotografías.

La actividad cerebral, por su parte, figura como una alternativa segura, pues dicho parámetro es único entre individuos, escasamente replicable, y difícilmente procesado por atacantes poco experimentados. Así pues, a largo de esta tesis, se condujo un estudio de 3 fases que tuvo por objetivo la fabricación de un sistema de autenticación basado en señales de electroencefalografía competente tanto eficaz como eficientemente con otras alternativas.

En la primera fase se identificaron las frecuencias de corte ideales para filtrar una señal cerebral. Con ellas, se emuló un escenario de autenticación empleando un clasificador de Bayes. En la segunda, se definió una metodología de validación de identidad basada en fronteras de *likelihood* y correlación de Pearson y se realizaron diversos ajustes a ésta e.g., combinaciones de características o sesiones de entrenamiento, para añadirle robustez ante la variabilidad de las señales con el tiempo, así como para hacerla aplicable a un entorno real. Finalmente en la tercera fase se implementó un aplicativo basado en esta metodología.

Palabras clave: *autenticación, EEG, descriptores estadísticos, extracción de características*

1. Introducción

La *autenticación* es un *servicio* fundamental para la seguridad informática que tiene por objetivo validar la identidad de un individuo que pretende acceder a un sistema restringido o contenido de carácter confidencial (Paul, Baras y Sadler, 2008). Para ello, existen tres posibles aproximaciones: por *conocimiento* e.g., de una contraseña textual o patrón gráfico, por *posesión* e.g., de una tarjeta inteligente, o por *biometría* e.g., mediante huellas digitales o análisis de la dinámica de pulsación de teclas (Velásquez, Caro, y Rodríguez, 2017). Esta última, denominada autenticación biométrica, pretende constatar la identidad de un sujeto con base en sus parámetros *físicos* o *conductuales*. (Barton, Byciuk, Harris, et al., 2005).

Cualquier sistema de autenticación fundamentado en la biometría emplea la similitud entre una muestra dada durante la inscripción al sistema y una proporcionada al reingresar al mismo como factor decisivo. Si éstas mantienen un grado de concordancia suficiente, el acceso será concedido. De lo contrario, se intuirá que el sujeto es un impostor y se denegarán los recursos solicitados. En esta metodología, a diferencia de la solicitud de contraseñas u objetos físicos que certifiquen la identidad i.e., por *posesión* o *token*, no es posible lograr la unicidad entre las muestras, dadas las variaciones corporales que se presentan a lo largo del tiempo. Por ello, es necesario establecer márgenes de error permitidos entre lo almacenado al momento de registro y las condiciones observadas al ingreso. Inherentemente, si el margen de error es reducido, cabe la posibilidad de que aún los sujetos autorizados sean rechazados, lo que derivará en inaccesibilidad a los recursos protegidos. Si, por el contrario, el margen es amplio, podría concederse el ingreso a farsantes, comprometiendo la seguridad del sistema.

Esta metodología de autenticación ha evolucionado sustancialmente, popularizándose y diversificándose al grado de ser, hoy en día, prácticamente un estándar de las tecnologías

emergentes. Algunos ejemplos son el análisis de la huella digital, mano o geometría de la palma, escaneo de retina e iris, mapeo facial, análisis del estilo del manuscrito, la dinámica de firmado, el reconocimiento de voz (Maltoni, Maio, Jain, y Prabhakar, 2009), identificación de patrones venales o de la marcha, análisis de señales de electro-oculografía, entre otros (Jiang, Al-Maadeed, Bouridane, et al., 2017).

Las alternativas de autenticación biométricas actualmente disponibles gozan de una efectividad bastante elevada, que ronda entre 80.37% y 99.99% (Shelupanov, Evsyutin, Konev, et al., 2019), (Sluganovic, Roeschlin, Rasmussen, et al., 2016). Esto, con apenas una porción de datos al registro e ingreso. (Arteaga-Falconi, Al Osman, y El Saddik, 2015), por ejemplo, plantearon un sistema de autenticación basado en electrocardiografía o ECG que acepta erróneamente a un sujeto en apenas 1.29% de los casos. Lo anterior, requiriendo solo 30 segundos de datos útiles i.e., de 2 min disponibles, para el registro de usuarios. Por su parte (Sluganovic, Roeschlin, Rasmussen, et al., 2016) exponen cómo algunos de sistemas de autenticación biométricos basados en movimientos oculares demoran en promedio 35 segundos para autenticar a un usuario. Esto, con una tasa de error promedio $\leq$19.63%.

No obstante, pese a su popularidad, desempeño óptimo y constante evolución, algunas de éstas soluciones albergan vulnerabilidades subyacentes casi irrevocables que exponen los recursos protegidos incluso a atacantes poco experimentados e.g., el análisis de huellas dactilares, es suceptible a señuelos de silicona fácilmente desarrollables (Keuning y Van der Putte,2005), el reconocimiento por voz puede ser burlado, tanto por imitadores (Lau, Wagner y Tran, 2004), como por grabaciones (Kinnunen, Wu, Lee, Sedlak, Chng, y Li, 2012), y, el escaneo de retina puede ser sobrepasado con fotografías simples impresas con dispositivos comerciales (Ruiz-Albacete, Tome-González, Alonso-Fernández, Galbally, Fierrez, 2008).

La actividad cerebral por su parte, pareciera ser una alternativa segura, pues dicho parámetro no sólo es único entre individuos (Miller y Donovan, 2009), sino que además, al no ser de naturaleza física es escasamente replicable. Esto sin mencionar que su análisis y procesamiento es una labor compleja que dificilmente puede ser efectuada por atacantes poco capacitados y que algunas investigaciones previas en este ámbito, e.g., las de (Ashby, Bhatia, Tenore, y Vogelstein, 2011) y (Khalifa, Salem, Roushdy y Revett, 2012) han sido exitosas al utilizar la actividad cerebral, recopilada mediante electroencefalografía como método de autenticación. Así pues surge la interrogante: ¿es posible fabricar un sistema de autenticación biométrico basado en señales de electroencefalografía que sea competente con alternativas existentes en términos de eficacia y eficiencia, pero que en añadidura permita minimizar las vulnerabilidades antedichas dadas sus características inherentes?

Para responder a dicha interrogante, que se presume es cierta, se efectuará una estudio de tres fases denominadas: *autenticación mediante una clase genérica*, *autenticación basada en fronteras* y *elaboración de un software de aplicación.* En la primera, se identificarán las bandas de frecuencia ideales para filtrar una señal EEG dada una tarea mental específica y, con ellas, se efectuará un intento de autenticar usuarios dividiéndolos en dos clases: *cliente* i.e., el usuario al que pertenece un recurso y *genérica* i.e., el resto de individuos. Estos, serán identificados con un clasificador Gaussiano ingenuo de Bayes. En la segunda fase se rescindirá el uso de esta metodología y se planteará un nuevo paradigma de autenticación basado en dos fronteras, una de correlación producto-momento de Pearson y otra de *likelihood.* Estas, deberán ser superadas por un sujeto entrante para calificarlo como cliente o impostor. Finalmente, en la fase III se fabricará un aplicativo basado en el patrón de diseño Model-View-Controller que, explotando las librerías *brainflow*, *tkinter* y *threading* de

Python 3 brindará el servicio de autenticación a un público general, explotando el modelo desarrollado en la fase II. Para lograr el objetivo de generar una solución competente, dicho aplicativo, deberá tener una efectividad igual o superior al antedicho mínimo de 80.37% y demorar menos de 35 segundos para autenticar a un sujeto.

2. Justificación

A pesar del proceso evolutivo y expansivo que han tenido las metodologías de autenticación biométrica en existencia, éstas poseen aún numerosas vulnerabilidades que, si bien se han minimizado, no se han logrado ni se lograrán erradicar dado su diseño conceptual. Tome, por ejemplo, el uso de la huella digital. Este mecanismo de seguridad, pese a la creencia popular, no analiza la estructura dactilar completa de un individuo. En su lugar, se identifican únicamente patrones en las crestas de la misma, las cuales suelen presentar discontinuidades, bucles o bifurcaciones denominadas *minucias*. (Keuning y Van der Putte,2005).

Si bien, dada la anatomía dactilar es posible observar centenares de estas variaciones, los escáneres de alta resolución, como los utilizados por agencias de justicia europeas, sólo consideran un total de 12 minucias, mientras que los dispositivos comerciales pueden únicamente reconocer un promedio de 8. (Keuning y Van der Putte, 2005). Esto garantiza, de acuerdo con sus fabricantes, un FAR i.e., False Acceptance Rate, de uno por cada millón de autenticaciones, una tasa ciertamente destacable. Es importante mencionar, sin embargo, que estas cifras se han logrado a partir de un sinfín de mejoras implementadas desde su lanzamiento en los años 80s, siendo ejemplos de estas la incorporación de sensores ultrasónicos, de temperatura, capacitivos y ópticos mediante cámaras CCD o CMOS entre otras tecnologías. (Xia y O'Gorman,2003).

Así pues, los estadísticos sugieren que esta tecnología es prácticamente inmune a confusiones, i.e., aceptar la huella de un individuo por otro. Sin embargo, existe un abismo exorbitante entre un fallo accidental del sistema, como el que plantean las cifras, y uno inducido, en el cual un atacante intenta suplantar al usuario acreditado. Es en este punto en el que el sistema pierde su enaltecida fidelidad. De acuerdo con Ton van der Putte y Jeroen Keuning en su contribución a la serie de libros de la *International Federation for Information Processing* (IFIPAICT) estos mecanismos pueden ser fácilmente engañados por medio de réplicas, las cuales son fabricables aún sin la cooperación del usuario certificado.

Sólo se requiere que la víctima deje plasmada su huella sobre cualquier superficie, incluida la lente del escáner con que se efectúa la autenticación. Eventualmente, un atacante entrenado podría emplearla como prototipo para generar un señuelo de silicona, el cual puede colocarse sobre el dedo de cualquier individuo y utilizarse para burlar al sistema. Es importante mencionar que, a pesar de la aparente complejidad de esta metodología, no se requieren procesos de larga duración, es posible con medios limitados y peor aún, es una medida imperceptible tanto por filtros de seguridad humanos como automatizados.

En las últimas décadas, se ha intentado combatir dicha vulnerabilidad por medio de diversos análisis de la epidermis, con los cuales, se pretende discrepar entre la presencia de una capa de piel humana sobre el sensor o un replicado de silicona. Una manera de llevar a cabo dicha discriminación es mediante la temperatura. En promedio, un dedo humano se encuentra entre 8 y 10 grados Celsius por encima de la temperatura ambiental. (Keuning y Van der Putte, 2005). Si bien la silicona causa una disminución de casi dos grados, al usar un señuelo con el grosor de una oblea, la variación aún sería aceptada. Esto generalmente ocurre dado que, diversos sensores como los de un teléfono celular, incorporan la

funcionalidad en exteriores, ampliando su espectro de aceptación. Ahora bien, es importante mencionar que dicho factor, no exime de riesgo a aquellos de uso restringido a interiores.

Adicionalmente, algunos escáneres de huella pretenden hacer la discriminación con un señuelo por medio de un análisis de conductividad, aunque dicho parámetro de filtrado es prácticamente inútil ante un atacante experimentado. (Matsumoto,2002). Si bien, la conductividad normal de un dedo es de aproximadamente 200KΩ (Keuning y Van der Putte, 2005), esta puede variar de forma radical. La temperatura a la que se ha expuesto la mano del usuario o incluso, la presencia de agua o sudor sobre ella, puede causar una fluctuación significativa. Por ello, los sensores de conductividad se ven forzados a dar espectros tan altos que unas simples gotas de saliva sobre la silicona serían suficientes para vulnerarlo.[1]

Finalmente, algunos sensores de huella han intentado reconocer el ritmo cardiaco del usuario y emplearlo como factor decisivo ante un señuelo, asumiendo que tal movimiento será imperceptible al ubicar una pieza de silicona sobre el dedo del atacante. Esto, cabe mencionar, no sólo resulta ineficiente sino además inútil para evitar la suplantación. Dadas las variaciones que pueden ocurrir en este parámetro como resultado de la agitación física del sujeto al momento de ingresar al sistema, los espectros de aceptación nuevamente son elevados, derivando así en la misma vulnerabilidad que representa el análisis conductivo. Dada la finura de la réplica de silicona y el antedicho margen de error elevado, el ritmo cardíaco del atacante podría ser igualmente identificado por el escáner (Keuning y Van der

[1] En una revisión de vulnerabilidades publicada por la Universidad Nacional de Yokohama se detectó, adicionalmente que, señuelos fabricados con caucho de silicona rellenados con carbón negro eléctricamente conductivo en 12%-16% han logrado vulnerar sin complicaciones los sistemas de análisis de conductividad. (Matsumoto, 2002).

Putte,2005). Con ello, es posible concluir que el paradigma de protección biométrica por huella digital es inseguro, dada la susceptibilidad de éste al engaño por réplicas de silicona.

La identificación del iris, por su parte, es una metodología de carácter más reciente, la cual, ha ganado una popularidad exorbitante gracias a la efectividad en sus algoritmos de identificación de usuarios. Aunque, pese a dichos resultados favorables en condiciones operativas estándar, diversas vulnerabilidades han sido expuestas. Un ejemplo de ello es proporcionado por Thalheim, Krissier y Zlegter, investigadores del departamento de ciencia computacional teórica e ingeniería de software de la *Technische Universität Berlin*. Su metodología experimental consistió en registrar a un sujeto ante un analizador de iris casero BM-ET100. Posteriormente se fotografió el ojo de los sujetos y se efectuó una impresión con calidad de imagen de 2400x1200 dpi. A esta, le fue realizado un corte en una porción del ojo. Posteriormente, otro individuo colocó el papel frente a su iris, de modo que la imagen fuese complementada adecuadamente. A pesar de dicha manipulación, el sistema concedió el acceso. Una vez logrado dicho resultado, se repitió el experimento probando con múltiples impostores. La conclusión obtenida fue que cualquier individuo que poseyera el patrón impreso podría suplantar al usuario registrado. (Thalheim, Krissier y Zlegter,2004)

Otro ejemplo de vulnerabilidad en este sistema biométrico es proporcionada por un estudio colaborativo entre miembros de la universidad de Halmstad, la Universidad Autónoma de Madrid, la Comisión Europea y el Instituto de Investigación Idlap. En este, se recopilaron muestras de 27 sujetos. Subsecuentemente, se generaron iris sintéticos de cada uno de los participantes, las cuales pasaron por un preprocesamiento basado en ecualización de histogramas y filtrado de ruido, para finalmente imprimirse en una pieza de papel estándar

con los dispositivos comerciales HP Deskjet 970cxi y HP LaserJet 4200L. (Ruiz-Albacete, Tome-González, Alonso-Fernández, Galbally, Fierrez, 2008).

El ataque consistió en registrar a un usuario empleando su iris auténtico para posteriormente, intentar el acceso mediante la impresión. Los resultados de esta prueba fueron contundentes, obteniendo rangos de efectividad entre las diversas rondas experimentales que fluctuaban entre 49.32% y 73.30%. (Ruiz-Albacete, Tome-González, Alonso-Fernández et al., 2008). Con ello, es posible afirmar que, si bien las imágenes fraudulentas recibieron un procesamiento con diversas metodologías de retoque, existe un riesgo probabilísticamente innegable al continuar usando dicho paradigma de autenticación.

Para concluir con el proceso de revisión de algunas alternativas biométricas populares, es menester analizar el caso del reconocimiento de voz, el cual se encarga de "aceptar o rechazar la identidad con base en una muestra del habla" (Kinnunen, Wu, Lee, et al., 2012). La discreción de este dispositivo, aunado a su potencial de error limitado lo ha convertido en una alternativa con gran aceptación pública, tornándolo en la metodología de autenticación para bancos, accesos a bases de datos e incluso para controles de seguridad de información confidencial (Lau, Wagner y Tran, 2004). Sin embargo, en diversas exploraciones académicas, se ha determinado que, pese a su popularidad, esta tecnología es de igual forma vulnerable ante fallos inducidos por atacantes experimentados.

Un primer ejemplo de ello, es provisto por un estudio desarrollado en la universidad de Canberra en Australia y presentado en el *International Symposium on Intelligent Multimedia, Video and Speech Processing*, 2004. En este, se recopiló una muestra de 138 sujetos, a los cuales se les solicitó inscribirse en un sistema de autenticación por reconocimiento de voz empleando secuencias de tres números, cada uno de dos dígitos.

Posteriormente, se contrataron imitadores con baja experiencia para analizar el FAR del sistema. Se estableció un margen de error del 0.5% y se solicitó a los participantes replicar la voz de los usuarios autorizados. El ataque de uno de los imitadores resultó exitoso en 6 de 40 intentos, arrojando un FAR de 30%. En condiciones similares, otro imitador logró un FAR de 35%. (Lau, Wagner y Tran, 2004). Con ello, es posible vislumbrar que, un simple mimetismo es suficiente para vulnerar un sistema de reconocimiento de voz, tornándolo así en una alternativa igualmente riesgosa para la protección de información altamente confidencial, tal y como se ha observado en otras metodologías biométricas.

Un estudio más reciente confirma la declaración anterior y, demuestra que estas vulnerabilidades aún persisten en múltiples sistemas de autenticación por voz. Los resultados de dicho experimento fueron presentados en el 2012 *IEEE International Conference on Acoustics, Speech and Signal Processing* (ICASSP), evidenciando el riesgo latente de intrusión al sistema a través de una grabación de la voz del usuario autentificado. Para ello, se realizaron 6,760 intentos de acceder al sistema, de los cuales 3,978 fueron genuinos y 2,782 falsos. Las pruebas se realizaron contra diversos estándares, como GMM-UBM, VQ-UBM, GLDS-SVM, GMM-SVM y GMM-JFA. Como resultado, se obtuvieron FAR mínimos de 7.63%, 7.56%, 7.16%, 3.75% y 3.24%; mientras, los máximos se situaron en 21.07%, 19.16%, 17.15%, 10.81% y 6.30% respectivamente (Kinnunen, Wu, Lee, Sedlak, Chng, y Li, 2012). En dicha información, es posible apreciar que, aun con el mínimo coeficiente de fallo 3 de cada 100 muestras resultarán en un FAR y, en el peor de los casos 1 de cada 5 derivarán en una aceptación falsa. Por tanto, es posible concluir que, este sistema de autenticación biométrico, tampoco se perfila como una alternativa segura.

Como se ha podido observar, las herramientas de autenticación biométricas más populares poseen hoy en día un desperfecto inevitable que, como se ha mencionado con anterioridad, radica en la necesidad de elementos físicos, o de fácil intercepción por atacantes externos. A diferencia de dichas metodologías, las autenticación basada en interfaces cerebro-computadora, que emplean como factor decisivo la actividad electroencefalográfica o EEG, parecieran ser una solución factible. Tal aseveración se sustenta, en primera instancia, en la investigación de (Miller y Donovan, 2009) titulada *unique and persistent individual patterns of brain activity across different memory retrieval tasks,* en la que se prueba la unicidad de las ondas cerebrales entre individuos.

De igual forma, dicha propuesta se sustenta en el hecho de que al no depender de elementos tangibles, el riesgo de señuelos es inherentemente nulo. Esto, en contraposición con lo observado en el análisis previo de la metodología basada en huella digital e iris. Adicionalmente, la propuesta de emplear dicha actividad como método de autenticación se fundamenta en el hecho de que la complejidad en el proceso de recopilación y análisis de señales EEG es inherentemente elevado. Lo anterior, en contraste con el reconocimiento por voz, cuyas ondas, son fácilmente replicadas o interceptadas por dispositivos comerciales como teléfonos celulares (Kinnunen, Wu, Lee, Sedlak, Chng, y Li, 2012).

En añadidura, es menester indicar que en la exploración previa se han destacado técnicas pasivas para suplantar al usuario y obtener acceso ilegítimo a un recurso aunque, de acuerdo con (Barton y Harris, 2005), existe de igual forma un riesgo latente de que el usuario sea forzado a través de la agresión física a proporcionar sus credenciales biométricas o bien, en casos más extremos, que se obtengan mediante amputación. En la solución propuesta, dicha amenaza es a futuro evitable. El departamento de ciencia computacional e ingeniería

informática de la universidad Da-Yeh en Taiwan destacó que existen un total de 8 tipos de emociones positivo-negativas: alegría, enfado, protección, tristeza, sorpresa, miedo, satisfacción y despreocupación, que son identificables mediante electroencefalografía.

En las pruebas realizadas por dicha institución, se empleó estimulación acústica para desencadenar dichas emociones. Posteriormente, se efectuó una recopilación de señales EEG de la zona del lóbulo frontal y se transformó la información a dominio de frecuencia para categorizar y calcular cada banda de potencia. Con ello, se logró identificar que las emociones antedichas no sólo son apreciables en un sujeto, sino que además es posible caracterizarlas por amplitud. Con esta información, la metodología propuesta podría a futuro detectar las variaciones en la actividad neuronal derivadas de la manipulación o extorsión y negar el acceso a un recurso o solicitar subyacentemente el auxilio de terceros.

Así pues, tras haber identificado las potenciales ventajas de este paradigma y la inexistencia de alternativas conceptualmente seguras se torna relevante y justificable pretender la fabricación de un sistema de autenticación biométrico basado en señales electroencefalográficas que sea competente con las alternativas existentes en términos de eficacia y eficiencia, pero que en añadidura permita minimizar las vulnerabilidades presentadas con anterioridad dadas sus características inherentes.

3. Objetivos

El objetivo general de esta tesis es fabricar de un sistema de autenticación biométrico basado en una interfaz cerebro-computadora, capaz de extraer características relevantes de las señales electroencefalográficas de un individuo, recopiladas durante la realización de diversas tareas mentales predefinidas. Como se ha mencionado, el antedicho sistema deberá ser efectivo y eficazmente comparable con otras soluciones, destacando entre ellas por su

robustez ante la personificación. Así pues, el sistema fabricado deberá ofrecer un desempeño $\geq 80.37\%$ y, por cuestiones de usabilidad, el tiempo requerido para registrar y autenticar un usuario deberá ser inferior a 35 segundos. La completitud del antedicho objetivo general require a su vez la satisfacción de los objetivos particulares subsecuentes:

1. Identificar las características y bandas de frecuencia ideales para autenticación.
2. Plantear un protocolo de adquisición de señales EEG y una política de seguridad que determinará el acceso o rechazo de un sujeto.
3. Ejecutar un análisis de desempeño.
4. Elaborar un esquema relacional de bases de datos, cuya implementación en un sistema de gestión de bases de datos permita almacenar e indexar convenientemente la información de los usuarios y sus respectivas señales electroencefalográficas para su consulta y actualización.
5. Diseñar una interfaz capaz de estimular la realización de tareas mentales y de recopilar la actividad electroencefalográfica derivada.

A cada objetivo particular previo, se asocian, respectivamente, las metas subsiguientes:

1. La completitud del primer objetivo particular requiere de un análisis por fuerza bruta de diversas frecuencias de corte. Con base en dicha exploración y, a modo de resumen, es necesario presentar el siguiente entregable: una lista de bandas de frecuencia tanto generales i.e., aplicables a todos los usuarios, como específicas i.e., de cada usuario. Asímismo, es mandatorio analizar la efectividad del sistema de autenticación empleando diferentes características. Como resultado, al concluir dicho experimento debe presentarse una lista de funciones potencialmente útiles, cuyo sustento debe basarse en una tabla con efectividades que denote un desempeño $\sim$80-

90% tras su extracción. Para este análisis se emplea el *dataset* IIb*,* de la tercera edición de la competencia de ICC de la *Technische Universität Graz*, cuyos detalles se presentan en secciones subsecuentes.

2. La satisfacción del segundo objetivo implica la presentación de una tabla de efectividad donde se indiquen las actividades mentales realizadas y su evidente utilidad i.e., ~85-90% como mínimo, en el proceso de autenticación. En añadidura a lo anterior, se debe indicar por escrito: el número de muestras requeridas para registrar a un usuario, las condiciones de adquisición de señales e.g., electrodos, la cantidad de experimentos por sesión, número de sesiones requeridas y su periodicidad, etc., así como la política bajo la cuál se concede acceso a un recurso.
3. Para llevar a cabo la satisfacción del tercer objetivo particular, se debe compilar una nueva base de datos con señales EEG de al menos 4 sujetos. En su elaboración es preciso seguir el protocolo de adquisición, filtrado y extracción de características definido con anterioridad. El sistema y su politica de seguridad deben aplicarse subsecuentemente sobre este nuevo conjunto de datos. Al finalizar, como entregable debe presentarse una tabla de efectividades derivadas de la generalización del modelo al nuevo *dataset*. Esta labor es fundamental para garantizar que el sistema y su lógica de negocio subyacente sean aplicables a cualquier colección de sujetos. En concordancia con el objetivo general, la tasa de éxito promedio vislumbrada en la tabla deberá ser igual o superior a 80.37%. En la compilación de la base es preciso emplear el dispositivo OpenBCI-Cyton con su respectivo módulo de adquisición de señales: OpenViBE. Para evaluar el desempeño, es menester utilizar el lenguaje de programación Python 3, en el cual, se deben importar las librerías: *scipy* y *numpy.*

4. La satisfacción del cuarto objetivo particular conlleva como meta o entregable el previamente aludido esquema relacional de base de datos en el lenguaje de modelado UML. En éste, se deben denotar las cardinalidades de cada entidad participante en el sistema y las restricciones referenciales, de dominio, y de valores nulos, que deberán imponerse para salvaguardar la consistencia de los datos. En su implementación se debe emplear el gestor MySQL 8.0.25. Las transacciones hacia ésta se deben lanzar mediante el lenguaje Python 3, que requiere el conector *mysql.connector.*
5. Finalmente, para satisfacer el quinto objetivo, es menester generar una pieza de software que presente en forma gráfica y cada n segundos una orden de realización de tarea mental al usuario. Este componente debe, en forma paralela, mantener un flujo activo de recepción datos entre el dispositivo de recopilación y el ordenador en que se ejecute, permitiendo la captura de la señal EEG derivada. Su completitud puede validarse introduciendo al instrumento de recopilación una señal de forma, frecuencia y amplitud conocidas, cuya forma en el dominio del tiempo debe coincidir con los datos compilados. En la implementación de este objetivo, fundamental para la disposición de datos que permitan determinar la identidad del usuario, se debe hacer uso del lenguaje Python 3, en conjunto con las librerías *numpy, brainflow, tkinter* y *threading*.

4. Marco teórico

4.1 Descripción de las interfaces cerebro-computadora

Las interfaces cerebro-computadora, comúnmente abreviadas como ICCs o BCIs, son herramientas tecnológicas de alto poder que permiten la comunicación entre un usuario y un sistema de cómputo sin la manipulación muscular física de un dispositivo de entrada

convencional como un ratón o un teclado (Nicolas-Alonso y Gomez-Gil, 2012) . En vez de recurrir a dichos mecanismos para inducir la orden del usuario, la interfaz se encarga de monitorear reiteradamente la actividad cerebral del sujeto para eventualmente procesarla con un algoritmo capaz de inferir sus intenciones y ejecutarlas (Minguez, 2008). Con ello, la mente, se transforma en la metodología para expresar control sobre el equipo.

El fenómeno tecnológico de las interfaces cerebro-computadora, de acuerdo con Yijun Wang y Tzyy-Ping Jung, miembros del Centro Swartz para la neurociencia computacional, se remonta a los años 70. En este periodo, la investigación de dichas herramientas se centró en el área biomédica, donde se pretendía la fabricación de dispositivos que asistiesen la movilidad y capacidades de pacientes con limitaciones motrices o del habla, y generasen canales de comunicación artificiales para pacientes con parálisis severa.

En sus primeras implementaciones, según relatan (Wang y Jung, 2011) las interfaces cerebro-computadora presentaban un carácter monotarea i.e., que únicamente eran capaces de laborar con una actividad mental específica, demandando al usuario concentración plena. Ejemplos de ello fueron los denominados deletreadores, piezas de software que presentaban un teclado virtual a sus usuarios con teclas que titilaban a una frecuencia diferente. Mediante el comportamiento inherente del cerebro que subyacentemente se sincroniza con las frecuencias antedichas i.e., potenciales evocados visuales de estado estacionario, los usuarios podían seleccionar la letra que deseaban plasmar en pantalla o concatenar en un arreglo de caracteres para formar palabras u oraciones (Ganin, Shishkin, Kochetova et al., 2012).

Al depender únicamente de la mirada, los usuarios de dicha plataforma no podían desviar la vista del monitor, ya que, de lo contrario, su orden no podría ser debidamente identificada. A fin de solventar dicha problemática, se desarrolló un nuevo paradigma que

hacía uso de las denominadas imágenes motoras, las cuales, consisten en la imaginación de un movimiento corporal, sin generar una salida física real (Decety, 1996). Estas, se emplean para seleccionar entre diversas opciones ofrecidas por el sistema. En el caso de los deletreadores, dicha metodología se aplicó mediante una flecha en la pantalla que apuntaba a una determinada fila y columna del teclado virtual, la cual, se desplazaba al imaginar el movimiento de un miembro como el brazo o la pierna, ya sea izquierdo o derecho.

Cuando dicha práctica se popularizó, las interfaces cerebro-computadora, según puntualizan Lance, Kerick, Ries y McDowell en su revisión bibliográfica titulada *Brain-Computer Interface technologies in the coming decades*, comenzaron a ofrecer una mayor cantidad de controles que eran manipulables a través de la actividad cerebral. Esto daría paso aplicaciones de mayor complejidad como cursores o dispositivos de comunicación plenamente manipulados mediante la actividad cerebral.

Hoy en día, dado el anterior proceso evolutivo; la popularización de técnicas para la recopilación de actividad cerebral poco invasivas como la electroencefalografía o EEG que cuantifica las manifestaciones eléctricas de actividad neuronal (Vidal, Burle, Spieser, et al., 2015) mediante electrodos colocados sobre el cuero cabelludo; y el descubrimiento de nuevas capacidades potenciales de las interfaces cerebro-computadora, el uso y estudio de estas herramientas para el área médica se ha masificado. Dicha tecnología, por ejemplo, ha mostrado ser de gran eficacia asistencial en pacientes que han sufrido infartos cerebrales, pérdida parcial o total del habla e incluso parálisis. En éstos ámbitos, según describen (McFarland y Wolpaw, 2008), se ha comenzado a transicionar de controles basados en software a alternativas mecánicas como brazos robóticos que permitirán a pacientes inmovilizados concretar sus actividades diarias y comunicarse físicamente con el exterior.

De igual forma, en el área médica se ha comenzado a analizar la utilidad de éstas herramientas como métodos de prevención y diagnóstico. Las ICC, por ejemplo, han demostrado capacidad para detectar condiciones cerebrales atípicas e.g., alteraciones en la estructura cerebral derivadas de tumores, trastornos convulsivos como la epilepsia, alteraciones del sueño e.g., narcolepsia, encefalitis, indicios de enfermedad de Parkinson, e incluso adicciones como el tabaquismo o alcoholismo (Abdulkader, Atia y Mostafa, 2015). Todo ello sido posible dada la habilidad que paulatinamente han adquirido dichas herramientas de analizar el estado cognitivo y emocional de un sujeto.

4.2 Trascendiendo las aplicaciones médicas

A finales de los 90s e inicios de la década de los 2000 comenzaron a vislumbrarse las primeras aplicaciones no-médicas de las ICC (Blankertz, Tangermann, Vidaurre et al., 2010). Algunos ejemplos comúnmente enunciados por la literatura son la ergonomía, la educación, el entretenimiento y, más recientemente, la seguridad informática (Abdulkader, Atia y Mostafa, 2015). En la primera de ellas i.e., el área ergonómica, se observó una utilidad de dichas herramientas como fuentes de información complementarias en estudios relacionados con interacción humano-computadora (Abdulkader, Atia y Mostafa, 2015).

A fin de ejemplificar lo anterior considere la publicación *Brain–Computer Interface Contributions to Neuroergonomics* de (Lotte y Roy, 2018). En esta, se expone de manera introductoria la existencia de tres tipos de interfaces cerebro-computadora: activas, reactivas y pasivas. El paradigma funcional de las primeras consiste en la realización de una tarea mental específica e.g., imaginar el movimiento de alguna extremidad, por parte del usuario. Mientras tanto y, de manera subyacente, la interfaz recopila e interpreta los patrones

neuronales generados, trasladándolos subsecuentemente en un comando que mas tarde será ejecutado e.g., el movimiento rectilíneo a izquierda o derecha de un cursor en pantalla.

Las interfaces reactivas, por su parte, presentan al usuario un conjunto de opciones predeterminadas. Cada una de ellas tienen un factor distintivo imperceptible a simple vista pero identificable por el cerebro e.g., la frecuencia de parpadeo. La metodología operacional de este tipo de interfaces requiere que el sujeto dirija su atención a la alternativa que pretende ejecutar. Subconscientemente, esto causará una sincronización de la actividad cerebral con el patrón único de la antedicha opción. En tanto ocurre lo anterior, la interfaz se encontrará analizando activamente el comportamiento neuronal del sujeto. Al detectar un patrón conocido ejecutará el comando asociado a éste. Un ejemplo simple de este tipo de interfaces son los anteriormente descritos deletreadores, basados en potenciales evocados P-300.

Para finalizar se encuentran las interfaces pasivas. Estas, de igual forma examinan ininterrumpidamente el estado mental de un individuo. No obstante y, en contraposición con las interfaces activas y reactivas, éstas no ejecutan comando alguno. En su lugar, dichas herramientas adaptan la configuración de un sistema a fin de mejorar la experiencia de usuario. Por ello, estas interfaces son el común denominador del ámbito ergonómico.

Ejemplos de lo anterior son provistos por (Lotte y Roy, 2018) y (Parasuraman y Wilson, 2008) quienes describen la utilidad de las interfaces pasivas en la adaptación de dificultad en videojuegos, el ajuste de pantallas de controladores de tráfico aéreo y el análisis adaptativo de cargas laborales en tareas de alta complejidad[2]. Asimismo (Abdulkader, Atia

[2] Dada la valiosa contribución de las interfaces cerebro-computadora al ámbito ergornómico se ha dado lugar al nacimiento de la "neuroergonomía", una ciencia de carácter emergente que, mediante la antedicha tecnología estudia las relaciones entre el estado cerebral y el desempeño de las tareas diarias (Mehta, y Parasuraman, 2013),

y Mostafa, 2015) describen la utilidad de estas interfaces para exponenciar las capacidades del IoT, e.g., permitiendo la generación de entornos domésticos auto-gestionables en los que se ajusta la iluminación y temperatura con base en el estado mental de sus ocupantes.[3]

Como se ha mencionado con anterioridad, el ámbito educativo es otra área de utilidad para las interfaces cerebro-computadora. (Van Erp, Lotte y Tangermann, 2012), por ejemplo, describen en su publicación titulada *Brain-computer interfaces: beyond medical applications* cómo esta tecnología permite vislumbrar y analizar el cerebro, su plasticidad y los cambios evolutivos que éste presenta ante diversas técnicas de capacitación. Esto, permite cuantificar el grado de progreso y aprendizaje de los estudiantes. (Van Erp, Lotte y Tangermann, 2012) comentan que ésta tecnología es particularmente útil en las denominadas *knowledge-based economies* i.e., sociedades vanguardistas predominantemente occidentales (Godin, 2006) y con población en edad avanzada que vislumbran el conocimiento como principal fuente de properidad y crecimiento económico (Tocan, 2012).

Asímismo, en el campo del entretenimiento, las ICC han demostrado un gran potencial, al ser útiles en la fabricación de videojuegos y material multimedia en realidad aumentada (Lécuyer, Lotte, Reilly et al., 2008). Algunos autores e.g., (Leite, Carvalho, Costa, et al., 2018) comentan que su popularidad en éste ámbito ha sido tal que incluso se ha dado paso a una nueva disciplina denominada *neurogaming.* Un ejemplo de lo anterior es

[3] En 2015 un estudio a cargo del departamento de instrumentación y electrónica de la Universidad de Hindustan en Chennai India demostró la utilidad de las ICC en el área ergonómica mediante un prototipo que recopilaba ondas EEG de los ocupantes de un hogar inteligente con electrodos basados en tecnología MEMS i.e., que no requieren la aplicación de un gel conductor (Blankertz, Tangermann, Vidaurre et al., 2010). Dicha señal era eventualmente transferida a un microprocesador central mediante bluetooth donde un algoritmo identificaba el estado psicológico, nivel de alerta y grado de somnolencia de los residentes. Con dicha información se efectuaba una adaptación automática de la iluminación y temperatura del entorno, a fin de brindar a los residentes descanso o estimulación acorde al nivel de sueño que presentasen (Abin y Ramachandraiah, 2012)

NeuroRacer, un videojuego tridimensional basado en interfaces cerebro-computadora y dirigido a un público objetivo de entre 20 y 79 años que impulsa a los usuarios a seguir visualmente un cursor en pantalla, para así dirigir un vehículo a través de una pista con diversos obstáculos. (Anguera, Boccanfuso, Rintoul et al., 2013)

Dicho proyecto, es potencialmente destacable puesto que no sólo contribuye al entretenimiento, sino también al ámbito educativo. Dado que, el control del juego recae en el pensamiento, es necesario que sus usuarios ejerzan un nivel alto de concentración. A largo plazo esto se traduce en una mayor capacidad de memorización y habilidad cognitiva por no mencionar su contribución al desarrollo del *multitasking*, condición en que los individuos pueden efectuar de manera competitiva más de una tarea a la vez. (Paszkiel, 2016).

Para finalizar el análisis aplicativo de las interfaces cerebro-computadora y demostrar efectivamente su trascendencia fuera del área médica, es menester señalar la contribución de éstas al ámbito de la seguridad informática. De acuerdo con (Abdulkader, Atia y Mostafa, 2015) las interfaces basadas en electroencefalografía podrían asistir esta disciplina al fungir como nuevos paradigmas de autenticación. Dicho procedimiento clave para los sistemas informáticos consiste en identificar de manera adecuada a un individuo ante un sistema informático (Li, Ding, y Conti, 2015) para subsecuentemente conferir o negar el acceso a un recurso de carácter confidencial o privado.

En éste ámbito existen ya algunas investigaciones preliminares, que han demostrado efectivamente la utilidad de las ICC en la autenticación de usuarios. Un ejemplo de lo anterior es provisto por (Ashby, Bhatia, Tenore et al., 2011) en su publicación titulada *Low-cost electroencephalogram (EEG) based authentication*. En ésta se describe la extracción de coeficientes de un modelo autoregresivo de 6to orden, densidad espectral y potencia total de

señales EEG de imaginación motora recopiladas con equipos de bajo coste. Las características antedichas se utilizan para alimentar una máquina de soporte vectorial que subsecuentemente se emplea como clasificador para identificar a un sujeto. Esta investigación logra resultados bastante destacables e.g., una efectividad de clasificación del 100%, aunque carece de ciertas consideraciones e.g., la potencial pérdida de efectividad al emplear diferentes sesiones y la aplicabilidad del paradigma con otro conjunto de sujetos.

4.3 Funcionamiento de una interfaz cerebro-computadora

Pese a destinarse a diversos propósitos y disciplinas las ICC suelen mantener un entre sí un mismo paradigma operativo que consta de cinco fases: *estimulación*, *adquisición de señal*, *preprocesamiento, extracción de características* y *clasificación* o *predicción.* (Van Gerven, Farquhar, Schaefer, et al., 2009). Este proceso se presenta de manera gráfica en la figura 1.

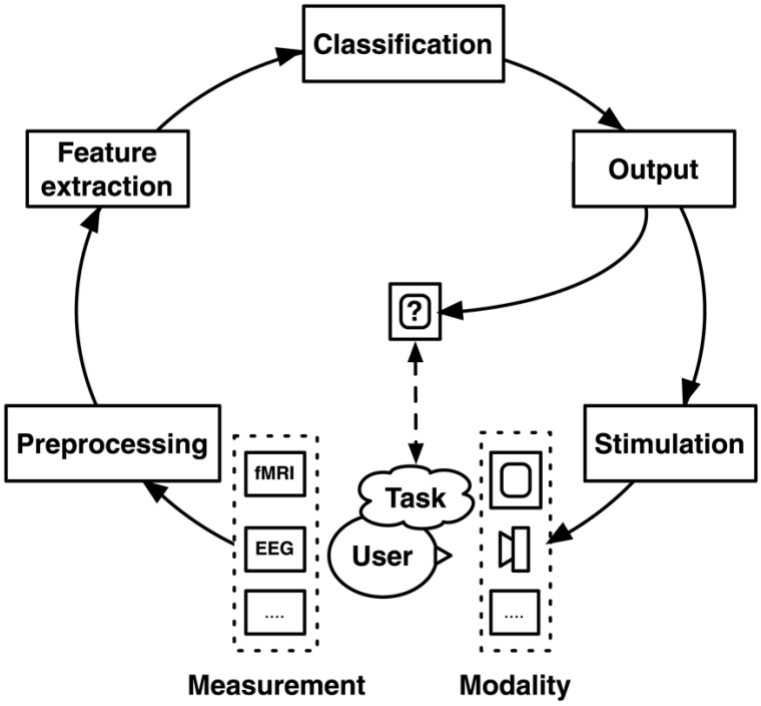


Figura 1. Paradigma operativo de una interfaz cerebro-computadora. Este elemento gráfico fue proporcionado por (Van Gerven, Farquhar, Schaefer, R, et al., 2009).

4.3.1 Estimulación

El antedicho ciclo comienza con el proceso de *estimulación*, durante el cuál un ordenador solicita ya sea de manera visual, auditiva o sensorial la realización de una tarea mental específica por parte del usuario. Esto, durante un periodo de tiempo establecido. Es menester señalar que la tarea seleccionada debe ser relativamente simple, ya que, de lo contrario, se produce fatiga mental y frustración (Curran y Stokes, 2003). Estas condiciones, pueden derivar en una pérdida de efectividad de la ICC de hasta de un 7% según las observaciones experimentales de (Myrden y Chau, 2015)[4]. Asímismo, es relevante hacer un intento por prolongar la actividad cerebral i.e., la duración de la tarea e inherentemente de la señal, tanto como sea posible, sin caer en la problemática anterior, ya que ello permite al sistema disponer de un mayor conjunto de datos, que permitirán interpretar con mayor eficacia la intención final del usuario (Van Gerven, Farquhar, Schaefer, et al., 2009).

4.3.2 Adquisición de señales

Una vez iniciada la estimulación, es menester dar paso a la *adquisición de señales,* que consiste en cuantificar la actividad mental del individuo. Para ello, la literatura propone diversas tecnologías y aproximaciones, que comúnmente son catalogadas en 2 subconjuntos: *invasivas* y *no-invasivas*. Entre las primeras se encuentra la electrocorticografía o EcoG y la adquisición intracortical o ICE. Ambas requieren la intervención de un neurocirujano que coloca electrodos debajo de la corteza cerebral, los cuales, capturan los potenciales generados

[4] Es importante señalar que, de manera inicial, la fatiga mental es común entre los usuarios de una interfaz cerebro-computadora dada su falta de experiencia con esta tecnología. No obstante el esfuerzo requerido para la realización de dichas tareas mentales suele decaer de manera progresiva dado que el usuario aprende a realizarlas en forma mecanizada i.e., sin prestar atención total a ellas (Miner, McFarland y Wolpaw, 1998). Es menester considerar esta cualidad cerebral al diseñar un paradigma de recopilación de datos, aunque de igual forma deben considerarse las advertencias de algunos autores como (Myrden y Chau, 2015) quienes señalan que al presentarse un fallo de las habilidades “automáticas” del usuario podría recaerse en la fatiga mental.

por el cerebro durante la estimulación, aunque evitando el ruido generado tanto por el cráneo como por el cuero cabelludo (Keene, Whiting y Ventureyra, 2000). Inherentemente estas metodologías ofrecen una alta calidad de señal, no obstante, su uso representa un riesgo de complicaciones médicas que van desde infecciones hasta daños motores. Esto, sin mencionar su extrema inviabilidad para aplicaciones reales (Abdulkader, Atia, y Mostafa, 2015).

Por su parte, dentro del conjunto de técnicas no invasivas la literatura suele enumerar cuatro posibles aproximaciones: la magnetoencefalografía o MEG que analiza el campo magnético que se produce sobre la superficie craneal (Wheless, Castillo, Maggio et al., 2004); la resonancia magnética funcional o fMRI que cuantifica las variaciones en la concentración de hemoglobina sanguínea y su relación con la actividad cerebral por medio de un contraste dependiente del oxígeno en la sangre o BOLD (Ayaz, Shewokis, Bunce y Onaral, 2011); la espectroscopía funcional del infrarrojo cercano o fNIRS que, de igual forma depende de la dinámica sanguínea para cuantificar la actividad cerebral del individuo, aunque utiliza una luz cercana al espectro infrarojo para determinarla (Abdulkader, Atia, y Mostafa, 2015); y finalmente la popular electroencefalografía o EEG.

Esta alternativa utilizada por primera vez en humanos hacia el año 1929 por el neurólogo y psiquiatra alemán Hans Berger (Lakshmi, Prasad, y Prakash, 2014), consiste en alojar una colección, tradicionalmente de 24 electrodos, sobre el cuero cabelludo y cuantificar los denominados “potenciales postsinápticos” (Mehta y Parasuraman, 2013) i.e., fluctuaciones de voltaje producidas por las neuronas, perceptibles sobre dicha superficie craneal (Abdulkader, Atia, y Mostafa, 2015).

Con el fin de obtener un amplio panorama sobre la dinámica cerebral en un momento determinado los electrodos previamente aludidos se colocan en diversos puntos estratégicos

e.g., el área frontal, parietal y temporal, así como el lóbulo occipital, agregando a lo anterior un electrodo de referencia colocado en la oreja (Homan, Herman, y Purdy, 1987). Dicha distribución corresponde con el denominado sistema internacional 10-20, actualmente aceptado y prescrito por la American Electroencephalographic Society (Nicolas-Alonso y Gomez-Gil, 2012). Su esquema y especificaciones se presentan en la figura número 2 de la sección de anexos.

Esta metodología de gran popularidad en la comunidad científica destaca por diversas razones e.g., su uso es relativamente simple y requiere de poca preparación previa (Gargiulo, Calvo, Bifulco, et al., 2010), el dispositivo de recopilación electroencefalográfico es portable, económico, seguro y poco intrusivo, el paradigma ofrece una amplia resolución temporal y es robusto ante variaciones electromagnéticas (Abdulkader, Atia, y Mostafa, 2015), por no mencionar su vasto espectro de aplicaciones que van desde la detección de anomalías fisiológicas y conductuales e.g., desordenes del sueño y epilepsia (Bubrick, Yazdani y Pavlova, 2014) hasta complejas aplicaciones ergonómicas y de entretenimiento.

Ahora bien, pese a las notables características anteriores, se debe señalar que la electroencefalografía no está exenta de desventajas. (Lakshmi, Prasad, y Prakash, 2014) señalan, por ejemplo, la suceptibilidad de las señales EEG a los previamente referenciados *artefactos* i.e., interferencias fisiológicas en la señal, comúnmente derivadas del parpadeo, movimiento ocular, latido del corazón y movimientos musculares. No obstante, (Urigüen y Garcia-Zapirain, 2015), presentan en su revisión titulada *EEG artifact removal—state-of-the-art and guidelines* diversas metodologías que permiten minimizar o suprimir el impacto de éstos en la calidad de la señal e inherentemente en el desempeño de la ICC. Algunos de éstos son la regresión, el filtrado, la separación ciega de fuentes o BSS, el análisis principal o

independiente de componentes i.e., PCA e ICA, entre otras. Así pues, dadas las cualidades de éste paradigma de recopilación, sus reducidas desventajas y la existencia de técnicas de mitigación para éstas, la EEG se emplea como método de adquisición a lo largo de esta tesis.

4.3.3 Preprocesamiento

Tras completar el proceso de recopilación, las señales resultantes deben ingresar a una fase de *preprocesamiento*. En esta, la información capturada recibe un tratamiento preliminar que tiene por objetivo reducir el ruido; normalizar, calibrar y ecualizar la señal; suprimir tendencias, minimizar la dimensionalidad y, sobre todo, eliminar artefactos (Oweis, Hamdi, Ghazali et al., 2013). Inherentemente, para ello, existen diversas aproximaciones e.g., la regresión en el dominio del tiempo o la frecuencia, la separación ciega de fuentes o BSS, el análisis de componentes independientes o ICA y el filtrado selectivo de frecuencias. Ésta última goza de una gran popularidad en proyectos basados en señales electroencefalográficas dada su notable capacidad para remover artefactos asociados a movimientos musculares (Motamedi-Fakhr, Moshrefi-Torbati, Hill et al., 2014), que, como se ha mencionado con anterioridad, son los más comunes y notorios en dicho método de adquisición.

El paradigma operativo de esta técnica de preprocesamiento se basa en la suposición de que los artefactos y la señal útil emplean diferentes bandas de frecuencia (Motamedi-Fakhr, Moshrefi-Torbati, Hill et al., 2014). Así pues, esta metodología implica el uso de los denominados filtros *paso baja, paso alta, paso banda* o *rechaza banda* i.e., *low-pass, high-pass, band-pass* y *band-stop* respectivamente, que permiten seleccionar, aislar y suprimir las frecuencias contaminantes. En la figura número 3 se exponen gráficamente las diferencias entre cada tipo de filtro y se brinda una descripción breve de su funcionamiento. Como es posible observar en este recurso gráfico, el filtro paso-baja o *low-pass* radica en establecer

una frecuencia de corte i.e., f_c y suprimir todos los componentes que excedan el antedicho umbral. De manera antagónica opera el filtro paso-alta o *high-pass* que, en contraposición con su previamente referenciado símil, elimina los componentes cuya frecuencia es insuficiente para superar la frontera f_c impuesta. Por su parte, el filtro paso-banda o *band-pass* requiere de dos frecuencias de corte i.e., f_{c1} y $f_{c2} \mid f_{c2} > f_{c1}$, entre las cuales deberán ubicarse todos los componentes de la señal que se pretenden conservar. Para finalizar y, nuevamente de forma antípoda, se encuentra el filtro rechaza-banda o *band-stop,* en el cuál se suprimen todos los componentes cuya frecuencia se localice entre f_{c1} y f_{c2}.

Cabe señalar que, con regularidad, en la implementación de lo anterior, se recurre a la aproximación de *Butterworth* estableciendo un *orden* llámese $n = 4$ e.g., (Murugappan y Murugappan, 2013), (Mazumder, 2019) y (Ferdous, Ali, Hamid, et al., 2016). Lo anterior, dada su respuesta casi plana y distosión reducida en la banda de paso (Ali, Radwan y Soliman, 2013). Por estas mismas razones, en secciones subsiguientes se recurrirá a dicha metodología aplicada a un filtro paso banda.

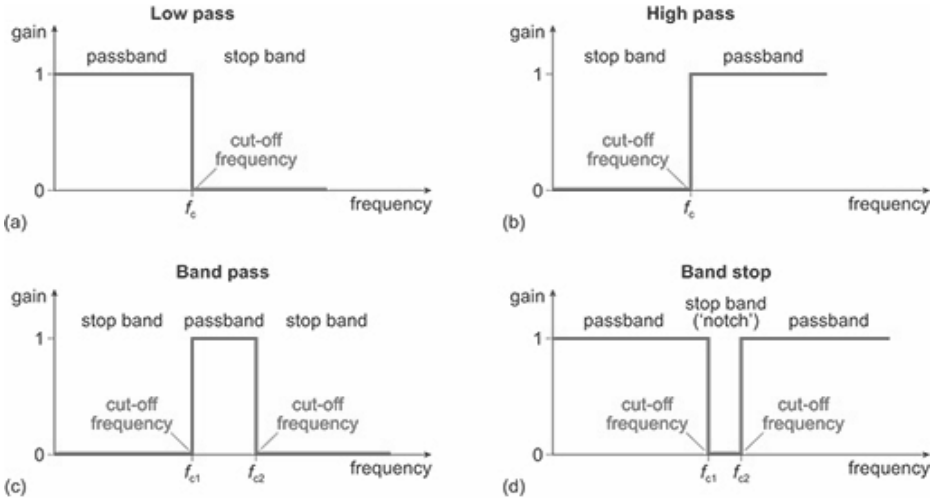


Figura 3. Tipos de filtrado selectivo de frecuencia. El gráfico presentado pertenece al curso *Electronic applications* de OpenLearn elaborado por (Jones, Clarke y Picto, 2020).

4.3.4 Extracción de características

Técnicamente una interfaz cerebro-computadora podría vislumbrarse como un sistema de reconocimiento de patrones (Nicolas-Alonso y Gomez-Gil, 2012) e.g., cada tarea mental constituye un patrón identificable cuya ocurrencia detona una respuesta del dispositivo. No obstante para lograr dicho efecto, es menester indicar con antelación a la ICC las cualidades distintivas de cada patrón. Este es precisamente el objetivo de la *extracción de características*: localizar información discriminatoria de cada patrón en la señal preprocesada que posteriormente sirva como pauta para identificar su reincidencia. Así pues, una característica puede definirse como un parámetro que brinda información de la estructura única y subyacente de una señal (Motamedi-Fakhr, Moshrefi-Torbati, Hill et al., 2014).

Inherentemente el proceso de extracción de características es altamente complejo y constituye por sí mismo un extenso campo de estudio. En primera instancia, dado que existen diversas aproximaciones e.g., *cruces a cero* i.e., puntos en que la onda atraviesa el eje de las x; *parámetros de Hjorth* i.e., indicadores extraídos a partir de la varianza de las derivadas de la señal; *características espectrales* i.e., factores distintivos de la señal en el dominio de la frecuencia; *dimensión fractal* i.e., una cuantificación de la complejidad de la señal y finalmente, *estadísticos instantáneos* i.e., descriptores estadísticos comunes y fácilmente computables en cuya extracción se asume que cada segmento de la señal es un proceso univariable e independiente (Motamedi-Fakhr, Moshrefi-Torbati, Hill et al., 2014).

De forma algorítmica, la extracción características consiste en, dada una señal en el dominio del tiempo representada como una matriz de $C \times M$ donde C indica el número de canales de recopilación e.g., electrodos y M el número de muestras en el tiempo, se particiona

M de cada canal en W ventanas de n muestras, ya sea con o sin superposición, y se extrae $\theta(M_x, M_{x+1}, \dots M_{x+n})$, donde θ es una función para computar la característica deseada i.e., asumiendo que cada partición es el antedicho proceso univariable e independiente. Inherentemente, al concluir el procedimiento anterior, se tendrá una nueva matriz de $C \times W$ que contiene los valores característicos.

Cada uno de los W vectores de cardinalidad C en que dicha matriz puede descomponerse i.e., de forma vertical, es denominado un *vector característico*. De acuerdo con la literatura la dimensión de dicho vector debe ser preferentemente mínima, a fin de reducir la complejidad del proceso de extracción de características e inherentemente el costo computacional que dicha labor genera en la ICC. No obstante este debe mantener una extensión suficientemente grande como para evitar la pérdida de información relevante (Nicolas-Alonso y Gomez-Gil, 2012). Algunos descriptores estadísticos potencialmente útiles para el objetivo de esta tesis se analizan en los apartados subsecuentes. En añadidura a éstos, se presentará el algoritmo de Katz para computar la dimensión fractal.

4.3.4.1. Desviación estándar

La desviación estándar es una métrica de índole estadística que permite cuantificar la dispersión alrededor de la media. Esta característica no-negativa tiene diversas utilidades, por ejemplo, para detectar anomalías. Dada una variable discreta x de n observaciones $x_1, x_2, \dots, x_n$ con media $\bar{x}$, la desviación estandar o $\sigma(x)$ se define como:

$$\sigma(x) = \sqrt{\frac{\sum_{k=1}^{n}(x_k - \bar{x})^2}{n}}$$

4.3.4.2. Rango intercuartílico

El rango intercuartílico o IQR es, de igual forma, una medida de dispersión que permite cuantificar la variabilidad de una distribución (Whaley, 2005). Tradicionalmente se define como el rango en el cual, se localizarán la mitad de las observaciones de una variable discreta x o bien como la diferencia entre el primer y tercer cuartil Q_1 y Q_3 i.e., percentiles 25 y 75:

$$IQR(x) = Q_3 - Q_1$$

4.3.4.3. Desviación de la mediana absoluta

La desviación de la mediana absoluta o MAD por sus siglas en inglés i.e., *median absolute deviation,* es una métrica de carácter estadístico que permite cuantificar la dispersión existente en una variable x. Esta herramienta no-paramétrica opera en forma similar a la desviación estándar, razón por la cuál no es inverosímil concebirla como característica. No obstante, en contraposición con σ, la MAD destaca por su robustez ante la presencia de anomalías en una distribución (Mazumder y Serfling, 2009). El estadístico, dada una variable discreta x de n observaciones $x_1, x_2, \dots, x_n$ con mediana $\tilde{x}$ es definido por la literatura como:

$$MAD(x) = \underset{n \geq x \geq 1}{\text{med}}(|x_i - \tilde{x}|)$$

Cabe señalar que, en forma análoga a la desviación estándar, este descriptor es potencialmente útil para detectar irregularidades en una distribución i.e., *outliers* (Leys, Ley, Klein et al., 2013). Esto, convierte a la MAD en un estadístico predilecto, por ejemplo, en sistemas de monitoreo de calidad en productos (Adekeye, 2012). Para dicho proceso de detección y posterior supresión de anomalías se toma como base el enfoque de *medias restringidas* i.e., una regla empírica de descarte basada en desviación estándar donde toda muestra $x_k > \bar{x} \pm \alpha\sigma(x)$, siendo α tradicionalmente 2.0, 2.5, 3.0 (Miller, 1991) e incluso

4.0 (Cousineau y Chartier, 2010), se elimina de x al considerarse un fallo en la recopilación (Anscombe, 1960). No obstante en este caso la desviación estándar $\sigma(x)$ es reeemplazada por la desviación de la mediana absoluta $MAD(x)$ y la media i.e., $\bar{x}$ por $\tilde{x}$.

Este cambio de estadístico es extensamente fundamentado por (Miller, 1991) y (Cousineau y Chartier, 2010). El primero indica que, si bien el paradigma de *medias restringidas* i.e., basado en desviación estándar, ha probado ser útil en diversos ámbitos y análisis e.g., el de (Takeda, Mishiba, Sugiura et al., 2009), dicha aproximación tiene un fallo metodológico subyacente y es su dependencia en la forma normal de los datos. No obstante, relata dicho autor, cuando se opera con información contaminada por anomalías la anterior forma no está garantizada. Esto se traduce en que $\bar{x}$ e inherentemente $\sigma(x)$ se encuentren sesgados. Por consecuente al aplicar la regla de descarte es posible que valores regulares sean suprimidos y determinadas muestras anómalas sean conservadas (Miller, 1991).

Este desperfecto, de acuerdo con (Cousineau y Chartier, 2010) es amplificado en forma inversamente proporcional por el tamaño de la muestra i.e., entre menor sea el número de observaciones n en x mayor será efecto de un *outlier* en éste. Lo anterior, se debe principalmente a la inestabilidad *de facto* de la asimetría estadística. En añadidura a lo anterior (Cousineau y Chartier, 2010) y (Leys, Ley, Klein et al., 2013) coinciden en que el método de *medias restringidas* i.e., basado en desviación estándar, es incapaz de detectar outliers si n es reducido, pues la media $\bar{x}$ por lo general tiende a la conservación. Algunos autores e.g., (Bilimoria, Cohen, Merkow et al., 2010) intentan mejorar la efectividad del removedor de *outliers* con metodologías más sofisticadas como la corrección de Bonferroni, no obstante esto incrementa sustancialmente la complejidad del proceso.

4.3.4.4. Algoritmo de dimensión fractal de Katz

Como se ha mencionado con anterioridad, la dimensión fractal es una cuantificación de la complejidad de una señal adquirida. Su origen se remonta al concepto matemático homónimo i.e., los *fractales* elementos geométricos con dimensionalidad no-entera (Motamedi-Fakhr, Moshrefi-Torbati, Hill et al., 2014). Un ejemplo de ello es el popular copo de nieve de Koch, una figura con perímetro de longitud infinita y área finita (Crilly, Eamshaw y Jones, 1991).

Su uso como característica, de acuerdo con (Motamedi-Fakhr, Moshrefi-Torbati, Hill et al., 2014) deriva de una extensión de esta idea a series de tiempo, donde la complejidad distintiva de la serie es proporcional a su dimensión fractal. Inherentemente este principio se aplica al dominio del tiempo de la señal. Esto, permite que el cómputo de dicho valor característico se realice bajo la misma aproximación de los *estadísticos instantáneos* i.e., fungiendo como θ de una ventana de n valores $M_x, M_{x+1}, \dots M_{x+n}$ en el dominio del tiempo.

Existen diversos algoritmos para llevar a cabo su estimación e.g., el *Petrosiano,* el de *Higuchi,* y el de *Katz* (Esteller, Vachtsevanos, Echauz et al., 1999). Este último tiene un rendimiento significativamente menor a sus contrapartes pero destaca por su capacidad de calcularse directamente sobre una onda sin preprocesamiento previo (Esteller, Vachtsevanos, Echauz et al., 1999). Dada una serie de n valores $x = x_1, x_2, \dots x_n$ la dimensión fractal mediante el algoritmo de *Katz* i.e., $katz(x)$ se computa como:

$$katz(x) = \frac{\log_{10}(n-1)}{\log_{10}(n-1) + \log_{10}(\frac{d}{L})}$$

Donde L representa la longitud de la curva o bien, la suma de las distancias euclidianas entre puntos sucesivos, y d el diámetro de la onda el cuál, se estima como la distancia entre el

primer elemento en la secuencia y el punto que genera la máxima distancia (Esteller, Vachtsevanos, Echauz et al., 1999). Así pues:

$$L = \sum_{i=1}^{n-1} \sqrt{(y_i - y_{i+1})^2 + (x_i - x_{i+1})^2}, \text{ donde } (y_i - y_{i+1})^2 = 1$$

$$d = \max_{n \geq i \geq 2} (dist(1,i)), \text{ donde } dist(1,i) = \sqrt{(1-i)^2 + (x_1 - x_i)^2}$$

4.3.5 Clasificación o predicción

Una vez que la interfaz cerebro-computadora ha completado las fases anteriores, es menester dar paso a la *clasificación* o *predicción.* En esta etapa se emplean los vectores característicos previamente identificados para, inicialmente, entrenar a un *clasificador* y, subsecuentemente, i.e., en una nueva iteración del ciclo funcional de la ICC, para determinar, dada una nueva señal, la tarea mental que la ha generado. Con dicho conocimiento es posible realizar, de manera subsecuente, una acción mecánica, adaptativa o funcional i.e., una traducción de las intenciones del usuario en comandos (Abdulkader, Atia, y Mostafa, 2015), dependiendo el tipo de interfaz que se esté desarrollando i.e., *activa, reactiva* o *pasiva.*

Inherentemente existe un amplio espectro de algoritmos de clasificación, a los cuales es posible atribuir las siguientes etiquetas según su modelo operacional: *generativo* o *discriminativo, estático* o *dinámico, estable* o *inestable* y/o *regularizado* (Torres, Torres, Hernández-Álvarez et al., 2020). Los clasificadores *generativos* basan su aprendizaje en probabilidades conjuntas $p(x, y) = p(y) \cdot p(x|y)$, donde $x = x_1, x_2, \dots, x_n$ es una serie de características con etiquetas $y = y_1, y_2, \dots y_k$, que transforman en probabilidades *a posteriori* i.e., $P(y|x)$ mediante el teorema de Bayes. Lo anterior se utiliza para clasificar nuevos vectores característicos con la etiqueta y_k que maximice $P(y|x)$ (Ng y Jordan, 2002).

Por el contrario, los clasificadores *discriminativos* establecen de antemano una frontera entre las n posibles clases basándose en $P(y|x)$ (Torres, Torres, Hernández-Álvarez et al., 2020). Dicho límite inherentemente se establece procurando la minimización del error. Como ejemplos de clasificadores *generativos* es posible resaltar *naive Bayes,* las redes Bayesianas y los modelos de Markov (Torres, Torres, Hernández-Álvarez et al., 2020), mientras que, en el caso de los clasificadores *discriminativos,* es posible señalar las máquinas de soporte vectoriales o SVMs y los perceptrones multicapa o MLPs (Li y Bilmes, 2006).

Por su parte el etiquetado de un modelo de clasificación como *estático* o *dinámico,* se basa en la capacidad adaptativa del mismo ante variaciones temporales (Torres, Torres, Hernández-Álvarez et al., 2020). De forma concreta, un clasificador *estático* ignora el contexto temporal al realizar una predicción y confía plenamente en las fronteras inicialmente determinadas para separar nuevos elementos hacia cada *cluster*. Mientras tanto, un clasificador *dinámico* intenta refinar la salida con cada instanciamiento (Yaghouby, 2015). Esta característica, si bien no es garantía de mejora en la efectividad (Abuhashish, Sunar, Kolivand et al., 2014), puede servir como técnica de mitigación ante la popular e inherentemente problemática cualidad evolutiva de las señales cerebrales (Zheng, Zhu y Lu, 2017). Como ejemplo de clasificador *estático* es posible resaltar nuevamente a los MLPs, mientras que, como ejemplo de clasificadores *dinámicos* cabe señalar a los previamente referenciados Modelos Ocultos de Markov (Lotte, Congedo, Lécuyer et al., 2007).

Como se ha mencionado con anterioridad, otras etiquetas atribuibles a un modelo de clasificación son *estable* o *inestable.* La categorización en este caso se basa en el grado de afectación que tienen las modificaciones del conjunto de datos de entrenamiento sobre el desempeño del clasificador (Torres, Torres, Hernández-Álvarez et al., 2020). Mientras que

en el primer grupo que, por ejemplo, alberga el análisis de discriminantes lineales o LDA y el algoritmo de k-vecinos cercanos o kNN una variación tendrá un efecto reducido o nulo, en el segundo grupo, que nuevamente alberga a los perceptrones multicapa, el impacto será sustancial pese a que la alteración sea mínima (Lotte, Congedo, Lécuyer et al., 2007).

Finalmente, los algoritmos de clasificación con modelo *regularizado* se encargan de introducir una función de penalización $\theta: \mathbb{R}^+ \to \mathbb{R}^+$ (Blanchard, Lugosi, y Vayatis, 2003) que pretende controlar la evolución paulatina del clasificador, previniendo el sobre-entrenamiento (Torres, Torres, Hernández-Álvarez et al., 2020). Algunos ejemplos en esta categoría, destacable por su nivel de generalización, son el discriminante lineal de Fisher regularizado y las SVM lineales (Torres, Torres, Hernández-Álvarez et al., 2020).

4.3.5.1. Clasificador Gaussiano ingenuo de Bayes

Como se ha mencionado con anterioridad, dentro del conjunto de modelos *generativos* es posible identificar al *clasificador ingenuo de Bayes* cuyo uso a lo largo de esta tesis será por demás extensivo. Para su definición considere un vector característico x de cardinalidad n i.e., $x = (x_1, x_2, \dots x_n)$, y un conjunto Ω de M clases i.e., $\Omega = \{\omega_1, \omega_2, \dots \omega_M\}$. La tarea de clasificación consiste en asignar el $\omega_k \in \Omega$ correspondiente a x. Así pues el clasificador puede vislumbrarse como la siguiente función de mapeo (Larrañaga, Inza y Moujahid, 1997):

$$\theta: (x_1, x_2, \dots x_n) \to \{\omega_1, \omega_2, \dots \omega_M\}$$

Para realizar la asignación considere, en primera instancia, $P(\omega_i)\ \forall i \in [1..M]$ como la probabilidad *a priori* de ocurrencia de la clase ω_i y asuma la existencia de la siguiente distribución de probabilidad conjunta (Larrañaga, Inza y Moujahid, 1997):

$$P(x_1, x_2, \dots x_n, \omega_i) = P(x_1, x_2, \dots x_n | \omega_i) \cdot P(\omega_i)$$

Dado que la complejidad de determinar la probabilidad condicional al lado derecho de la expresión puede ser elevada si la cardinalidad del vector característico x es alta, la regla "ingenua" de Bayes supone que $x_1, x_2, \dots x_n$ son valores independientes (Rish, 2001). Así pues, es posible reformular la antedicha expresión como se propone a continuación:

$$P(x_1, x_2, \dots x_n, \omega_i) = P(\omega_i) \cdot \prod_{k=1}^{n} P(x_k|\omega_i)$$

Ahora bien, asumiendo que la información sigue una distribución Gaussiana, que la clase ω_i tiene una media μ_i y una desviación estándar σ_i, la antedicha aproximación puede extenderse a lo que algunos autores e.g., (Jahromi, Taheri, 2017) denominan un *clasificador Gaussiano ingenuo de Bayes.* En éste el cómputo de la probabilidad conjunta se redefine:

$$P(x_1, x_2, \dots x_n, \omega_i) = P(\omega_i) \cdot \prod_{k=1}^{n} \mathcal{N}(x_k;\ \mu_i\ , \sigma_i)$$

$$\mathcal{N}(x_k;\ \mu_i\ , \sigma_i) = \frac{1}{\sqrt{2\pi(\sigma_i)^2}}\, e^{-\frac{1}{2}\left(\frac{x_k - \mu_i}{\sigma_i}\right)^2}$$

Una vez realizada dicha expansión y, con base en el teorema de Bayes, es posible computar la probabilidad *a posteriori* i.e., $P(\omega_i|x_1, x_2, \dots x_n)$, cuya definición matemática se presenta a continuación. Es menester indicar que, si bien $P(x)$ i.e., la función de densidad de probabilidad del vector característico x, figura dentro de la ecuación subsecuente, en diversas implementaciones del clasificador suele ignorarse dada su constancia.[5]

$$P(\omega_i|x) = \frac{P(\omega_i) \cdot \prod_{k=1}^{n} \mathcal{N}(x_k;\ \mu_i\ , \sigma_i)}{P(x)}$$

[5] $P(x)$ es denominada una constante de normalización. La función de este parámetro es ajustar el *likelihood* del numerador a una *probabilidad* en rango [0,1]. Como es posible observar $P(x)$ no es afectada por el argumento ω_i ingresado i.e., éste será idéntico en cada instancia, pues la colección de datos es fija. Sin este valor $P(\omega_i|x)$ podría generar valores superiores a 1, pero la lógica de comparación del clasificador seguirá siendo funcional.

Una vez que se dispone de las probabilidades *a posteriori* se busca la clase ω_i que genera el máximo valor $P(\omega_i|x)$. El vector característico es subsecuentemente asignado a ω_i (Larrañaga, Inza y Moujahid, 1997). Dicho razonamiento se describe a continuación:

$$\text{Si } P(\omega_i|x) = \max_{M \geq k \geq 1} P(\omega_k|x) \rightarrow x \text{ se clasifica como } \omega_i$$

4.3.5.2. Prueba de Gaussianidad D'Agostino

Una condición fundamental para emplear el antedicho clasificador es que los datos se ajusten a una distribución normal. Para validar esta conjetura, es menester aplicar una *prueba de Gaussianidad.* En este ámbito existen diversas aproximaciones e.g. *Lilliefors, Shapiro-Wilks, Kolmogorov-Smirnov, Andersor-Darling y D'Agostino-Pearson* (Razali y Wah, 2011). Para fines de esta tesis se ha optado por la última i.e., *D'Agostino-Pearson*, debido al alto poder analítico, relativa simplicidad y carácter vanguardista que (Arnold, Iskander y Zoubir, 1995) remarca sobre esta en su publicación *Testing Gaussianity with the characteristic function*.

Para ejecutarla, dada una muestra aleatoria $x = x_1, x_2, \dots x_n$ de $n \geq 20$ observaciones y un nivel de significancia α (Hernández-Loeza, 1995) empíricamente igual a 0.05 o 0.01 (Yadav y Saha, 2020) es menester plantear, en primera instancia, una hipótesis nula y una hipótesis alternativa, cuya definición, debe ser la siguiente (Alonso y Montenegro, 2015):

$$H_0: x \text{ se ajusta a una distribución normal}$$

$$H_1: x \text{ no se ajusta a una distribución normal}$$

El paradigma por el cuál la prueba rechaza H_0 y adopta H_1 o bien evita el descarte de H_0 al no existir evidencia suficiente de H_1 se basa en una cuantificación de las diferencias en curtosis y asimetría estadística entre la muestra evaluada y una distribución normal. Por esta doble verificación, tradicionalmente a la prueba D'Agostino se le etiqueta como *omnibus*

(Wyłomańska, Iskander y Burnecki, 2020). La validación inicia con $\sqrt{\beta_1}$ i.e., el coeficiente de asimetría de x, que idealmente debería ser 0 i.e., denotando ausencia de sesgo. Para validar la existencia de cercanía suficiente entre $\sqrt{\beta_1}$ y 0, relata la prueba, es menester computar el estadístico z_s que se define, según (D'agostino y Belanger 1990) en la forma subsiguiente:

$$z_s = d\ \ln\left(\frac{T}{a} + \sqrt{\left(\frac{T}{a}\right)^2 + 1}\right)$$

Donde:

$$T = \sqrt{\beta_1\left(\frac{(n+1)(n+3)}{6(n-2)}\right)}$$

$$C = \frac{3(n^2+27n-70)(n+1)(n+3)}{(n-2)(n+5)(n+7)(n+9)}$$

$$W = \sqrt{-1+\sqrt{2(C-1)}},\ a = \sqrt{\frac{2}{W^2-1}},\ d = \frac{1}{\sqrt{\ln W}}$$

La antedicha lógica se repite en forma subsecuente para el coeficiente de curtosis i.e., β_2, el cuál idóneamente, i.e., bajo el supuesto de una distribución normal, debería adquirir un valor de 3 (DeCarlo, 1997). A partir de éste (D'agostino y Belanger 1990) definen un nuevo estadístico para validación denominado z_k, cuya definición se presenta a continuación:

$$z_k = \frac{\left(1-\frac{2}{9A}\right) - \left(\frac{1-\frac{2}{A}}{1+G\sqrt{\frac{2}{A-4}}}\right)^{\frac{1}{3}}}{\sqrt{\frac{2}{9A}}}$$

Donde:

$$G = \frac{\beta_2 - \left(\frac{3n-3}{n+1}\right)}{\sqrt{\frac{24n(n-2)(n-3)}{(n+1)^2(n+3)(n+5)}}}$$

$$E = \frac{6(n^2-5n+2)}{(n+7)(n+9)}\sqrt{\frac{6(n+3)(n+5)}{n(n-2)(n-3)}},\quad A = 6 + \frac{8}{E}\left(\frac{2}{E} + \sqrt{1+\frac{4}{E^2}}\right)$$

Para finalizar, la prueba D'Agostino *ominbus* realiza una combinación de los valores previamente determinados mediante un nuevo estadístico i.e., K^2, que es igual a la suma de los cuadrados de z_s y z_k (D'agostino y Belanger 1990). A partir de este indicador, que se asume sigue una distribución chi-cuadrada con dos grados de libertad, se determina p. Con dicha probabilidad ya computada resta sólo responder a la prueba de hipótesis:

$p \leq \alpha \rightarrow$ Se rechaza H_0 i.e., x no se ajusta a una distribución normal

$p > \alpha \rightarrow$ No es posible rechazar H_0 i.e., x parece ajustarse a una distribución normal

4.4 Autenticación

Como se ha mencionado en forma introductoria, la *autenticación* es un procedimiento vital para la seguridad informática, cuyo objetivo es verificar la identidad de un sujeto que pretende ingresar a un sistema restringido o contenido de carácter confidencial (Paul, Baras y Sadler, 2008). Dicho proceso, de gran relevancia y popularidad en diversos ámbitos e.g., en el aseguramiento de edificios y en la restricción de acceso a servidores (Yacoub, 1998), conlleva tres fases: registro, ingreso y autenticación (Hwang, Lee y Tang, 2002). La primera de ellas consiste en recopilar la información personal de un individuo, sus configuraciones de seguridad, políticas de control de acceso y parámetros distintivos i.e., llave o credencial, y resguardarlas en una base de datos (Kim, Lee, 2017). Dicho proceso, por lo general, implica el uso de transformaciones, mayoritariamente criptográficas, que codifican la llave en un

formato humanamente ininteligible previo a su almacenamiento. Esto minimiza el riesgo de exposición en el supuesto de que la base de datos se vea comprometida.

El segundo paso i.e., el ingreso, consiste en recibir las credenciales de un sujeto que afirma ser determinado individuo. Esto, mediante diversas metodologías y plataformas. (Hwang, Lee y Tang, 2002), ejemplifica dicho proceso con la inserción de una tarjeta inteligente en un dispositivo. Durante esta fase, de acuerdo con los autores previamente referenciados, se realizan diversas tareas y consideraciones e.g., asegurar la validez de la credencial proporcionada y vigilar que el contenido de ésta no se vea expuesto a potenciales atacantes. Finalmente, el tercer paso i.e., la autenticación, consiste en verificar la igualdad o similaridad de la credencial con los datos proporcionados al registro, brindando o denegando de manera subsecuente y, en concordancia con lo anterior, el acceso al recurso protegido.

Inherentemente y, dado el procedimiento descrito con anterioridad, en cualquier paradigma de autenticación se ven involucradas dos clases de entidad que deben ser correctamente identificadas: *clientes* i.e., usuarios registrados y con autorización para acceder a un determinado contenido, e *impostores* i.e., individuos que pretenden personificar a un cliente para ganar acceso no autorizado al sistema.

Dicho proceso se asemeja al de identificación, no obstante, la autenticación trabaja con un conjunto abierto de sujetos y realiza comparaciones uno a uno para determinar la pertenencia a cada clase i.e, dado un cliente C con llave o características F_c y un individuo I que pretende ingresar como C con una llave o características F_I, se verifica que $F_C = F_I$ o bien que la similitud $\delta(F_C, F_I) \geq T$ donde T es un umbral de seguridad. Si la condición se cumple, se concluye que I es el cliente, catalogándolo como impostor en caso contrario.

(Ben-Yacoub, 1998). Por su parte, la identificación labora con un conjunto cerrado de sujetos, llámese S, se realizan comparaciones uno a muchos y no se reconocen las antedichas clases de sujetos i.e., clientes e impostores, pues se asume que sólo usuarios registrados participarán en el sistema (Ben-Yacoub, 1998). En este caso, se extrae $\delta(F_I, F_s)\ \forall s \in S$. Se catalogará a I como el $s \in S$ que alcance el máximo valor de similaridad δ. Inherentemente se espera que si $I = C$ el sistema obtenga el máximo $\delta(F_I, F_s)$ cuando $s = C$, de lo contrario se tendrá un fallo del clasificador. Estas problemáticas se analizarán a detalle en secciones subsiguientes.

Ya que se ha presentado un panorama general del término *autenticación*, su objetivo, paradigma aplicativo y diferencias con otros procedimientos similares e.g., la identificación, es menester comentar las metodologías o mecanismos existentes para su implementación. Para ello, cabe señalar, en primera instancia, la existencia de tres posibles aproximaciones para validar la identidad de un sujeto: por *conocimiento* e.g., de una contraseña textual o patrón gráfico, por *posesión* e.g., de una de una tarjeta inteligente o llave electrónica o por *biometría* e.g., mediante huellas digitales (Velásquez, Caro, y Rodríguez, 2017).

La autenticación basada en conocimiento y, específicamente implementada mediante contraseñas es notablemente popular. Esto, principalmente debido a su simplicidad y rapidez. No obstante este paradigma conlleva diversas desventajas. (Chou, Lee, Yu, et al., 2013), por ejemplo, exponen la suceptibilidad casi inherente de ésta metodología a ataques de diccionario e incluso describen cómo el refinamiento de estas agresiones mediante modelos

probabilísticos puede incrementar en un 273% las probabilidades ya elevadas i.e., de entre 10 y 30% (Bishop y Klein, 1995)[6] de descubrir o *crackear* una contraseña[7].

Esta amenaza es por supuesto previsible o, al menos minimizable mediante políticas de seguridad estrictas, donde se obligue a los usuarios a emplear contraseñas complejas y diferentes para cada servicio. No obstante, esto conduce al segundo desperfecto de la metodología: el riesgo de olvido, el cual es potencial si se considera que en promedio un individuo debe recordar en promedio 15 contraseñas diferentes (Ives, Walsh y Schneider, 2004) que generalmente involucran caracteres textuales, numéricos y especiales, así como variabilidad de mayúsculas y minúsculas, dados los protocolos de seguridad vanguardistas[8].

Como se ha mencionado con anterioridad, otra posible metodología para autenticar sujetos es mediante posesión de un elemento ya sea físico o digital que funge como llave. Un ejemplo de implementación de esta metodología es Kerberos, una solución fabricada en 1988 por el *MIT's Project Athena* (Miller, Neuman, Schiller et al., 1988) que consiste en el montaje de un servidor de distribución, desde el cual se generan los denominados *ticket granting tickets* o TGTs i.e., credenciales encriptadas con un NIP que fungen como el elemento llave

[6] Para determinar esta elevada cifra (Bishop y Klein, 1995) solicitaron a diversos administradores de servicios proveer una lista con las contraseñas de sus usuarios. Subsecuentemente se ejecutó un programa de descifrado automático sobre el antedicho conjunto. Los resultados concluyeron que en promedio en un solo día era posible descifrar entre un 10 y 30% de las contraseñas provistas i.e., entre 5 y 15 de 50. Esto, demuestra la debilidad de este paradigma ante ataques automatizados. (Shay y Bertino, 2009)

[7] Otras aproximaciones de mayor complejidad e.g., la de (Kelly, 2010) demuestran cómo incluso mediante la acústica del teclado es posible capturar estas contraseñas.

[8] Para contrarestar este desperfecto en la acualidad suelen emplearse administradores de contraseñas que salvaguardan las credenciales para diversos sitios, requiriendo un solo identificador. No obstante, de acuerdo con (Li, He, Akhawe et al., 2014) estas soluciones presentan diversas vulnerabilidades y deficiencias e.g., permiten el uso de identificadores simples, en algunos casos son suceptibles a ataques por fuerza bruta, o requieren acciones no intuitivas del usuario para evitar la exposición de las credenciales. Para demostrar lo anterior los autores previamente referenciados analizaron cinco administradores de contraseñas basados en web. En un 80% de ellos i.e., 4 los atacantes consiguieron extraer credenciales arbitrarias de los usuarios explotando las antedichas vulnerabilidades.

en posesión. Estos, por ejemplo, permiten el acceso a estaciones de trabajo o servicios de una red. Este paradigma implica dos fases de autenticación. La primera ocurre cuando el usuario ingresa a *Kerberos* para generar el TGT, mientras que la segunda, sucede al ingresar el antedicho *ticket* junto con su NIP ante el denominado *autenticador* que permite finalmente el acceso al servicio o recurso solicitado (Steiner, Neuman y Schiller et al., 1988).

Dado el uso de las antedichas fases de autenticación *Kerberos* es vislumbrado como una alternativa segura y capaz de amortizar ciertas deficiencias del paradigma basado en conocimiento. No obstante esta aproximación sufre de múltiples deficiencias inherentes del esquema basado en *posesión* que fueron expuestas por (Lizama y Gómez, 2003) en el segundo congreso iberoamericano de seguridad informática: el potencial riesgo de extravío o sustracción de los TGTs y su posterior uso por entidades no autorizadas, las cuales no tendrán oposición significativa en su explotación pues "el NIP de la tarjeta, por sí solo, constituye un mecanismo débil de autentificación" (Lizama y Gómez, 2003).

Así pues, tras haber analizado los paradigmas de autenticación basados en conocimiento y posesión junto a sus inherentes deficiencias, resta sólo explorar la alternativa biométrica. Como se ha mencionado de manera introductoria, esta metodología pretende brindar o denegar el acceso a un recurso protegido fundamentándose en las características inherentes del *cliente*. Esto elimina el potencial riesgo de olvido o sobresimplificación de la llave que se ha expuesto en la aproximación basada en contraseñas y a su vez previene el potencial riesgo de extravío o sustracción de las credenciales que (Lizama y Gómez, 2003) han advertido en paradigmas basados en posesión e.g., *Kerberos.*

La autenticación biométrica a su vez se divide en dos posibles aproximaciones: *fisiológica* y *conductual* (Weaver, 2006). La primera hace uso de características corpóreas

únicas, no duplicables e intransferibles del individuo, que permiten distinguirlo casi de manera inequívoca. Algunos ejemplos comúnmente citados por la literatura son el reconocimiento facial, el uso de la huella digital, el reconocimiento de iris y retina, el análisis de la geometría de la palma, entre otros (Bhattacharyya, Ranjan, Alisherov, et al., 2009). No obstante estas alternativas, como se ha evidenciado en la Sección II de este documento, poseen severas deficiencias en materia de seguridad o usabilidad que derivan de su diseño y concepción suceptible a personificaciones con artefactos relativamente simples.

La segunda subcategoría i.e., *conducual,* hace referencia a la identificación de patrones de comportamiento únicos e inherentes del individuo, que permiten distinguirlo de sus semejantes. Algunos ejemplos tradicionalmente listados por la literatura son la escritura, la dinámica de marcha y pulsación de teclas y finalmente la identificación de patrones venales (Bhattacharyya, Ranjan, Alisherov, et al., 2009), (Soni, Gupta, Rao et al., 2010).

Esta tesis, como se ha mencionado con anterioridad, propone y defiende la añadidura de un nuevo paradigma a este conjunto basado en señales electroencefalográficas. Dicha afirmación se sustenta en las observaciones de (Tavor, Jones, Mars, et al., 2016) y (Miller, Donovan, Van Horn, et al., 2009) quienes han demostrado la unicidad de los patrones neuronales entre individuos pese a la realización de tareas mentales semejantes. Sin embargo, para ello existe un extensa labor pendiente e.g., plantear un paradigma para la adquisición y procesamiento de las señales, combatir la problemática de la mutabilidad de las señales electroencefalográficas con el tiempo (Maiorana y Campisi, 2017), diseñar una metodología de validación convenientemente estricta, entre otros ámbitos.

4.5 Indicadores de desempeño en sistemas de autenticación

Como se ha mencionado en la Sección I, cualquier sistema de autenticación biométrico debe establecer una metodología para cuantificar la similitud entre los parámetros físicos o conductuales del sujeto presentados en la fase de *registro* y, subsecuentemente, en la de *ingreso*. Si estos mantienen un grado de concordancia suficiente, el acceso será concedido. De lo contrario, se intuirá que el sujeto es un impostor y se denegarán los recursos solicitados.

En esta metodología de autenticación, cabe recordarlo, no es posible verificar la unicidad entre las muestras proporcionadas en cada fase a diferencia de, por ejemplo, la aproximación basada en contraseñas. Lo anterior dadas las variaciones corporales que se presentan con el tiempo. Algunos ejemplos de la literatura son: los cambios en la dinámica neuronal asociados al humor (Wyczesany, Kaiser, y Coenen, 2008), los cortes o laceraciones en el tejido que impactan la forma de las huellas digitales (Uludag, Ross y Jain, 2004) y finalmente las variaciones sonoras propias del sujeto o resultantes de ruido de fondo en modalidades de reconocimiento de voz (Camlikaya, Kholmatov y Yanikoglu, 2008).

Dado lo anterior, se requiere establecer un margen de error permitido o frontera de seguridad que permite una cierta fluctuación entre lo almacenado al registro y las condiciones observadas al ingreso. Inherentemente, estas fronteras impactan directamente en la efectividad del sistema biométrico. Si el margen es en extremo reducido la posibilidad de que aún sujetos autorizados sean rechazados por el sistema i.e., se genere un falso rechazo o FR, por sus siglas en inglés, es elevado. Esto, derivará en una condición de inaccesibilidad a los recursos protegidos. Si por el contrario el margen es amplio, existe un potencial riesgo de conceder el acceso a impostores, constituyendo una falsa aceptación o FA, de igual forma por sus siglas en inglés, que comprometerá la seguridad del contenido en resguardo.

Para determinar si una frontera de seguridad es adecuada es menester contar con una serie de métricas, cuyos valores dependen de la cantidad de FR y FA que ésta genera y su proporción con respecto a las aceptaciones verdaderas o TA i.e., cuando un *cliente* es aceptado, los rechazos verdaderos o TR i.e., cuando un *impostor* es rechazado o bien el total de accesos intentados i.e., NA. Dichas métricas son comúnmente definidas por la literatura como FRR, i.e., tasa de falso rechazo, FAR, i.e., tasa de falsa aceptación, TER i.e., tasa total de error y TSR i.e., tasa total de éxito o efectividad (Teoh, Samad, Hussain, 2004). Dichas medidas se presentan formal y matemáticamente a continuación:

$$FAR = \frac{FA}{FA + TR}$$

$$FRR = \frac{FR}{FR + TA}$$

$$TER = \frac{FA + FR}{NA}$$

$$TSR = \frac{TA + TR}{NA} = 1 - TER$$

5. Metodología

Para satisfacer el objetivo principal, que consiste en la fabricación de un sistema de autenticación basado en interfaces cerebro-computadora, se propuso un paradigma de trabajo dividido en tres fases: clase genérica, frontera de seguridad y aplicación.

5.1 Fase I

En la primera fase, se siguió la denominada aproximación de "clase genérica", cuya ejecución, a su vez, se desarrolló en 2 subsecciones: *selección de bandas de frecuencia* y *autenticación*. Esto, en concordancia con lo presentado en (Farias-Castro y Salazar-Varas,

2020). Durante esta primera etapa se empleó el “DataSet IIb”, ofrecido públicamente por el instituto de ingeniería neural de la *Technische Universität Graz* para la *BCI competition IV*. La descripción de este recurso se realiza en forma detallada en la Sección 5.4.1.

5.1.1 Selección de bandas de frecuencia

Como se ha mencionado con anterioridad, un proceso clave en la elaboración de cualquier ICC es el preprocesamiento de los datos. Dicha labor, en concordancia con lo estipulado en secciones previas, consiste mayoritariamente en un filtrado de la señal EEG. Para ello, es menester conocer las frecuencias de corte F_L y F_H, entre las cuales se pretende filtrar. Esto, consituye a la fecha un problema de investigación abierto. Así pues, la identificación de dichas F_L y F_H más apropiadas fue el objetivo de esta subetapa.

Para localizarlas, se elaboró un clasificador Gaussiano ingenuo de Bayes que, de manera empírica se entrenó con el 50% de los experimentos disponibles de cada clase y sujeto. Los datos proporcionados al clasificador pasaron por un filtro *Butterworth bandpass* de cuarto orden con una sola banda, determinada por las frecuencias de corte F_L y F_H. Los vectores característicos se generaron empleando la función de desviación estándar $\sigma(x)$. Para garantizar que la información sigue una distribución Gaussiana, se aplicó la prueba D’Agostino *ominibus* y, ante un potencial incumplimiento de dicha condición se ejecutó la meotodología de remoción de *outliers* basada en desviación de la mediana absoluta, tal como se describe en (Leys, Ley, Klein, et al., 2013). En todas las instancias experimentales se empleó la totalidad de canales disponibles.

Para determinar los valores más apropiados de F_L y F_H se siguió una aproximación por fuerza bruta. En ésta, se consideraron todas las combinaciones binarias de sujetos i.e.,

S_{n_1}, S_{n_2} $\forall\, n_1, n_2 \in [1,9]$ tal que $n_1 \neq n_2$. Lo anterior, inherentemente excluyendo todas las combinaciones simétricas irrelevantes de tipo (n_1, n_2), (n_2, n_1). En cada instancia del antedicho proceso se evaluó la efectividad de todas las combinaciones posibles y coherentes de F_L y F_H e.g., en la primera iteración, se analizó el desempeño del clasificador al distinguir entre S_1 y S_2, dadas las frecuencias de corte $F_L = 1$ y $F_H = 2$. Subsecuentemente se evaluó el desempeño al establecer $F_L = 1$ y $F_H = 3, \ldots, F_L = 1$ y $F_H = 49$. Al finalizar, se analizó la efectividad dado $F_L = 2$ y $F_H = 3$. Este proceso se repitió hasta $F_L = 48,\ F_H = 49$. Una vez concluida la búsqueda se ajustó la combinación de sujetos e.g., a S_1 y S_3, efectuando nuevamente las evaluaciones previamente descritas. La combinación de frecuencias F_L y F_H que alcanzó el mejor desempeño para cada combinación de S_{n_1} y S_{n_2} fue almacenada.

Al finalizar la aproximación por fuerza bruta, se recopilaron los datos almacenados y, con éstos, se elaboraron dos gráficos de barras que cuantificaron las apariciones de cada banda de frecuencia $\in [1,49]$ entre el conjunto de ideales. Para fines de ejemplificación asuma que $F_L = 1$ y $F_H = 5$ determinan la banda de filtrado más efectiva para una combinación de sujetos S_{n_1}, S_{n_2}. Por lo tanto, se sumaría 1 al conteo de apariciones de 1 a 5Hz. Posteriormente, asuma que $F_L = 2$ y $F_H = 4$ determinan una segunda banda de filtrado ideal para una combinación de sujetos S_{n_1},, S_{n_2}, diferente. En este caso se sumaría 1 a las apariciones de las frecuencias 2-4Hz. Esto, generaría un gráfico donde las frecuencias 1 y 5Hz poseen una única aparición mientras que, las comprendidas en el rango 2-4 tienen 2. Asumiendo que no hay más combinaciones de sujetos, podría concluirse que la banda con mayor número de intersecciones es la más efectiva de manera global i.e., 2-4Hz.

5.1.2 Autenticación

En éste punto, se pretendió analizar el desempeño del clasificador Gaussiano ingenuo de Bayes al distinguir entre un *cliente* y un *impostor.* Lo anterior, explotando la banda de frecuencia de mayor utilidad. Para ello, se fabricaron dos clases denominadas *cliente* y *genérica.* El entrenamiento de la primera consistió en el 50% de los datos de un sujeto *aislado,* llámese S_k. Por su parte, el entrenamiento de la segunda clase i.e., la *genérica,* se compuso de una mezcla del 50% de los datos de cada $S_n \forall n \mid n \neq k$.

Ante esta lógica, y, dado un nuevo vector característico $\vec{x}$ extraído del 50% de experimentos restantes de un sujeto cualquiera, es posible concluir que si $\vec{x}$ pertenece a S_k y el clasificador concluye *cliente,* se ha producido un TA. Si por el contrario, el clasificador concluye *genérica,* se ha producido un FR. De manera análoga, si se toma $\vec{x}$ de algún sujeto S_n donde $n \neq k$ y el clasificador concluye *cliente,* se considera un FA, mientras que, si el clasificador concluye *genérica,* se asume la aparición de un TR. Con la cuantificación de frecuencia de aparición de estos escenarios, fue posible computar los indicadores globales FRR, FAR, TER y TSR, que permitieron vislumbrar la efectividad del paradigma. Así pues, la metodología a seguir en la fase I se sintetiza en el gráfico subsecuente:

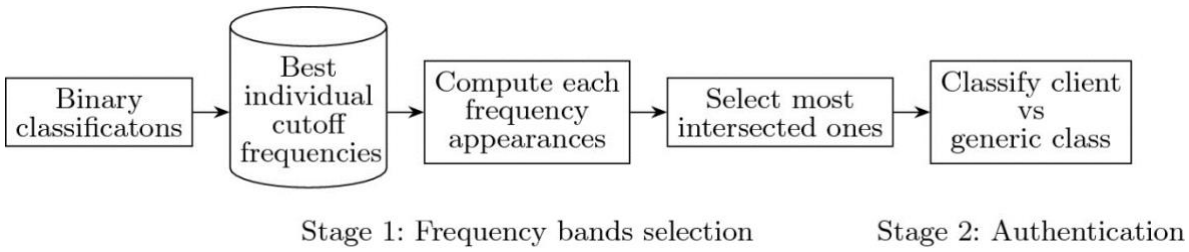


Figura 3. Metodología de la fase I. El proceso se divide en dos etapas i.e., *selección de bandas de frecuencia* y *autenticación.* Este recurso gráfico se incluyó en la publicación *Person Authentication Based on Standard Deviation of EEG Signals and Bayesian Classifier* de 2020.

Con el procedimiento anterior, se demostró la factibilidad de un sistema de autenticación basado en señales EEG. No obstante, como es posible intuir, la conformación de la clase genérica, que permite el funcionamiento de la solución en la fase I, conlleva un elevado costo computacional. Para solucionarlo, era menester diseñar una alternativa que no requiera de su conformación. Este nuevo paradigma fue el objetivo de la fase II.

5.2 Fase II

En esta etapa se efectuaron un total de siete pruebas i.e., *piloto,* de *combinación de movimientos e incremento de bandas,* de desempeño en *diferentes días,* empleando *múltiples características,* con *bandas específicas al usuario,* de *reducción decaracterísticas y del conjunto de entrenamiento* y, finalmente de *generalización.*

5.2.1 Prueba piloto

Durante esta prueba se planteó una nueva aproximación para categorizar a un sujeto como *cliente* o *impostor*, basándose en una frontera. Con ésta, se validó que un nuevo vector característico $\vec{x}$ i.e., los datos proporcionados al acceder al sistema, fuesen lo suficientemente parecidos a los de entrenamiento como para validar la identidad de un sujeto. Para establecer la frontera se seleccionó a un sujeto cliente, llámese S_k, y se computó un vector de medias y desviaciones estándar $\vec{\mu}, \vec{\sigma}$ extraído a partir de los vectores característicos de entrenamiento, que nuevamente fueron el 50% de los experimentos disponibles de dicho sujeto.

Subsecuentemente, por cada vector característico $\vec{v}$ en dicha colección, se computó el coeficiente de correlación producto-momento de Pearson de éste contra $\vec{\mu}$ y, asumiendo que $\vec{\mu}, \vec{\sigma}$ constituyen una clase, la probabilidad de pertenencia de $\vec{v}$ a ésta. Al finalizar, se extrajo la menor correlación y probabilidad cuantificada y se establecieron éstos valores como la

frontera de cada parámetro. Una vez completado dicho proceso se autenticaron los vectores característicos restantes del sujeto S_k y la totalidad de vectores disponibles de cada sujeto $S_n \; \forall n \; \in [1,9] \mid n \neq k$. Bajo esta nueva lógica si un vector $\vec{x}$ perteneciente a S_k supera la frontera se contabilizaría un TA, mientras que, en caso contrario, se consideraría un FR. De manera análoga si $\vec{x}$ pertenece a algún $S_n \mid n \neq k$ y el sistema determina que la frontera de correlación y probabilidad no es excedida, se contabilizaría un TR, o un FA en caso contrario. Nuevamente, con la frecuencia de cada escenario se determinó el indicador global de desempeño TSR, que permitió vislumbrar la efectividad del nuevo paradigma.

5.2.2 Combinación de movimientos e incremento de bandas de frecuencia

En este punto se analizó el impacto en la efectividad de la solución previa al introducir una mayor cantidad de bandas de frecuencia en el filtrado y, al establecer como condición que, para permitir un ingreso se debe contar con la aprobación de un experimento tanto de la mano izquierda como derecha i.e., de la clase ω_1 y ω_2.

5.2.3 Desempeño en diferentes días

En esta etapa se separaron los datos de entrenamiento en sesiones y, se modificó el paradigma de entrenamiento y acceso, empleando ahora, en vez del 50% de experimentos disponibles de un sujeto S_k para el entrenamiento, la totalidad de datos disponibles de éste en una sesión δ_k. El acceso, subsecuentemente, se realizó con datos de una $\delta_n \; \forall n \; \in [1,3] \mid n \neq k$. Esto, permitió analizar el impacto de las variaciones en la actividad cerebral, inherentes del paso del tiempo, en la efectividad general del sistema de autenticación.

5.2.4 Múltiples características

Posteriormente y, a fin de dar mayor robustez al sistema, se evaluó la efectividad de la metodología al incorporar la desviación de la mediana absoluta, el rango intercuartilico y la dimensión fractal de *Katz* a la entonces única función de desviación estándar, utilizada para computar el vector característico.

5.2.5 Incorporación de bandas específicas al usuario

Subsecuentemente, se probó la efectividad del sistema cuando, en añadidura a las frecuencias de corte globales ideales se identificaron las frecuencias de mayor utilidad para cada sujeto S_n y éstas, se utilizaron tanto para entrenar a un nuevo sujeto como para autenticarlo.

5.2.6 Reducción de características y del conjunto de entrenamiento

Al terminar, se analizó el desempeño del sistema al reducir el número de características y su robustez ante una reducción gradual del número de experimentos disponibles para el entrenamiento de N hasta sólo 2. Este proceso fue de vital relevancia, pues permitió el uso de la metodología en una aplicación real que no requiere datos excesivos para un alta.

5.2.7 Generalización

Para esta sección se utilizó una base de datos registrada por el propio grupo de investigación. Su descripción se presenta en la Sección 5.4.1. Sobre este recurso, se repitió el paradigma de entrenamiento y autenticación basado en fronteras que se concibió hasta la prueba número 6 i.e., reducción de características y del conjunto de entrenamiento. No obstante, dado que en esta base de datos no se condujo una aproximación por fuerza bruta como la descrita en la fase I, se ignoraron meramente las bandas específicas al usuario. El resultado de esta prueba

permitió validar si el paradigma propuesto se sostiene aún con sujetos y condiciones de recopilación e.g., canales, diferentes.

5.3 Fase III

Finalmente, en la fase III se retomó la metodología previamente validada y, con ella, se fabricó una interfaz gráfica que emplearía el lenguaje de programación Python 3, las librerías *Tkinter*, *Threading, Brainflow* y una base de datos relacional. Este aplicativo, que constituye el producto final de esta tesis, permitió a usuarios reales utilizar el servicio de autenticación basado en señales electroencefalográficas.

5.4 Bases de datos

5.4.1 Dataset IIb

Esta base de datos almacena la actividad EEG de 9 sujetos $S_1, S_2, \dots S_9$ al imaginar el movimiento de la mano izquierda y derecha i.e., clases ω_1 y ω_2. Las señales de cada sujeto son representadas con matrices $A_1^{\omega_1}, A_1^{\omega_2}, A_2^{\omega_1} \dots A_9^{\omega_2}$ de $C \times M \times E$ donde $C = 3$ especifica el número de electrodos bipolares utilizados i.e., C1, C4 y Cz, $M = 500$ indica el número de muestras tomadas por experimento i.e., 2 segundos intermedios multiplicados por la frecuencia de muestreo de 250Hz y E el número de experimentos no-artefacto, disponibles.

Por cada sujeto, el *dataset* alberga 5 sesiones de grabación, efectuadas en diferentes días. Las primeras dos se desarrollaron sin *feedback,* componiéndose cada una de 6 corridas de 10 experimentos por clase i.e., se dispone de un total de 60 experimentos tanto de ω_1 como de ω_2. Cada prueba en dichas sesiones tuvo un periodo de imaginación de 4 segundos. En las últimas 3 sesiones se ejecutaron 4 corridas de 20 experimentos por clase. En éstas se

incorporó *feedback* y se estableció el periodo de imaginación de 4.5 segundos. Información adicional sobre este recurso puede consultarse en (Leeb, Brunner, Müller-Putz, et al., 2008).

Para fines de esta tesis se laboró meramente con las primeras 3 sesiones, lo que implicó la disponibilidad de hasta 200 experimentos E por clase i.e., $E = 60 + 60 + 80$. No obstante, de acuerdo con (Leeb, Brunner, Müller-Putz, et al., 2008), los elementos considerados por analistas expertos como "artefactos" se removieron del *dataset*. Esto redujo la disponibilidad a entre 159 y 166 experimentos.

5.4.1 Nuevo *dataset* conformado por el equipo de investigación

Este recurso alberga en formato de compatibilidad para MATLAB las grabaciones EEG de 4 nuevos sujetos S_n durante la realización de las mismas clases de tarea mental que en el *dataset IIb* i.e., movimiento de la mano izquierda y derecha i.e., ω_1 y ω_2. Para la recopilación de datos se empleó el módulo OpenBCI Cyton con frecuencia de muestreo de 250Hz. Los canales utilizados en esta nueva instancia fueron C3, CP1 y C4, en concordancia con el estándar internacional 10-20. Para la conformación de esta base de datos se efectuaron dos sesiones en un mismo día, cada una constituida por 40 experimentos de ω_1 y ω_2.

6. Resultados y discusión

6.1 Fase I: Sistema de autenticación basado en una clase genérica

6.1.1 Selección de bandas de frecuencia

Como se mencionó en el apartado de metodología, el desarrollo del primer experimento en la fase I requeriría del *dataset IIb*. Dado que se cuenta con el registro de EEG de 9 individuos, el número total de combinaciones binarias entre sujetos S_{n_1} y S_{n_2} fue de 36. Las dos clases a considerar ω_1 o ω_2 corresponden a imaginación del movimiento de mano derecha o mano

izquierda, respectivamente. Las señales de cada sujeto son representadas en matrices $A_1^{\omega_1}, A_1^{\omega_2}, A_2^{\omega_1} \ldots A_9^{\omega_2}$ de $C \times M \times E$ donde $C = 3$ representa el número de electrodos bipolares utilizados i.e., C1, C4 y Cz, $M = 500$ indica el número de muestras consideradas por experimento i.e., 2 segundos con una frecuencia de muestreo de 250Hz y $E \in [159,166]$ representa el número de experimentos útiles i.e., no-artefacto, disponibles.

Posteriormente y, dando inicio al proceso iterativo, se seleccionó una permutación de sujetos e.g., S_1 y S_2, una clase de movimiento, ω_1 o ω_2, y se extrajeron los datos de cada sujeto en dicha clase e.g., $A_1^{\omega_1}, A_2^{\omega_1}$. Los datos pasaron por un filtro Butterworth paso-banda de cuarto orden con frecuencias de corte F_L y F_H. Sobre los datos resultantes, se aplicó un proceso de extracción de características, empleando como única función la desviación estándar. Esto, modificaría la forma de la señal a $C \times 1 \times E$, que es idéntico a $C \times E$ i.e., se dispone de E vectores característicos de cardinalidad $C = 3$.

Previo al entrenamiento del clasificador, se realizó la prueba D'Agostino *omnibus* con α empíricamente igual a 0.01. Puesto que en la mayoría de casos observados esta condición fallaba, fue necesario introducir el método de detección de *outliers* basado en desviación de la mediana absoluta o MAD descrito por (Leys, Ley, Klein, et al., 2013). Este, suprime los datos que sobresalen de la antedicha distribución, "ajustando" el resto de valores.

Durante este proceso se computó la mediana $\tilde{x}$ y la MAD de los E experimentos disponibles en cada uno de los C canales de recopilación, con estos valores, se estableció un umbral $T_n \forall n \in [1, C]$ de $\tilde{x} \pm 3.5\, MAD$. Cualquier vector $\vec{x}$ con al menos un $\vec{x}_n$ fuera del umbral establecido por su correspondiente T_n es considerado *outlier*. Tras remover dichos valores y ejecutar nuevamente las pruebas D'Agostino *omnibus,* se observó un ajuste a la

distribución en un 90.51% de las pruebas, con apenas un 10.68% promedio de pérdidas de información, un valor suficiente como para dar continuidad.

Así pues, de los vectores disponibles de cada sujeto, se seleccionaron aleatoriamente el 50% i.e., siguiendo la metodología de validación cruzada. Estos, se usarían para el entrenamiento de un clasificador Gaussiano ingenuo de Bayes. Posteriormente, se solicitaría al mismo determinar la entidad a la que pertenecían los vectores restantes de cada sujeto, de modo tal que un $\vec{x}$ perteneciente a S_{n_1} pero clasificado como S_{n_2} o viceversa constituye un error, mientras que un vector correctamente asociado a su autor representa un acierto. Así pues, la efectividad de una ronda del clasificador se cuantifica como la proporción entre aciertos y pruebas ejecutadas. Para validar que la selección de datos de entrenamiento y clasificación no influyesen en el resultado, en añadidura a la selección aleatoria, el antedicho proceso se realizó 30 veces. El desempeño final de una tarea de clasificación es el promedio de efectividades obtenidas en cada iteración.

Una vez realizados los procesos anteriores para cada una de las 36 combinaciones de sujetos, empleando ω_1 y ω_2, así como todas las posibles bandas delimitadas por F_L y F_H, identificar las frecuencias de corte ideales para cada clase de movimiento y permutación de individuos es un proceso trivial. Las tablas 1.1, y 1.2 de la sección de anexos exponen la efectividad máxima alcanzada en cada combinación de sujetos junto a las frecuencias de corte que la han producido. Esto, respectivamente para cada clase de movimiento i.e., ω_1 y ω_2. Ahora bien, como se ha indicado en el apartado de metodología, con base en dicha información es posible elaborar gráficos de barras que cuantifiquen las apariciones de cada frecuencia $\in [1{,}49]$ en el conjunto de ideales i.e., en las enumeradas en las tablas 1.1, y 1.2.

Con estos, es posible identificar las bandas de frecuencia globalmente más efectivas. Lo anterior, seleccionando a aquellas que presenten un mayor número de intersecciones. Las figuras 5 y 6 de la sección de anexos, que corresponden con dichos gráficos para ω_1 y ω_2, muestran que las bandas más efectivas bajo la lógica antedicha son aproximadamente 36-43, 4-8 y 23-35Hz. Por ello, se usarán en el filtrado en la próxima etapa i.e., *autenticación.*

6.1.2 Autenticación con clase genérica

Para finalizar y, nuevamente en concordancia con lo establecido en (Farias-Castro y Salazar-Varas, 2020), se dio paso a la segunda subsección de la fase I i.e., *autenticación.* En ésta se pretendía analizar el desempeño del clasificador Gaussiano ingenuo de Bayes para identificar a un *cliente* y un *impostor.* Para ello, se seleccionó, en primera instancia, a un sujeto *cliente* o *aislado* e.g., S_1 y un tipo de movimiento e.g., ω_1. Posteriormente, y con base en dicha selección se determinaron las matrices que conformarían la clase *cliente* y *genérica*. Cabe recordar que el entrenamiento de ésta última se efectúa mediante una mezcla del 50% de los datos de cada sujeto diferente del *cliente.* Así pues, se rescataron las matrices $A_1^{\omega_1}$ para la primera clase y $A_2^{\omega_1}, A_3^{\omega_1}, \dots, A_9^{\omega_1}$ para la segunda. En cada una se aplicó un filtro Butterworth *bandpass* de cuarto orden que produciría 3 bandas de frecuencia: 36-43, 4-8 y 23-35Hz.

Cabe recordar que hasta antes de este procedimiento, la forma de cada matriz era $C \times M \times E$ donde $C = 3$ representa el número de electrodos bipolares, $M = 500$ indica el número de muestras consideradas por experimento y E representa el número de experimentos útiles disponibles. No obstante, en este punto, dada la introducción de múltiples bandas de filtrado, la anterior dimensionalidad se vería incrementada con $B = 3$, de modo que la forma

resultante es $B \times C \times M \times E$. Por ello, al realizar la subsecuente extracción de características, nuevamente empleando la función σ, la forma resultante sería $B \times C \times E$.

Al concluir dicha labor, se daría paso al proceso de remoción de *outliers* basado en desviación de la mediana absoluta. Al aplicar esta lógica, en cada matriz se obtuvo una estructura idéntica i.e., $B \times C \times E'$ con $E' \leq E$. Ahora bien, en este punto, cada combinación frecuencia-canal podría vislumbrarse como una característica. Por lo tanto, se optó por redimensionar la matriz a la forma $BC \times E'$ i.e., obteniendo E' vectores característicos $\vec{x}$ de cardinalidad $BC = 9$. Con ello se dio fin al preprocesamiento de los datos.

Así pues, se daría paso al entrenamiento del clasificador. Para ello, se extrajo el 50% de los experimentos disponibles de cada sujeto. El conocimiento de la primera clase i.e., la *cliente,* se estableció computando la media y desviación estándar de cada canal en los datos del sujeto *aislado* e.g., S_1, mientras que en el caso de la clase *genérica* dicho entrenamiento se efectuó calculando media y desviación estándar de las muestras seleccionadas de todos los sujetos restantes e.g., $S_2, S_3, \ldots S_9$. Para finalizar, se daría paso a la clasificación utilizando como datos de prueba los experimentos restantes.

Tras repetir el antedicho proceso con todas las posibles selecciones de sujetos *aislados* e *impostores* i.e., miembros de la clase *genérica,* se obtuvo un FRR promedio de ~6%, un FAR y un TER medio del 5.18%, y un TSR promedio del 94.82% para la clase de movimiento ω_1, mientras que para la clase ω_2 se produjo un FRR, FAR y TER medio del 5.94%, con un TSR promedio del 94.06%. Estos resultados pueden constatarse con los valores presentados en las tablas 1.3 y 1.4 de la sección de anexos. Como conclusión de esta primera fase es posible afirmar que las efectividades obtenidas son ciertamente prometedoras y que éstas sustentan

la posibilidad de un aplicativo real dado que requieren de un escaso número de canales, por no mencionar que la metodología de trabajo es relativamente simple. No obstante, esta es optimizable mediante una remoción de la antedicha clase genérica, que inherentemente incrementa el costo computacional y limita la escalabilidad de la solución.

6.2 Fase II: Sistema de autenticación basado en fronteras

6.2.1. Prueba piloto

Para dar inicio a la prueba piloto de esta fase, se dispuso nuevamente del *dataset IIb*, enlistado en la sección de metodología. Como se demostró en la fase I y en (Farias-Castro y Salazar-Varas, 2020) el filtrado de la señal en el conjunto de frecuencias de corte ideales i.e., 36-46Hz, 4-8Hz y 23-35Hz, es fundamental para lograr una autenticación eficiente. Por ello, en esta aproximación las señales pasaron nuevamente por un filtro *Butterworth* de cuarto orden donde se mantuvieron exclusivamente las frecuencias antedichas. Este proceso inherentemente generó una dimensión adicional en las matrices i.e., $B = 3$ i.e., el número de bandas de frecuencia.

Subsecuentemente, se dio paso a la extracción de características, concretamente, la desviación estándar. Con ello, se logró una reducción en la dimensionalidad de las matrices $A_n^{\omega_k}$, a la forma $B \times C \times E$ i.e., restando E vectores característicos $\vec{x}$ de cardinalidad 3 filtrados en B bandas. Al concluir la antedicha labor, se aplicó sobre el resultado el ya aludido proceso de remoción de *outliers* basado en desviación de la mediana absoluta. Esto redimensionaría la matriz a la forma $BC \times E'$ i.e., obteniendo E' vectores característicos $\vec{x}$ de cardinalidad $BC = 9$. Con ello se dio fin al preprocesamiento de los datos.

Así pues, se seleccionaron las matrices modificadas $A_n^{\omega_1}$ y $A_n^{\omega_2}$ correspondientes al sujeto S_n y, nuevamente de forma empírica y aleatoria, se eligió el 50% de los E' experimentos en cada una para fines de entrenamiento. De estos se computó σ_n, μ_n $\forall n \in [1, BC]$ i.e., la media y desviación estándar de cada característica, generando así dos vectores de conocimiento $\vec{\sigma}$ y $\vec{\mu}$ de cardinalidad 9 por cada clase de movimiento ω_k. Al finalizar, dado que en esta fase la lógica de comparación de probabilidades del clasificador ingenuo de Bayes no aplicará dado que no se constituirá una clase genérica, era menester establecer una nueva metodología de autenticación que se basaría en una frontera de decisión. Esta permitiría al sistema identificar si el nuevo $\vec{x}$ dado es suficientemente similar a los datos de entrenamiento, permitiendo o no su acceso i.e., autenticando, sin depender de la repudiada clase genérica.

Una primera aproximación fue el uso del coeficiente de correlación producto-momento de Pearson r dado su uso para la determinación de similaridad entre usuarios en sistemas de recomendación (Sheugh y Alizadeh, 2015) y entre huellas digitales cromatográficas en la medicina tradicional China (Yong-suo, Qing-hua, Rong et al., 2004) . Esta medida de asociación que permite "cuantificar la intensidad de una asociación lineal entre dos variables" (Sedgwick, 2012) e.g., a y b, se define de forma subsiguiente:

$$r = \frac{\sum_{i=1}^{n}(a_i - \bar{a})(b_i - \bar{b})}{\sqrt{\sum_{i=1}^{n}(a_i - \bar{a})^2} \cdot \sum_{i=1}^{n}(b_i - b)^2}$$

En la anterior función $\bar{a}$ y $\bar{b}$ representan la media de n observaciones a_i y b_i en a y b respectivamente, mientras que la salida i.e., r es un valor real $\in [-1,1]$, donde 1 representa una alta relación positiva y -1 una alta relación inversa entre a y b. El valor 0, por su parte, denota la ausencia de relación alguna entre las variables introducidas.

Volviendo al objetivo y contexto en que la antedicha métrica se usaría, se computó r brindando como a cada uno de los $E_{ent} = \lfloor E'/2 \rfloor$ vectores característicos $\vec{x}$ de entrenamiento y $\vec{\mu}$ como b i.e., el vector de conocimiento con valores medios. Lo anterior se repitió para ambas clases de movimiento: ω_1 y ω_2 i.e., mano izquierda y derecha. Al concluir, se empleó la función de agregación *mínimo* para localizar la menor correlación que tiene un $\vec{x}$ realmente perteneciente al sujeto S_n. Se determinó que generalmente $\forall a | a$ pertenece a S_n: $r(a, \vec{\mu}) \geq 0.72$. Así pues este valor se estableció como una primera frontera de decisión.

La observación previa permite generar inherentemente la siguiente función booleana $\theta_1(\vec{x})$. Esta determina si el experimento o vector característico $\vec{x}$ de un sujeto a autenticar, según su correlación con los datos de entrenamiento, i.e., del sujeto registrado S_n es aceptado, en cuyo caso devuelve verdadero, o rechazado i.e., en caso contrario.

$$\theta_1(\vec{x}) = T \leftrightarrow r(\vec{x}, \vec{\mu}) \geq 0.72, \quad \theta_1(\vec{x}) = F \leftrightarrow r(\vec{x}, \vec{\mu}) < 0.72$$

Continuando con la exploración de potenciales métricas y fronteras de decisión se consideró factible extrapolar parte de la lógica previamente explotada en el clasificador de Bayes, adaptándola inherentemente a la falta de una clase genérica. En este, tal como se expuso en la fase I, suele computarse la altura de la curva gaussiana $\mathcal{N}$ dado $\vec{x}$ y los vectores de entrenamiento $\vec{\mu}, \vec{\sigma}$. Subsecuentemente, se multiplica el resultado por la probabilidad *a priori* de una clase para determinar la probabilidad *a posteriori* i..e., de pertenencia a ésta. En este caso, sin embargo, dado que la probabilidad *a priori* de ambas clases es idéntica, pues se usa un mismo número de experimentos para el entrenamiento de cada una, la multiplicación por este valor es irrelevante, por lo que puede suprimirse del modelo:

$$\mathcal{N}(\vec{x};\ \vec{\mu},\vec{\sigma}) = \prod_{n=1}^{C} \frac{1}{\vec{\sigma}_n\sqrt{2\pi}} e^{-\left(\frac{\vec{x}_n-\vec{\mu}_n}{2\vec{\sigma}_n}\right)^2}$$

Típicamente, en un clasificador ingenuo de Bayes, tras computar un conjunto de $\mathcal{N}_1$, $\mathcal{N}_2$ ... $\mathcal{N}_k$ dado $\vec{x}$ y los vectores $\vec{\mu},\vec{\sigma}$ de cada clase se identifica el máximo valor de dicha colección y $\vec{x}$ se clasifica como miembro de la clase que representa. Si bien en esta nueva aproximación el antedicho conjunto de valores $\mathcal{N}$ no estará disponible, esta métrica puede ser igualmente decisiva si en vez de emplearla como método de comparación de probabilidades de pertenencia a clases se vislumbra como una frontera i.e., permitiendo establecer una probabilidad mínima de pertenencia.

Esta lógica puede vislumbrarse también aplicada en la literatura. Por ejemplo, (Park, 2008) describe cómo en aplicaciones donde se requiere la clasificación de pixeles para garantizar la calidad en la producción de aves de corral durante la pos-cosecha se suele establecer una frontera mínima de probabilidad de pertenencia a una clase para garantizar que un pixel sólo sea clasificado si éste logra un $\mathcal{N}$ mínimo. Con ello, se evita poblar una clase de un número sustancial de elementos que pese a disponer de la máxima probabilidad de pertenencia son tan poco similares que potencialmente serán un fallo del clasificador.

Ahora bien, tras haber establecido la lógica con que se establecería la segunda frontera, es menester asignarle un valor y construir una función booleana derivada de ésta. Aplicando el mismo paradigma que se utilizó con la correlación producto-momento de Pearson se computó $\mathcal{N}$ proporcionando como argumentos cada uno de los E_{ent} vectores característicos $\vec{x}$ de entrenamiento, $\vec{\mu}$ y $\vec{\sigma}$ i.e., los vectores de conocimiento con valores medios y desviaciones estándar. Nuevamente, lo anterior se repitió para ambas clases de

movimiento: ω_1 y ω_2 i.e., mano izquierda y derecha. Al concluir, se empleó la función de agregación *mínimo* para localizar la menor probabilidad que tiene un $\vec{x}$ realmente perteneciente al sujeto S_n. Se determinó que $\forall \vec{x} \mid \vec{x}$ pertenece a S_n: $\mathcal{N}(\vec{x};\ \vec{\mu}, \vec{\sigma}) \geq 0.76$. Así pues el antedicho valor se estableció como una segunda frontera de decisión.

La observación previa permite generar la función booleana $\theta_2(\vec{x})$, cuyo paradigma operativo se asemeja al de θ_1. Esta, se define de la forma subsiguiente:

$$\theta_2(\vec{x}) = T \leftrightarrow \mathcal{N}(\vec{x};\ \vec{\mu}, \vec{\sigma}) \geq 0.76, \quad \theta_2(\vec{x}) = F \leftrightarrow \mathcal{N}(\vec{x};\ \vec{\mu}, \vec{\sigma}) < 0.76$$

Ahora bien, dado que ambas funciones toman la misma entrada y devuelven un valor booleano, es posible concatenarlas generando $\theta_3(\vec{x})$ que valida ambas condiciones:

$$\theta_3(\vec{x}) = T \leftrightarrow \theta_1(\vec{x}) \wedge \theta_2(\vec{x}), \quad \theta_3(\vec{x}) = F \leftrightarrow \neg\theta_1(\vec{x}) \vee \neg\theta_2(\vec{x})$$

Una vez establecidas las antedichas funciones se tomaron los $E_{clasif} = \lceil E'/2 \rceil$ vectores de clasificación $\vec{x}$ del sujeto S_n inicialmente seleccionado y se ordenó al programa computar $\theta_3(\vec{x})$ para determinar la superación o incumplimiento de cada uno de las fronteras de correlación y probabilidad previamente establecidas. Como los datos de entrenamiento pertenecen a S_n es posible aseverar que $\theta_3(\vec{x}) \rightarrow F$ constituye un fallo del programa o, formalmente y en el contexto de la autenticación, un FR, mientras que $\theta_3(\vec{x}) \rightarrow T$ implica un acierto o TA (Jain, 2002). Las efectividades resultantes se asentaron en las tablas 2.1 y 2.2, presentes en la sección de anexos.

Subsecuentemente y, de manera análoga, se seleccionó el 100% de los experimentos de cada $S_k\ \forall\ 1 \leq k \leq 9 \mid k \neq n$ y se solicitó al programa ejecutar el paradigma previamente expuesto para determinar la aprobación o rechazo de sus vectores característicos empleando θ_3. En este escenario, dado que los vectores $\vec{x}$ de entrada no pertenecen a S_n i.e., el sujeto

de entrenamiento, es posible aseverar que $\theta_3(\vec{x}) \rightarrow F$ constituye un TR, mientras que $\theta_3(\vec{x}) \rightarrow T$ representa un FA. De igual forma, los resultados obtenidos se asentaron en las tablas 1 y 2. Los experimentos anteriores se repitieron en dos ocasiones, i.e., para: ω_1 y ω_2. Para finalizar, se computó la efectividad promedio de cada clase de movimiento.

Los valores resultantes, cuyos detalles se aprecian en la tabla 2.1 y 2.2 de la sección de anexos, muestran una efectividad promedio de 84.71% empleando ω_1 y de 84.72% al utilizar ω_2. Dichos valores iniciales son prometedores pues indican que el sistema goza de una capacidad, aunque aún ciertamente limitada, de identificar a sujetos. Esto es inherente dado que superan el umbral de la aleatoriedad en el modelo i.e., 50%.

6.2.2. Combinación de movimientos e incremento de bandas de frecuencia

Es menester indicar que si bien las cifras anteriores son ya elevadas, presentan aún un gran número de *falsas aceptaciones*, una condición potencialmente no deseada en el sistema. Buscando su corrección, se probaron diversos incrementos. El primero de ellos fue una combinación de clases i.e., ω_1 y ω_2, de modo que, fuese necesaria la aprobación de un experimento tanto de la mano izquierda como derecha para brindar acceso a un sujeto. Esto, conforma una nueva función booleana θ_4:

$$\theta_4(\vec{x}, \vec{y} \mid \vec{x} \in \omega_1 \wedge \vec{y} \in \omega_2) = T \leftrightarrow \theta_3(\vec{x}) \wedge \theta_3(\vec{y})$$

$$\theta_4(\vec{x}, \vec{y} \mid \vec{x} \in \omega_1 \wedge \vec{y} \in \omega_2) = F \leftrightarrow \neg\theta_3(\vec{x}) \vee \neg\theta_3(\vec{y})$$

Así mismo, se planteó la posibilidad de extender el número de bandas de frecuencia, bajo la esperanza de que una mayor cantidad de datos pudiesen incrementar la efectividad de la solución, decrementando a su vez los casos de FA. Como es posible observar en las figuras 5 y 6 de la sección de anexos, en añadidura a las antedichas bandas 36-43, 4-8 y 23-35Hz

destacan 20-23 y 18-22Hz en frecuencia de aparición como “más útiles”. Así pues, se optó por considerar ambas para esta segunda prueba de la fase II. Al concluir cada una de las adecuaciones antedichas, se repitieron las ejecuciones de la evaluación piloto. Los resultados obtenidos, cuyos detalles se observan en las tablas 2.3 y 2.4 de la sección de anexos, muestran una efectividad global o TSR del 89.56% tras la mera introducción de θ_4 i.e., habiendo proporcionado un incremento de entre 4.84% y 4.85% por la simple combinación de movimientos, y de 91.01% tras incluir, en añadidura a lo anterior, las previamente aludidas bandas de frecuencia i.e., 20-23 y 18-22Hz. Esto, se traduce en un 1.45% de TSR adicional, en su totalidad debido a un decremento de casos de FA. Esta aseveración puede constatarse al observar los ligeros decrementos en TA que el ajuste ha generado. Esto, inherentemente, eleva la cantidad de FR generados por lo que en teoría el TSR debería disminuir. Si a pesar de ello, se registra un incremento, es sin lugar a dudas debido a la baja en el número de FA, que ha superado el error introducido por los nuevos casos de FR.

6.2.3. Pruebas en diferentes días

Habiendo ya alcanzado un TSR razonable y disminuido las instancias de FA, era menester validar que los resultados anteriores fuesen sostenibles en condiciones realistas. En este entorno, como se mencionó en la sección 4, predomina un riesgo potencial para el desempeño de cualquier ICC basada en señales EEG, que deriva de la inestabilidad de éstas con el tiempo (Zheng, Zhu y Lu, 2017). Los datos utilizados hasta este punto, tanto para entrenamiento como para clasificación, son una combinación de tres sesiones de recopilación: δ_1, δ_2 y δ_3 efectuadas en diferentes días. Esta mezcla, de cierto modo ha permitido preliminarmente que el sistema sea inmune a las variaciones, no obstante, cuantificar el impacto de estas es de

gran importancia. Para validar lo anterior se separó, de manera inicial, la información en sesiones y se replanteó el experimento como se presenta de manera subsiguiente.

En primera instancia, se modificó el paradigma de selección de datos tanto para entrenamiento como para autenticación. En contraposición con el particionamiento 50-50 previamente efectuado, en esta nueva instancia de pruebas se optó por entrenar con la totalidad de experimentos disponibles de una sesión, llámese δ_{x_1}. Posteriormente, en el acceso, se emplearían los vectores característicos extraídos a partir de los datos de una segunda sesión $\delta_{x_2} | \, x_1 \neq x_2$. Dada la existencia de 3 sesiones, es posible el planteamiento de 3 permutaciones de interés i.e., $P_A: \{x_1 = 1, x_2 = 2\}$, $P_B: \{x_1 = 1, x_2 = 3\}$ y $P_C: \{x_1 = 2, x_2 = 3\}$. Esto, ignorando combinaciones simétricamente redundantes.

Tras efectuar dichos ajustes en la selección de datos se repitieron los experimentos replicando las condiciones de la prueba de combinación de movimientos e incremento de bandas de frecuencia. Los resultados, cuyos detalles se presentan en las tablas 2.5 a 2.7 de la sección de anexos muestran una sustancial caída en la efectividad que deriva de la variabilidad con el tiempo de las señales EEG. En la primer combinación i.e., P_A el TSR ha disminuido a 67.07% constituyendo una baja de 23.94%. En el caso de P_B la efectividad sufre una merma de 28.63% resultando en un TSR de 62.38%. Finalmente, en el caso de P_C, el TSR se sitúa en 76.40%, producto de una caída ciertamente menor aunque de igual forma significativa de 14.61%. Con esta información, es evidente que un ajuste en el protocolo de autenticación es necesario si se pretende competir con las soluciones en existencia.

6.2.4. Múltiples características

Para dar inicio al proceso de rectificación descrito con anterioridad se optó por introducir un mayor número de características. Esto, implica que para aceptar o rechazar un vector, éste debe ser semejante o divergente en un mayor número de parámetros. No obstante, como se indicó en la sección teórica, es menester que la cardinalidad de dicho vector no se incremente de manera sustancial, ya que de lo contrario el rendimiento de la solución se verá afectado (Nicolas-Alonso y Gomez-Gil, 2012). Por ello se propuso meramente la introducción de las características descritas en la sección 4.3.4 i.e., rango intercuartil, desviación de la mediana absoluta y dimensión fractal de Katz. Esto, en añadidura a la ya utilizada desviación estandar, cuya utilidad se validó previamente para (Farias-Castro y Salazar-Varas, 2020).

De manera inicial esta aproximación parecía poco prometedora. Al cuantificar el TSR de cada característica adicional en forma independiente i.e., sin combinar, se obtuvo respectivamente para las combinaciones de sesiones P_A, P_B y P_C: 66.80%, 60.89% y 71.85% con rango intercuartil, 67.15%, 59.76% y 71.91% con desviación de la mediana absoluta y 57.33%, 58.83% y 66.99% con dimensión fractal de Katz. Estos valores pueden constatarse en las tablas 2.8 a 2.16 de la sección de anexos. No obstante se observó en dichos resultados que las efectividades bajas altas y bajas variaban conforme la característica e.g., al utilizar la permutación de sesiones P_c, entrenando con datos del sujeto 1 y accediendo con vectores del 2, se obtiene un TR en el 8.57% de los casos si la característica σ es utilizada. Si estas mismas condiciones se replican con la dimensión fractal por algoritmo de Katz, el TR se logra en el 100% de los casos. Esto permitía vislumbrar que pese a la falta de eficacia individual, la combinación podría ser de gran utilidad.

Así pues se planteó una nueva regla de aceptación y rechazo θ_5. Para su exposición considere π como un conjunto de F funciones i.e., $\pi = \{\sigma(\vec{x}),\ iqr(\vec{x}),\ MAD(\vec{x}),\ katz(\vec{x})\}$ y $\theta_4(\vec{x}|\ \pi_k)$ como "el estado de verdad de θ_4 con $\vec{x}$ dado el uso de la característica π_k":

$$\theta_5(\vec{x}|\ \pi) = T \leftrightarrow \theta_4(\vec{x}|\ \pi_1) \wedge \theta_4(\vec{x}|\ \pi_2) \wedge \ldots \wedge \theta_4(\vec{x}|\ \pi_F)$$

$$\theta_5(\vec{x}|\ \pi) = F \leftrightarrow \neg\theta_4(\vec{x}|\ \pi_1) \vee \neg\theta_4(\vec{x}|\ \pi_2) \vee \ldots \vee \neg\theta_4(\vec{x}|\ \pi_F)$$

Tras aplicar θ_5 y repetir los experimentos sosteniendo el resto de condiciones i.e., bandas de frecuencia, combinación de clases, etc., se observó de manera casi inmediata una alza en la efectividad a 78.41% con la permutación de sesiones P_A, 74.30% dado P_B y 83.30% con P_C. Con respecto al experimento descrito en la sección 6.2.3 i.e., donde sólo se empleó la desviación estándar, se obtiene una alza de 11.34%, 11.92% y 6.9% respectivamente para cada combinación de sesiones. Esto demuestra que las características adicionales contribuyen al proceso de autenticación, aunque únicamente si se realiza un mezclado de ellas. Los detalles de los resultados anteriores pueden constatarse en las tablas 2.17 a 2.19.

6.2.5. Bandas específicas al usuario

En este punto la efectividad alcanzada es ya razonable. No obstante, las cifras logradas, en su mayoría se encuentran aún por debajo, tanto de las metas establecidas en forma inicial, como de los TSR ofrecidos por otras soluciones. Por lo anterior, era menester continuar con el proceso de rectificación del paradigma. Como se observó con anterioridad, la provisión controlada de una mayor cantidad de datos puede contribuir de manera sustancial a un incremento de la tasa total de éxito. La inclusión de nuevas características podría parecer la aproximación más simple y conveniente para continuar el escalamiento del TSR. Sin embargo, al observar los detalles presentados en las tablas 2.8 a 2.16 de la sección de anexos,

es posible vislumbrar la existencia de casos donde ninguna característica ha logrado un desempeño apropiado, especialmente en instancias donde debe rechazarse a un impostor. Tome por ejemplo la instancia de entrenamiento con datos del S_5 y de acceso con información perteneciente al S_2. Sin importar la característica utilizada la efectividad no supera la frontera de 11.11% y, de hecho, esta sólo es alcanzada parcialmente por la dimensión fractal de Katz, usando la permutación de sesiones P_A. En el resto de escenarios no se ha evitado el acceso.

Por lo anterior, es que, lejos de pretender la adición de mas características, es menester examinar la posibilidad de uso de otro parámetro potencialmente distintivo del sujeto. Como se ha mencionado en la sección número 4, el patrón de actividad cerebral de un individuo es único (Miller y Donovan, 2009). Esto, de acuerdo con algunas observaciones de (Eagleman, Drover, Drover et al., 2018). Dicha unicidad pareciera, de igual forma, vislumbrarse en las bandas de frecuencia en que la actividad de cada sujeto predomina. Esto, puede asumirse a partir de los datos preliminares que permitieron la conformación las gráficas de barras presentadas en las figuras 5 y 6 de la sección de anexos. Tras consultar dicha información, fue posible identificar que en añadidura a las bandas "generales" i.e., de utilidad para identificar a cualquier sujeto, existe la siguiente colección de bandas "específicas" que permiten identificar con mayor exactitud a un determinado sujeto S_n en el movimiento ω_k.

	Movimiento ω_1			Movimiento ω_2		
S_1	39-40	36-38	41-47	39-49	37-38	41-43
S_2	28-34	41-46	11-12	11-12	31-32	41-42
S_3	36-41	42-48	32-34	36-41	35-36	41-45
S_4	33-38	11-12	39-41	4-6	11-12	34-38
S_5	18-19	20-24	25-48	20-21	22-25	27-29
S_6	5-6	21-25		4-7	38-46	38-46
S_7	4-7	36-37	38-46	5-7	37-38	38-45
S_8	31-33	34-36	37-38	32-33	34-36	37-38
S_9	39-40	41-47	47-48	3-6	39-40	41-45

Tabla 2.20 Bandas de frecuencia (Hz) "específicas"
para cada sujeto S_n en el movimiento ω_k

Dada la información presentada en la tabla 2.20, se procedería a repetir la experimentación previa. No obstante, en este caso, se incluirían en el entrenamiento de cada sujeto los datos de sus bandas correspondientes i.e., de modo que *B* se verá incrementado. Al autenticar, se emplearían tanto las bandas generales como específicas del S_n que se afirma ser para determinar la veracidad de la aserción, esperando que, si el sujeto entrante es impostor, sus señales diferirán al menos en las bandas específicas.

De igual forma, dado que se observó un gran número de casos donde TA=0% o muy bajo, indicando que el sujeto es irreconocible en la segunda sesión y que si bien la efectividad es alta, esto se debe a las múltiples instancias de TR, se optó por combinar las sesiones de entrenamiento, tomando datos de δ_{n_1} y δ_{n_2} y accediendo con δ_m, donde $n_1 \neq n_2 \neq m$. Esto, redefiniría las permutaciones a P_A': $\{n_1 = 1, n_2 = 2, m = 3\}$, P_B': $\{n_1 = 1, n_2 = 3, m = 2\}$ y P_C': $\{n_1 = 2, n_2 = 3, m = 1\}$. Los resultados obtenidos con estas adaptaciones, cuyos detalles se presentan en las tablas 2.21 a 2.23 en la sección de anexos, mostraron un TSR de

91.97% con $P_A{}'$, 92.02% con $P_B{}'$ y de 91.59% con $P_C{}'$. Estos valores son destacables pues se ejecutan en un entorno más realista y se asemejan al desempeño de otras alternativas de autenticación en existencia e.g., (Shelupanov, Evsyutin, Konev, et al., 2019).

6.2.6. Reducción de características y del conjunto de entrenamiento

Ya que se ha alcanzado la efectividad esperada del sistema, con un nivel reducido de FAs y un incremento de TAs, es preciso velar por la eficiencia y usabilidad práctica de éste. Para ello, se realizó, en primera instancia, un análisis teórico de las características utilizadas. En éste, se recordó un desperfecto fundamental de la dimensión fractal de *Katz,* que es precisamente su rendimiento. Para validar que el incremento temporal causado por ésta no fuese elevado, se optó por ejecutar la solución, proporcionando como entrada todas las posibles combinaciones de sujetos para entrenamiento y autenticación, aunque empleando como única característica la desviación estándar, cuya importancia es elevada de acuerdo con las observaciones de la fase I, y cuya complejidad de cómputo es relativamente baja.

Al concluir, se repetiría este mismo experimento, empleando ahora la dimensión fractal de *Katz.* Esto, inherentemente planteará un punto de comparación. En el primer caso, el tiempo promedio fue de 3070ms, mientras que, en el segundo, se obtuvieron 4041ms. Esto, plantea un alza del 31.63%, un valor ciertamente significativo. Ahora, si bien esto convierte a la dimensión fractal en un potencial candidato a eliminación, es preciso analizar si su impacto en la efectividad puede justificar su manutención.

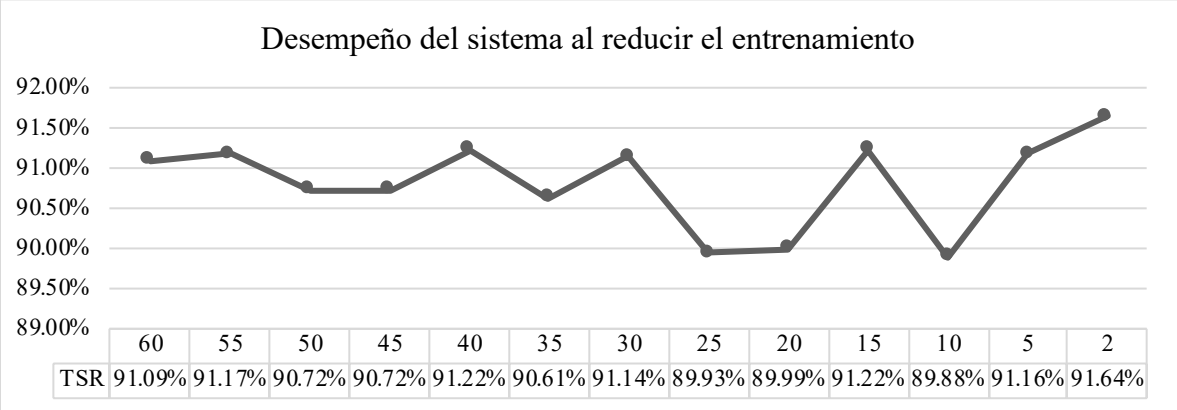
Para ello, se repiteron las labores que derivaron en los resultados presentados en las tablas 2.21 a 2.23, aunque, exceptuando a la dimensión fractal como característica. Esto, produjo un TSR de 90.90% con la permutación de sesiones $P_A{}'$, de 90.65% con $P_B{}'$ y de

91.15% con $P_C{}'$. Dichos valores pueden constatarse examinando las tablas 2.24 a 2.26 en la sección de anexos. Esto implica, respectivamente, una disminución de apenas 1.07%, 1.37% y 0.44% en la efectividad. Dicho valor, ciertamente insignificante, no fundamenta la presencia de dicha característica, por lo que se optó por removerla provisionalmente.

En este punto, se ha velado ya por una optimización del sistema, aunque la usabilidad o practicidad del mismo aún no se ha considerado. Esto, se realizó posteriormente. Como es inherente en cualquier servicio de autenticación, es menester que el volumen de datos necesarios tanto al registro como al ingreso sea reducido, minimizando el tiempo total requerido para validar la identidad y las solicitudes de información al usuario. Hasta este punto el número de experimentos requeridos para el alta de un sujeto eran aproximadamente 60, de los cuáles, en promedio 53 eran conservados i.e., tras la antedicha pérdida del 10.68% dada la remoción de outliers. Así pues se seleccionó aleatoriamente la permutación $P_C{}'$ y se visualizó la efecividad del sistema al reducir gradualmente, en intervalos de 5, hasta 2^9 el número de experimentos utilizados. Esto, produjo el gráfico vislumbrado en la figura 7.

Como es posible observar en este elemento gráfico, el máximo de efectividad es alcanzado al entrenar con 2 experimentos. Con ello, se logra un resultado similar, e incluso superior, al obtenido empleando 60 i.e., con una variación +0.55%. Esto, implica que una minimización del entrenamiento requerido hasta dicho valor es posible sin pérdidas de TSR. Es preciso indicar que, en cada caso, los experimentos usados para entrenar se seleccionan aleatoriamente de los resultantes tras la supresión de *outliers*.

[9] Se optó por este caso dado que inherentemente el entrenamiento con 0 experimentos es imposible y, debido a que 1 único experimento no permite computar una desviación estándar útil, necesaria para la frontera basada en altitud de la curva Gaussiana.



	60	55	50	45	40	35	30	25	20	15	10	5	2
TSR	91.09%	91.17%	90.72%	90.72%	91.22%	90.61%	91.14%	89.93%	89.99%	91.22%	89.88%	91.16%	91.64%

Figura 7. Desempeño del sistema de autenticación durante una reducción del entrenamiento.

6.2.7. Generalización de la metodología

Tras haber obtenido los resultados previos, se hizo posible el planteamiento de un protocolo tanto de recopilación de datos como de autenticación, el cual es aplicable a un entorno realista. Este, requiere el filtrado Butterworth paso-banda de cuarto orden de una señal EEG adquirida en 2 sesiones con 3 canales predominantemente ubicados en la zona centro de la corteza cerebral entre las frecuencias generales 36-43, 4-8, 23-35, 20-23 y 18-22Hz y, si se encuentran disponibles, aquellas bandas asociadas a cada sujeto. De la señal resultante, deben extraerse las características: desviación estándar, rango intercuartílico y desviación de la mediana absoluta. Los vectores resultantes deben pasar por un removedor de *outliers* que suprimirá experimentos con valor fuera del rango de aceptación $MAD \pm 3.5\, mediana$. De éstos, es posible seleccionar 2 en forma aleatoria y entrenar. De seguirse los pasos anteriores, el TSR obtenido se proyecta en aproximadamente 91.64%, una cifra ciertamente competente.

Para validar que dicho modelo es aplicable a otros conjuntos de datos, pese a las variaciones que éstos presenten y el inherente uso de otros sujetos, se fabricó un segundo *dataset*, el cuál, de acuerdo con las especificaciones brindadas en la sección de metodología, alberga, en formato de compatibilidad para MATLAB, las grabaciones EEG de 4 nuevos

sujetos durante la realización de las mismas tareas mentales i.e., movimiento de la mano izquierda y derecha.

Inherentemente, dada la disposición de sólo dos sesiones, fue necesario entrenar con ambas para satisfacer en mayor medida el antedicho protocolo, de modo que, en este caso, $P_A{}'$:$\{n_1 = 1, n_2 = 2, m = 1\}$, $P_B{}'$:$\{n_1 = 1, n_2 = 2, m = 2\}$ y $P_C{}'$ será inexistente. Si bien esto incumple la condición previa $n_1 \neq n_2 \neq m$, en el acceso ningún vector usado para entrenar sería autenticado. Tras aplicar la metodología propuesta se obtuvieron los resultados que se muestran en las tablas 2.27 y 2.28 de la sección de anexos. Estos, muestran un TSR de 93.14% para $P_A{}'$ y de 95.33% para $P_B{}'$, con un FAR de 0.00 en el primer caso y 0.02 en el segundo. Estos valores, potencialmente realistas y deseables en un aplicativo de uso cotidiano superan significativamente el objetivo de 80.37%, suponiendo un primer éxito del proyecto.

6.3 Fase III: Elaboración de un software de aplicación

6.3.1. Módulo de recopilación de datos

Tras haber diseñado tanto un paradigma de adquisición de señales electroencefalográficas como un mecanismo de autenticación de usuarios efectivo en condiciones realistas, se daría paso a la elaboración de un software de aplicación capaz de explotar dicho conocimiento para dar servicio a un usuario final. Como se mencionó en la sección de metodología, el primer paso para ello consistió en la fabricación de un módulo de Python 3 que permitiese recopilar la actividad EEG observada por una tarjeta de adquisición, específicamente OpenBCI Cyton. Para ello, se recurrió a la librería *BrainFlow*, una API uniforme con compatibilidad para C++, C#, Java, MATLAB, Julia, e inherentemente Python, que permite la extracción de diversos tipos de señales e.g., EEG, EMG y ECG de un sinfín dispositivos comerciales disponibles.

Una vez instalado e importado dicho módulo, se procedió a la definición de una clase Lector. El constructor de ésta recibe como argumento el tipo de tarjeta a utilizar e.g., *Cyton, Ganglion, Cyton* con *Daisy* o simulador; una lista de canales a considerar, la frecuencia de muestreo y el puerto en el que se aloja la tarjeta de adquisición e.g., COM3. En el interior de esta clase se define, de igual forma, un método denominado *recopilarDatosExperimento*. Este, recibe como argumento la duración de un experimento, la cantidad de segundos a remover e.g., de una duración de 4s se debe suprimir 1s al inicio y 1s al final, conservando únicamente los dos intermedios; y una función o *callback* a llamar tras completarse la recopilación. El método, se encarga de inicializar el flujo de datos con el casco, esperar el tiempo especificado para la recopilación y, una vez transcurrido este lapso temporal, finalizar la recepción de datos, invocar al *callback* y devolver los datos en forma de matriz $C \times M \times 1$.

Una vez elaborada esta clase, se procedería a validar su funcionamiento. Para ello, el canal 1 de la tarjeta de adquisición OpenBCI Cyton se estimuló con una señal senoidal con frecuencia de 2Hz, amplitud 0.5Vp y *offset* de 0.1V. Una vez realizado lo anterior, se generó una instancia de Lector, solicitando un escaneo de los canales 1, 2 y 3 durante un periodo de 5 segundos. Como es posible observar en la parte izquierda de la figura número 8, que muestra la señal compilada en el dominio del tiempo, existe una coincidencia apropiada con la expectativa: el canal 1 muestra una onda senoidal con los parámetros indicados mientras que los canales 2 y 3 se mantienen en cero. Al finalizar este experimento, la señal senoidal se conectó al canal 2. Los valores resultantes se muestran en la parte derecha del recurso gráfico previamente referenciado. Como es posible observar, el módulo ha respondido nuevamente en forma adecuada.

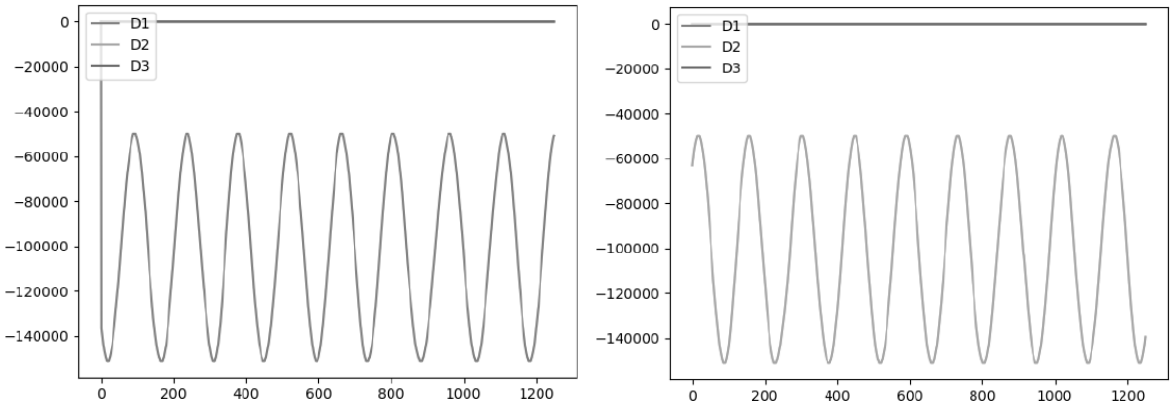


Figura 8. Valores obtenidos por el módulo recopilador de señales. Como es posible observar, la forma coincide con la expectativa, validando el funcionamiento del desarrollo.

6.3.2 Política de aceptación

En este punto se dispone ya de un módulo recopilador de señales de EEG, así como un paradigma de autenticación altamente efectivo y aplicable a entornos realistas. Sin embargo, pese al desempeño favorable de este último, es posible aún vislumbrar la presencia de casos FR y FA. Previamente se ha asumido que un sujeto podrá ser aceptado siempre que un vector característico perteneciente a éste supere las fronteras establecidas. No obstante es posible relajar o endurecer esta política a consideración del usuario final. Para ello, se propusieron 3 niveles de seguridad: *reducido, intermedio* y *máximo.* En cada uno, se requiere la disposición de 5 experimentos, no obstante, el número de muestras aprobadas de dicho conjunto varía. En el primer nivel se propone conceder el acceso con una tasa de aprobación del 20% i.e., 1 de los 5 experimentos. Esto, se espera, minimizará el FRR, aunque, cabe la posibilidad de un incremento en el FAR. En el segundo caso, se propone el ingreso al aprobarse el 60% de los experimentos compilados i.e., 3 de 5. Este nivel será recomendado por defecto en el desarrollo final. Para concluir, se encuentra el nivel de seguridad más elevado i.e., *máximo*. Este, propone el ingreso únicamente si el 100% de los experimentos son aprobados.

Inherentemente esta opción tiene el potencial de reducir significativamente el FAR, aunque puede representar un alza en el FRR.

6.3.3 Base de datos

Una vez desarrollado el módulo de adquisición de datos, así como la política de aceptación, era preciso diseñar una metodología de almacenamiento. Para ello, se procedería, inherentemente, al desarrollo de un esquema relacional de bases de datos empleando el lenguaje de modelado UML, cuya implementación se efectuaría subsecuentemente en el aludido gestor MySQL 8.0.25. Este, se presenta en la figura número 9. Como es posible observar en este modelo, el número de entidades involucradas es sumamente reducido, puesto que únicamente es necesario representar a un usuario y los vectores característicos de entrenamiento que ha proporcionado.

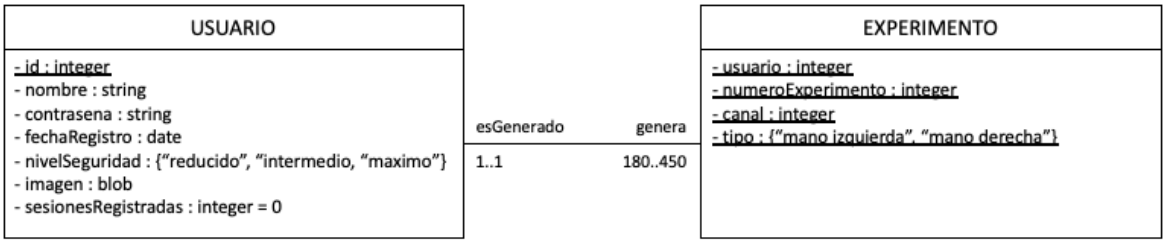


Figura 9. Esquema relacional de la base de datos. El modelo propuesto consta de dos entidades: usuario y experimento. La primera, representa a un sujeto registrado en el sistema, mismo que posee un identificador entero único autoincrementable, un nombre, una contraseña[10], una fecha de registro, un nivel de seguridad i.e., reducido, intermedio o máximo, una imagen y un total de sesiones registradas. La segunda presenta una llave foránea a un usuario, un número de experimento, un número de canal y una clase de movimiento i.e., mano izquierda o derecha

Inherentemente la tabla EXPERIMENTO puede crecer sustancialmente con el transcurso del tiempo, pues en cada sesión de acceso se disponen de nuevos datos que potencialmente son útiles para lograr un reentrenamiento que salvaguarde la efectividad del sistema i.e., es de

[10] Se ha provisto un campo de contraseña para permitir al usuario recuperar el acceso en caso de TR. No obstante, dicho campo puede eliminarse a futuro para evitar los riesgos asociados a su uso.

interés almacenarlos. Esto puede restringir nuevamente la escalabilidad del aplicativo, sin mencionar que, los experimentos longevos y su manutención pueden afectar el desempeño de la solución a futuro. Para tratar dichos inconvenientes se buscará que el software final, ante un caso de ingreso elimine de la base de datos la información de mayor antigüedad. Posteriormente, ingresará los nuevos datos i.e., los vectores utilizados para autenticarse, procurando que el número experimentos por usuario no exceda un número N, que en este caso se ha asignado $N = 5$. Esto, proveerá una evolución paulatina del entrenamiento, lo que prolongará la efectividad, sin impactar en el rendimiento.

6.3.4 Arquitectura del aplicativo final

Una vez desarrollada una base de datos, así como un módulo que permite la recopilación de señales EEG en tiempo real, era preciso dar paso a la fabricación de un aplicativo con GUI capaz de brindar el servicio de autenticación a un cliente final. Para su desarrollo se siguió la popular infraestructura de software *Model-View-Controller* que divide a la solución en tres elementos arquitectónicos: una capa de datos i.e., el *Model*, una capa de presentación i.e., el *View* y finalmente una capa de lógica de negocio i.e., el *Controller*. El primero se conformó por una clase homónima, que define los métodos necesarios para las operaciones de ingreso y recuperación de información desde o hacia la base de datos e.g., la creación de un nuevo usuario o la extracción de los datos de entrenamiento de un sujeto.

El segundo elemento está conformado por un total de 6 clases, la primera de ellas abstracta, que emplean el módulo *Tkinter* de Python para la fabricación de la interfaz gráfica: *View, ViewPrincipal, ViewPanel, ViewCrearUsuario, ViewRecopilador* y *ViewIniciado*. En la primera se define el proceso de construcción de una ventana con un alto, largo, color de

fondo y título predefinido. Asimismo, se definen métodos abstractos e.g., *establecerListeners* que permitirán el relacionamiento de cada elemento gráfico en la GUI con un *controller*. Esta, es extendida por *ViewPanel,* una clase concreta que contruye debidamente una interfaz siguiendo los parámetros ya definidos en *View* y agregando elementos particulares como una cinta grisácea en la parte superior de la ventana donde se incluirán las opciones del aplicativo en cada ventana. Finalmente, de ésta, heredan las clases *ViewPrincipal, ViewCrearUsuario, ViewRecopilador* y *ViewIniciado,* las cuales, permiten, respectivamente, la selección de un usuario para autenticación, el registro de un nuevo sujeto en la base de datos, la presentación de estímulos al usuario durante la compilación de señales y la configuración de una cuenta tras un inicio de sesión exitoso. El diseño de estas interfaces, vislumbrado en un ordenador con sistema MacOS X Catalina se aprecia en las figuras 10 a 13 de la sección de anexos.

Finalmente, para concluir con la descripción de la arquitectura, es menester examinar la capa lógica i.e., el *controller.* Esta, de manera análoga, se compone de 6 clases: *Controller, ControllerCrearUsuario, ControllerIniciado, ControllerPrincipal, ControllerRecopilador* y *ControllerSelectorSeguridad*. La primera, define un constructor que recibe un *model* y un *view* para su relacionamiento. Asímismo, dicha clase define un método *inicializarView* que genera una vista determinada y la enlaza con una instancia de *controller*. Esto, permite la atención de los eventos disparados por el usuario en la interfaz gráfica. De dicha clase hereda *ControllerSelectorSeguridad,* la cual define los métodos necesarios para dar funcionalidad a los selectores de seguridad i.e., los botones empleados por un usuario para elegir el perfil de protección de su cuenta. Estos, como es posible observar en las figuras 11 y 12 de la sección de anexos, están presentes tanto en *ViewCrearUsuario* como en *Viewiniciado.*

Inherentemente, de la clase antedicha, surgen las extensiones *ControllerIniciado y ControllerCrearUsuario.* La primera, se encarga de recopilar información de la base de datos i.e., mediante el *model,* para popular la vista desplegada tras el inicio de sesión. Asímismo, los objetos de esta clase atienden las solicitudes de eliminación de cuentas y las canalizan a la función de la capa de datos correspondiente. *ControllerCrearUsuario,* por su parte, se encarga de validar que la información proporcionada por un individuo en *ViewCrearUsuario* sea correcta e.g., evitando nombres en blanco; contraseñas con longitud inferior a 8 caracteres o que carecen de mayúsculas, minúsculas, números o símbolos; la omisión de datos de entrenamiento, entre otros. De igual forma, las instancias de esta clase se encargan de solicitar al *model* la creación de una cuenta, de lanzar un selector para que el usuario especifique un fichero en formato *mat* con una señal para entrenar o bien de invocar a *ControllerRecopilador* para iniciar un escaneo de datos electroencefalográficos en tiempo real.

Este último i.e., *ControllerRecopilador,* se encarga de conducir la estimulación de un sujeto, recopilar sus datos EEG mediante el módulo Lector.py y procesarlos i.e., mediante el *model*, siguiendo la metodología descrita al final de la fase II. Dicho proceso, cabe resaltar, se desarrolla en forma concurrente i.e., en un hilo de ejecución independiente. Esto, se debe a que la interfaz gráfica basada en *Tkinter* bloquea el *thread* principal en espera de eventos que atender. Lo anterior, evita que la recopilación de datos se mantenga activa y la ejecución de cambios en la interfaz requeridos al transicionar de una actividad mental a otra se lleven a cabo. Para implementar dicha concurrencia se emplea la librería *threading* de Python.

Para concluir, se encuentra el *ControllerPrincipal,* una subclase de *Controller* que implementa la funcionalidad del *ViewPrincipal.* Para ello, dicho componente de software requiere de una invocación a diversos módulos previamente definidos e.g., para validar la

identdad de un usuario, esta porción de la capa lógica efectúa, en primera instancia, un llamado al *ControllerRecopilador.* Este, como se ha mencionado con anterioridad, se encarga de conducir una ronda de estimulación del sujeto mientras compila, en forma paralela, sus datos EEG. Al finalizar dicho módulo realiza un procesamiento de los datos y determina si, dadas las fronteras de un perfil, el sujeto entrante es aceptado o rechazado. Dicho estado se devuelve al *ControllerPrincipal* que transiciona al *ViewIniciado* si el resultado es aprobatorio o bien lanza un mensaje de fallo en caso contrario.

6.3.5 Pruebas en modo *pseudo-online* y *online*

Una vez desarrollado el aplicativo, era menester dar paso a una prueba de desempeño final. Esta, se dividiría en dos fases: una *pseudo-online* i.e., empleando archivos con formato de compatibilidad para MATLAB tanto para el entrenamiento como para la autenticación, y una *online* i.e., explotando el recopilador de datos EEG en tiempo real para ambas cuestiones. El primero, tuvo por objetivo validar que la metodología propuesta funcionase apropiadamente en la solución final, mientras que el segundo pretendía cuantificar una tasa de efectividad y consumo temporal del aplicativo, con lo cual, sería posible constatar el cumplimiento o no del objetivo principal de esta tesis que, cabe recordarlo, consiste en un TSR igual o mayor a 80.37%, con un periodo de entrenamiento y autenticación no mayor a 35 segundos.

Para tales pruebas se reclutaron 3 sujetos S_n adicionales. El primero, se involucraría en ambas fases de experimentación mientras que S_2 y S_3 participarían meramente en una. La primer prueba i.e., *pseudo-online* consistió en registrar a S_1 y S_2 como clientes del aplicativo con perfil de seguridad *intermedio*. Subsecuentemente S_1 intentaría ingresar en 8 ocasiones a su cuenta y en 5 a la de su contraparte i.e., S_2. De manera similar, S_2 intentaría acceder en

3 ocasiones a su perfil y en 3 al de su homólogo. Como resultado, el FAR obtenido fue de 0.0 i.e., ningún sujeto logró una personificación. Por su parte, el FRR se colocó en 0.09. Lo anterior, derivado de un único caso de FR. Esto, genera un TER de 0.05 y un TSR del 94.74%. Dicha cifra ciertamente corrobora el funcionamiento de la metodología en el aplicativo.

Mientras tanto, en la prueba *online* se realizó el alta de dos sujetos: S_1 y S_3, brindando a ambos perfiles el nivel de seguridad *intermedio*. Subsecuentemente, S_1 intentaría acceder 7 veces a su perfil y 3 al de su contraparte. De manera análoga S_3 intentó ingresar en 5 ocasiones a su cuenta y en 2 a la de su homólogo. Nuevamente la prueba concluyó con un FAR de 0.0. Dicha cifra, sugiere que cualquier recurso protegido por el sistema será inmune a intentos de personificación. El FRR, por su parte, escaló hasta 0.2. Esto, tras 2 intentos fallidos de ingreso de S_1 y 1 de S_3. Esto, escaló el TER hasta 0.15, lo que generó un TSR de 85.00%, una cifra que, si bien es menor, supera notablemente el umbral de 80.37%.

Ante tales resultados favorables restaba únicamente contabilizar el consumo temporal del aplicativo durante la autenticación. El protocolo de entrenamiento e ingreso, establece la necesidad de 5 experimentos de 4 seg. i.e., 20 seg. en total, no obstante, a dicha cifra, resta añadirle la demora derivada del procesamiento de datos. Para ello, se contabilizó la diferencia en milisegundos entre el instante en que al sistema recibe la matriz de información y procede a su filtrado hasta el momento en que se emite un veredicto de aceptación o rechazo. Lo anterior mediante el módulo *time* de Python. El lapso resultante fue de 3052ms. Esto, produce un tiempo total de autenticación de 23 segundos, muy por debajo del límite establecido. Con ello, el objetivo principal de esta tesis puede considerarse satisfecho.

7. Conclusiones y recomendaciones

A lo largo de este documento se expuso el desarrollo de un sistema de autenticación basado en señales electroencefalográficas. El proyecto, motivado por los riesgos de suplantación persistentes en algunas soluciones de identificación biométrica e.g., el reconocimiento de voz, iris o huellas dactilares, se desarrolló en tres fases. La primera fase, i.e., *basada en una clase genérica,* inició con un proceso de identificación de frecuencias de corte ideales para filtrado.

Para ello se empleó el *DataSet IIb de la BCI competition IV*, una compilación de la actividad EEG de 9 sujetos durante la realización de 2 tareas mentales i.e., imaginación de movimiento de la mano izquierda y derecha. De esta, se identificaron todas las posibles combinaciones binarias no-redundantes entre sujetos, se computó la efectividad de un clasificador ingenuo de Bayes al determinar la pertenencia de un vector característico a su respectivo autor empleando todas las posibles frecuencias de corte F_L y F_H, y finalmente, de los resultados obtenidos, se identificaron los puntos con mayor número de intersecciones.

Las frecuencias ideales previamente localizadas se usaron, en forma subsecuente, en la autenticación de sujetos. Durante esta etapa se filtró la señal en las bandas antedichas y se conformaron dos clases: una *cliente* y una *genérica*, albergando esta última los datos de entrenamiento de todos los sujetos con excepción de los del cliente. Nuevamente se empleó un clasificador de Bayes que debió identificar si un vector pertenecía a un cliente o, si por el contrario, se relacionaba con el resto de sujetos. Con base en la tasa promedio de aciertos y fallos derivada de este proceso se computó un TSR que alcanzó un valor de ~95%.

La segunda fase i.e., *autenticación basada en fronteras*, destacó algunos problemas de la aproximación previa e.g., la casi nula escalabilidad y el alto costo computacional que implica la conformación de la clase genérica. Ante ello, se planteó un nuevo paradigma de autenticación, en el cuál, se determina mediante los datos de entrenamiento, un vector medio $\vec{\mu}$ y de desviaciones estándar $\vec{\sigma}$ por cada cliente. Subsecuentemente, dado un nuevo vector característico $\vec{x}$ se computa la correlación producto-momento de Pearson entre $\vec{x}$ y $\vec{\mu}$, así como el *likelihood* de $\vec{x}$ dado $\vec{\mu}$ y $\vec{\sigma}$. En caso que ambos valores superen una frontera se produce una aceptación, generando un rechazo en caso contrario. Dicha aproximación produjo de manera inicial un desempeño ciertamente loable i.e., TSR de 84.71% empleando ω_1 y de 84.72% al utilizar ω_2. No obstante, dichos valores ignoraban problemáticas asociadas al uso de señales EEG e.g., su variación paulatina con respecto al tiempo.

Tras introducir dicha variable, así como diversas medidas para mitigar su impacto en la efectividad, las cuales fueron: , una combinación de las clases de movimiento ω_1 y ω_2, un incremento en el número de bandas de frecuencia y una ampliación del vector característico con funciones adicionales, específicamente: el rango intercuartílico, la desviación de la mediana absoluta y la dimensión fractal de *katz,* se logró un TSR de entre 91.59% y 92.02%. Dicho valor fue ciertamente destacable, sin embargo, alcanzarlo requería de un entrenamiento excesivo y un elevado consumo tanto temporal como computacional, lo que imposibilitaba su uso en aplicaciones realistas. Ante ello, se suprimió a la dimensión fractal de *katz* como característica y se redujo gradualmente el conjunto de datos de entrenamiento hasta solo dos experimentos. Pese a lo anterior el resultado fue positivamente sostenido, obteniendo un TSR de 91.64%.

Posteriormente se analizó si dicho modelo podía ser generalizado a otras colecciones de datos, para lo cual se constituyó un nuevo *dataset* de 4 sujetos que realizaron las mismas tareas mentales ω_1 y ω_2 descritas con anterioridad i.e., movimiento de la mano izquierda y derecha. Sobre éste se aplicó el paradigma fabricado, obteniendo en una efectividad de entre 93.14% y 95.33%, con un FAR máximo de 0.02. Dichos valores no sólo permitieron constatar la utilidad del modelo sino también asegurar que la solución fabricada sería competente tanto eficaz como eficientemente con otras alternativas de autenticación biométrica en existencia.

Para finalizar, en la tercera fase, i.e., *elaboración de un software de aplicación,* se fabricó un módulo de recopilación de datos EEG en tiempo real empleando la librería *BrainFlow* de *Python3* y se corroboró su funcionamiento conectando la tarjeta de adquisición a un generador de señales, graficando la lectura obtenida y comparándola con la expectativa. Subsecuentemente, se diseñó una base de datos relacional capaz de albergar la información compilada y se procedió a su implementación en el gestor MySQL 8. Finalmente, se elaboró una aplicación basada en el patrón de diseño Model-View-Controller que explotaba los recursos anteriores para brindar el servicio de autenticación. Esto, siguiendo el paradigma validado en la fase 2. El aplicativo ofreció dos métodos de acceso*: pseudo-online* y *online,* el primero de ellos empleando un archivo de MATLAB como llave y el segundo con una recopilación en tiempo real. En el primer caso se obtuvo un TSR del 94.74%, mientras que en el segundo se logró una efectividad del 85.00%, con FAR de 0%. Estos resultados destacan por varias razones:

1. El TSR obtenido i.e., 85.00% supera a otras soluciones de autenticación biométrica cuya efectividad ronda entre 80.37% y 99.99% (Shelupanov, Evsyutin, Konev, et al.,

2019), (Sluganovic, Roeschlin, Rasmussen, et al., 2016). Esto, pese a las múltiples añadiduras y mejoras que dichos paradigmas maduros han recibido.

2. El FAR de la aplicación final es de 0.0%. Esto, implica que, si bien el sistema puede juzgar erróneamente a un sujeto, esto nunca comprometerá la seguridad del recurso protegido. En el peor caso sólo reducirá su disponibilidad.
3. El aplicativo final requiere solo 5 experimentos de 4 seg. para el entrenamiento y acceso. Lo anterior, aunado al inherente retraso del procesamiento i.e., ∼3052ms, implica un tiempo total de autenticación de aproximadamente 23 segundos. Esto, supera con creces a otras soluciones biométricas que pueden demorar entre 35 segundos y 2 minutos para recopilar datos y emitir un veredicto (Arteaga-Falconi, Al Osman, y El Saddik, 2015), (Sluganovic, Roeschlin, Rasmussen, et al., 2016).
4. En las pruebas finales se han realizado ingresos aún después de 3 días sin generar un decremento en el TSR. Esta cualidad no sólo prueba que la metodología propuesta es robusta sino que también, junto al punto anterior y el hecho de que en cada instancia se han usado solo 3 canales, constatan la aplicabilidad en un entorno realista.
5. Como se comentó con anterioridad, los *datasets* utilizados en la evaluación presentan múltiples diferencias , principalmente las características técnicas del equipo de registro y el entorno en que se llevó acabo la adquisición de los datos. Esto, demuestra que el paradigma desarrollado soporta variaciones en el entorno aplicativo.
6. La metodología requiere de un preprocesamiento simple, así como una extracción de características relativamente triviales, por lo que su implementación es por demás

rápida y sencilla. Esto, permite vislumbrarlo como un posible estándar o *framework* para autenticación basada en electroencefalografía.

8. Bibliografía

1. Abdulkader, S. N., Atia, A., & Mostafa, M. S. M. (2015). *Brain computer interfacing: Applications and challenges*. Egyptian Informatics Journal, 16(2), 213-230.
2. Abuhashish, F. A., Sunar, M. S., Kolivand, H., Mohamed, F., & Mohamad, D. B. (2014). *Feature extracted classifiers based on eeg signals: a survey*. Life Science Journal, 11(4).
3. Adekeye, K. S. (2012). *Modified simple robust control chart based on median absolute deviation.* International Journal of Statistics and Probability, 1(2), 91.
4. Alenius, F. (2010). Authentication and Authorization: Achieving Single Sign-on in an Erlang Environment.
5. Ali, A. S., Radwan, A. G., & Soliman, A. M. (2013). *Fractional order Butterworth filter: active and passive realizations*. IEEE journal on emerging and selected topics in circuits and systems, 3(3), 346-354
6. Alonso, J. C., & Montenegro, S. (2015). *Estudio de Monte Carlo para comparar 8 pruebas de normalidad sobre residuos de mínimos cuadrados ordinarios en presencia de procesos autorregresivos de primer orden*. Estudios Gerenciales, 31(136), 253-265.
7. Anguera, J. A., Boccanfuso, J., Rintoul, J. L., Al-Hashimi, O., Faraji, F., Janowich, J., ... & Gazzaley, A. (2013). *Video game training enhances cognitive control in older adults*. Nature, 501(7465), 97-101.

8. Anscombe, F. J. (1960). *Rejection of outliers*. Technometrics, 2(2), 123-146.

9. Arnold, M. J., Iskander, D. R., & Zoubir, A. M. (1995, May). *Testing Gaussianity with the characteristic function*. In 1995 International Conference on Acoustics, Speech, and Signal Processing (Vol. 3, pp. 2012-2015) IEEE.

10. Arteaga-Falconi, J. S., Al Osman, H., & El Saddik, A. (2015). *ECG authentication for mobile devices*. IEEE Transactions on Instrumentation and Measurement, 65(3), 591-600.

11. Ashby, C., Bhatia, A., Tenore, F., & Vogelstein, J. (2011, April). *Low-cost electroencephalogram (EEG) based authentication*. In 2011 5th International IEEE/EMBS Conference on Neural Engineering (pp. 442-445). IEEE.

12. Ashby, C., Bhatia, A., Tenore, F., & Vogelstein, J. (2011, April). Low-cost electroencephalogram (EEG) based authentication. In 2011 5th International IEEE/EMBS Conference on Neural Engineering (pp. 442-445). IEEE.

13. Ayaz, H., Shewokis, P. A., Bunce, S., & Onaral, B. (2011, August). *An optical brain computer interface for environmental control*. In 2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society (pp. 6327-6330). IEEE.

14. Barton, B., Byciuk, S., Harris, C., Schumack, D., & Webster, K. (2005). *The emerging cyber risks of biometrics*. Risk Management, 52(10), 26-31.

15. Ben-Yacoub, S. (1998). *Multi-modal data fusion for person authentication using SVM* (No. REP_WORK). IDIAP.

16. Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). *Biometric authentication: A review*. International Journal of u-and e-Service, Science and Technology, 2(3), 13-28.

17. Bilimoria, K. Y., Cohen, M. E., Merkow, R. P., Wang, X., Bentrem, D. J., Ingraham, A. M., ... & Ko, C. Y. (2010). *Comparison of outlier identification methods in hospital surgical quality improvement programs*. Journal of Gastrointestinal Surgery, 14(10), 1600-1607.

18. Bishop, M., & Klein, D. V. (1995). *Improving system security via proactive password checking*. Computers & Security, 14(3), 233-249.

19. Blanchard, G., Lugosi, G., & Vayatis, N. (2003). *On the rate of convergence of regularized boosting classifiers*. Journal of Machine Learning Research, 4(Oct), 861-894.

20. Blankertz, B., Tangermann, M., Vidaurre, C., Fazli, S., Sannelli, C., Haufe, S., ... & Mueller, K. R. (2010). *The Berlin brain–computer interface: non-medical uses of BCI technology*. Frontiers in neuroscience, 4, 198.

21. Bubrick, E. J., Yazdani, S., & Pavlova, M. K. (2014). *Beyond standard polysomnography: advantages and indications for use of extended 10–20 EEG montage during laboratory sleep study evaluations*. Seizure, 23(9), 699-702.

22. Bump, W. M. (1991). The Normal Curve Takes Many Forms: A Review of Skewness and Kurtosis.

23. Camlikaya, E., Kholmatov, A., & Yanikoglu, B. (2008, March). *Multi-biometric templates using fingerprint and voice*. In Biometric technology for human

identification V (Vol. 6944, p. 69440I). International Society for Optics and Photonics.

24. Chou, H. C., Lee, H. C., Yu, H. J., Lai, F. P., Huang, K. H., & Hsueh, C. W. (2013). *Password cracking based on learned patterns from disclosed passwords*. IJICIC, 9(2), 821-839.
25. Cousineau, D., & Chartier, S. (2010). *Outliers detection and treatment: a review*. International Journal of Psychological Research, 3(1), 58-67.
26. Crilly, A. J., Eamshaw, R. A., & Jones, H. (1991). *Introduction Fractals and Chaos*. In Fractals and chaos (pp. 1-4). Springer, New York, NY.
27. Curran, E. A., & Stokes, M. J. (2003). *Learning to control brain activity: A review of the production and control of EEG components for driving brain–computer interface (BCI) systems*. Brain and cognition, 51(3), 326-336.
28. D'agostino, R. B., Belanger, A., & D'Agostino Jr, R. B. (1990). *A suggestion for using powerful and informative tests of normality*. The American Statistician, 44(4), 316-321.
29. DeCarlo, L. T. (1997). *On the meaning and use of kurtosis*. Psychological methods, 2(3), 292.
30. Decety, J. (1996). *The neurophysiological basis of motor imagery*. Behavioural brain research, 77(1-2), 45-52.
31. Eagleman, S. L., Drover, C. M., Drover, D. R., Ouellette, N. T., & MacIver, M. B. (2018). *Remifentanil and nitrous oxide anesthesia produce a unique pattern of EEG activity during loss and recovery of response*. Frontiers in human neuroscience, 12, 173.

32. Esteller, R., Vachtsevanos, G., Echauz, J., & Lilt, B. (1999, May). *A comparison of fractal dimension algorithms using synthetic and experimental data*. In 1999 IEEE International Symposium on Circuits and Systems (ISCAS) (Vol. 3, pp. 199-202). IEEE.

33. Farias-Castro, D., & Salazar-Varas, R. (2020, Octubre). *Person Authentication Based on Standard Deviation of EEG Signals and Bayesian Classifier*. En Mexican International Conference on Artificial Intelligence (pp. 390-400). Springer, Cham.

34. Ferdous, M. J., Ali, M. S., Hamid, M. E., & Molla, M. K. I. (2016). *A comparison of butterworth bandpass filter and discrete wavelet transform filter for the suppression of ocular artifact from EEG signal*. International Journal of Research in Engineering Technology, 1(4).

35. Galbally, J., Fierrez, J., & Ortega-García, J. (2007). *Vulnerabilities in biometric systems: Attacks and recent advances in liveness detection*. Database, 1(3), 1-8.

36. Ganin, I. P., Shishkin, S. L., Kochetova, A. G., & Kaplan, A. Y. (2012). P *300-based brain-computer interface: The effect of the stimulus position in a stimulus train*. Human Physiology, 38(2), 121-128.

37. Gargiulo, G., Calvo, R. A., Bifulco, P., Cesarelli, M., Jin, C., Mohamed, A., & van Schaik, A. (2010). *A new EEG recording system for passive dry electrodes*. Clinical Neurophysiology, 121(5), 686-693.

38. Godin, B. (2006). *The knowledge-based economy: conceptual framework or buzzword?.* The Journal of technology transfer, 31(1), 17-30.

39. Gutiérrez, E., Galera, V., Martínez, J. M., & Alonso, C. (2007). *Biological variability of the minutiae in the fingerprints of a sample of the Spanish population*. Forensic Science International, 172(2-3), 98-105.

40. Hagemann, D., Naumann, E., Lürken, A., Becker, G., Maier, S., & Bartussek, D. (1999). *EEG asymmetry, dispositional mood and personality*. Personality and Individual Differences, 27(3), 541-568.

41. Heeger, D. J., & Ress, D. (2002). *What does fMRI tell us about neuronal activity?*. Nature Reviews Neuroscience, 3(2), 142-151.

42. Hernández Loeza, F. J. (1995). *Pruebas de normalidad para los residuos de un ajuste de regresión*.

43. Holder, E. H., Robinson, L. O., & Laub, J. H. (2011). *The fingerprint sourcebook*. US Department. of Justice, Office of Justice Programs, National Institute of Justice.

44. Homan, R. W., Herman, J., & Purdy, P. (1987). Cereb*ral location of international 10–20 system electrode placement*. Electroencephalography and clinical neurophysiology, 66(4), 376-382.

45. Huber, P. J. (1981). *Robust Statistics*. New York: John Wiley and Sons. HuberRobust statistics1981.

46. Hwang, M. S., Lee, C. C., & Tang, Y. L. (2002). *A simple remote user authentication scheme*. Mathematical and Computer Modell ing, 36(1-2), 103-107.

47. Ives, B., Walsh, K. R., & Schneider, H. (2004). T*he domino effect of password reuse*. Communications of the ACM, 47(4), 75-78.

48. Jahromi, A. H., & Taheri, M. (2017, October). *A non-parametric mixture of Gaussian naive Bayes classifiers based on local independent features*. In 2017 Artificial Intelligence and Signal Processing Conference (AISP) (pp. 209-212). IEEE.

49. Jain, A. K., Griess, F. D., & Connell, S. D. (2002). *On-line signature verification*. Pattern recognition, 35(12), 2963-2972.

50. Jiang, R., Al-Maadeed, S., Bouridane, A., Crookes, D., Beghdadi, A.: *Biometric Security and Privacy*, 1st edn. Springer, Cham (2017). https://doi.org/10.1007/ 978-3-319-47301-7 9

51. Jones A., Clarke B., & Picto P. (2020). *Electronic applications*. OpenLearn, 30

52. Kao, F. C., Wang, S. R., & Chang, Y. J. (2015). *Brainwaves analysis of positive and negative emotions*. WSEAS Trans. Inf. Sci. Appl, 12, 200-208.

53. Keene, D. L., Whiting, S., & Ventureyra, E. C. G. (2000). *Electrocorticography*. Epileptic Disorders, 2(1), 57-64.

54. Kelly, A. (2010). *Cracking passwords using keyboard acoustics and language modeling.* University of Edinburgh, http://citeseerx.ist.psu.edu/viewdoc/download, 54.

55. Khalifa, W., Salem, A., Roushdy, M., & Revett, K. (2012, May). A survey of EEG based user authentication schemes. In 2012 8th International Conference on Informatics and Systems (INFOS) (pp. BIO-55). IEEE.

56. Kim, H., & Lee, E. A. (2017). Authen*tication and Authorization for the Internet of Things*. IT Professional, 19(5), 27-33.

57. Kinnunen, T., Wu, Z. Z., Lee, K. A., Sedlak, F., Chng, E. S., & Li, H. (2012, March). *Vulnerability of speaker verification systems against voice conversion spoofing attacks: The case of telephone speech*. In 2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 4401-4404). IEEE.

58. Kostyunina, M. B., & Kulikov, M. A. (1996). *Frequency characteristics of EEG spectra in the emotions*. Neuroscience and Behavioral Physiology, 26(4), 340-343.

59. L. Sheugh and S. H. Alizadeh, "*A note on pearson correlation coefficient as a metric of similarity in recommender system,*" 2015 AI & Robotics (IRANOPEN), 2015, pp. 1-6, doi: 10.1109/RIOS.2015.7270736.

60. Lakshmi, M. R., Prasad, T. V., & Prakash, D. V. C. (2014). *Survey on EEG signal processing methods*. International Journal of Advanced Research in Computer Science and Software Engineering, 4(1).

61. Lance, B. J., Kerick, S. E., Ries, A. J., Oie, K. S., & McDowell, K. (2012). *Brain–computer interface technologies in the coming decades*. Proceedings of the IEEE, 100(Special Centennial Issue), 1585-1599.

62. Larrañaga, P., Inza, I., & Moujahid, A. (1997). *Tema 6. Clasificadores Bayesianos*. Departamento de Ciencias de la Computación e Inteligencia Artificial–Universidad del País Vasco-Euskal Herriko Unibertsitatea.

63. Lau, Y. W., Wagner, M., & Tran, D. (2004, October). Vuln*erability of speaker verification to voice mimicking*. In Proceedings of 2004 International Symposium on Intelligent Multimedia, Video and Speech Processing, 2004. (pp. 145-148). IEEE.

64. Lécuyer, A., Lotte, F., Reilly, R. B., Leeb, R., Hirose, M., & Slater, M. (2008). *Brain-computer interfaces, virtual reality, and videogames*. Computer, 41(10), 66-72.

65. Leeb, R., Brunner, C., Müller-Putz, G., Schlögl, A., & Pfurtscheller, G. (2008). *BCI Competition 2008–Graz data set B*. Graz University of Technology, Austria, 1-6.

66. Leys, C., Ley, C., Klein, O., Bernard, P., & Licata, L. (2013). Detec*ting outliers: Do not use standard deviation around the mean, use absolute deviation around the median*. Journal of experimental social psychology, 49(4), 764-766.

67. Li, Q., Ding, D., & Conti, M. (2015, September). *Brain-computer interface applications: Security and privacy challenges*. In 2015 IEEE conference on communications and network security (CNS) (pp. 663-666). IEEE.

68. Li, X., & Bilmes, J. (2006, May). *Regularized adaptation of discriminative classifiers*. In 2006 IEEE International Conference on Acoustics Speech and Signal Processing Proceedings (Vol. 1, pp. I-I). IEEE.

69. Li, Z., He, W., Akhawe, D., & Song, D. (2014). *The emperor's new password manager: Security analysis of web-based password managers*. In 23rd {USENIX} Security Symposium ({USENIX} Security 14) (pp. 465-479).

70. Lin, C. T., Lin, B. S., Lin, F. C., & Chang, C. J. (2012). *Brain computer interface-based smart living environmental auto-adjustment control system in UPnP home networking*. IEEE Systems Journal, 8(2), 363-370.

71. Lizama, P. L., & Gómez, R. (2003). *Autenticación Biométrica On Card en el Protocolo de Kerberos*. In Memoria del Segundo Congresos Iberoamericano de Seguridad Informática. México (pp. 249-266).

72. Lotte, F., & Roy, R. N. (2019). *Brain–computer interface contributions to neuroergonomics*. In Neuroergonomics (pp. 43-48). Academic Press.

73. Lotte, F., Congedo, M., Lécuyer, A., Lamarche, F., & Arnaldi, B. (2007). *A review of classification algorithms for EEG-based brain–computer interfaces*. Journal of neural engineering, 4(2), R1.

74. Maiorana, E., & Campisi, P. (2017). *Longitudinal evaluation of EEG-based biometric recognition*. IEEE Transactions on Information Forensics and Security, 13(5), 1123-1138.

75. Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). *Handbook of fingerprint recognition*. Springer Science & Business Media.

76. Marcel, S., Mill ÃÅan, J.D.R.: *Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation*. IEEE Trans. Pattern Anal. Mach. Intell. 29(4), 743-752 (2007)

77. Matsumoto, T. (2002, December). *Gummy and conductive silicone rubber fingers importance of vulnerability analysis*. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 574-575). Springer, Berlín, Heidelberg.

78. Mazumder, I. (2019, March). *An analytical approach of EEG analysis for emotion recognition.* In 2019 Devices for Integrated Circuit (DevIC) (pp. 256-260). IEEE.

79. Mazumder, S., & Serfling, R. (2009). *Bahadur representations for the median absolute deviation and its modifications*. Statistics & probability letters, 79(16), 1774-1783.

80. McFarland, D. J., & Wolpaw, J. R. (2008). *Brain-computer interface operation of robotic and prosthetic devices*. Computer, 41(10), 52-56.

81. Mehta, R. K., & Parasuraman, R. (2013). *Neuroergonomics: a review of applications to physical and cognitive work*. Frontiers in human neuroscience, 7, 889.

82. Miller, J. (1991). *Reaction time analysis with outlier exclusion*: Bias varies with sample size. The quarterly journal of experimental psychology, 43(4), 907-912.

83. Miller, M. B., Donovan, C. L., Van Horn, J. D., German, E., Sokol-Hessner, P., & Wolford, G. L. (2009). *Unique and persistent individual patterns of brain activity across different memory retrieval tasks*. Neuroimage, 48(3), 625-635.

84. Miller, S. P., Neuman, B. C., Schiller, J. I., & Saltzer, J. H. (1988). *Kerberos authentication and authorization system*. In Project Athena Technical Plan.

85. Miner, L. A., McFarland, D. J., & Wolpaw, J. R. (1998). *Answering questions with an electroencephalogram-based brain-computer interface*. Archives of physical medicine and rehabilitation, 79(9), 1029-1033.

86. Minguez, J. (2008). *Tecnologıa de interfaz cerebro-computador*.

87. Motamedi-Fakhr, S., Moshrefi-Torbati, M., Hill, M., Hill, C. M., & White, P. R. (2014). *Signal processing techniques applied to human sleep EEG signals—A review*. Biomedical Signal Processing and Control, 10, 21-33.

88. Mullinger, K., & Bowtell, R. (2011). *Combining EEG and fMRI*. In Magnetic Resonance Neuroimaging (pp. 303-326). Humana Press.

89. Murugappan, M., & Murugappan, S. (2013, March). Hu*man emotion recognition through short time Electroencephalogram (EEG) signals using Fast Fourier*

Transform (FFT). In 2013 IEEE 9th International Colloquium on Signal Processing and its Applications (pp. 289-294). IEEE.

90. Myrden, A., & Chau, T. (2015). *Effects of user mental state on EEG-BCI performance*. Frontiers in human neuroscience, 9, 308.
91. Naseer, N., & Hong, K. S. (2015). *fNIRS-based brain-computer interfaces: a review*. Frontiers in human neuroscience, 9, 3.
92. Ng, A. Y., & Jordan, M. I. (2002). *On discriminative vs. generative classifiers: A comparison of logistic regression and naive bayes*. In Advances in neural information processing systems (pp. 841-848).
93. Nicolas-Alonso, L. F., & Gomez-Gil, J. (2012). *Brain computer interfaces, a review*. sensors, 12(2), 1211-1279.
94. Oweis, R. J., Hamdi, N., Ghazali, A., & Lwissy, K. (2013). *A comparison study on machine learning algorithms utilized in P300-based BCI*. J Health Med Informat, 4(126), 2.
95. Pankanti, S., Prabhakar, S., & Jain, A. K. (2002). *On the individuality of fingerprints*. IEEE Transactions on pattern analysis and machine intelligence, 24(8), 1010-1025.
96. Parasuraman, R., & Wilson, G. F. (2008). *Putting the brain to work: Neuroergonomics past, present, and future*. Human factors, 50(3), 468-474.
97. Park, B. (2008). *Quality inspection of poultry carcasses*. In Computer Vision Technology for Food Quality Evaluation (pp. 157-187). Academic Press.

98. Paszkiel, S. (2016). *Control based on brain-computer interface technology for video-gaming with virtual reality techniques*. Journal of Automation, Mobile Robotics and Intelligent Systems, 3-7.

99. Paul, L. Y., Baras, J. S., & Sadler, B. M. (2008). *Physical-layer authentication*. IEEE Transactions on Information Forensics and Security, 3(1), 38-51.

100. Pinti, P., Tachtsidis, I., Hamilton, A., Hirsch, J., Aichelburg, C., Gilbert, S., & Burgess, P. W. (2020). *The present and future use of functional near-infrared spectroscopy (fNIRS) for cognitive neuroscience*. Annals of the New York Academy of Sciences, 1464(1), 5.

101. Razali, N. M., & Wah, Y. B. (2011). *Power comparisons of shapiro-wilk, kolmogorov-smirnov, lilliefors and anderson-darling tests*. Journal of statistical modeling and analytics, 2(1), 21-33.

102. Rish, I. (2001, August). *An empirical study of the naive Bayes classifier*. In IJCAI 2001 workshop on empirical methods in artificial intelligence (Vol. 3, No. 22, pp. 41-46).

103. Ruiz-Albacete, V., Tome-González, P., Alonso-Fernández, F., Galbally, J., Fierrez, J., & Ortega-García, J. (2008, May). *Direct attacks using fake images in iris verification*. In European Workshop on Biometrics and Identity Management (pp. 181-190). Springer, Berlín, Heidelberg.

104. Schalk, G. (2010). *Can electrocorticography (ECoG) support robust and powerful brain-computer interfaces?*. Frontiers in neuroengineering, 3, 9.

105. Sedgwick, P. (2012). *Pearson's correlation coefficient*. Bmj, 345.

106. Shay, R., & Bertino, E. (2009). *A comprehensive simulation tool for the analysis of password policies*. International Journal of Information Security, 8(4), 275-289.

107. Shelupanov, A., Evsyutin, O., Konev, A., Kostyuchenko, E., Kruchinin, D., & Nikiforov, D. (2019). *Information Security Methods—Modern Research Directions*. Symmetry, 11(2), 150.

108. Sluganovic, I., Roeschlin, M., Rasmussen, K. B., & Martinovic, I. (2016, October). *Using reflexive eye movements for fast challenge-response authentication*. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 1056-1067).

109. Soni, M., Gupta, S., Rao, M. S., & Gupta, P. (2010). *A new vein pattern-based verification system*. International Journal of computer science and information security, 8(1), 58-63.

110. Sorger, B., & Goebel, R. (2020). *Real-time fMRI for brain-computer interfacing*. In Handbook of clinical neurology (Vol. 168, pp. 289-302). Elsevier.

111. Steiner, J. G., Neuman, B. C., & Schiller, J. I. (1988, February). *Kerberos: An Authentication Service for Open Network Systems*. In Usenix Winter (pp. 191-202).

112. Takeda, K., Mishiba, M., Sugiura, H., Nakajima, A., Kohama, M., & Hiramatsu, S. (2009). *Evaluated reference intervals for serum free thyroxine and thyrotropin using the conventional outliner rejection test without regard to presence of thyroid antibodies and prevalence of thyroid dysfunction in Japanese subjects*. Endocrine journal, 56(9), 1059-1066.

113. Tavor, I., Jones, O. P., Mars, R. B., Smith, S. M., Behrens, T. E., & Jbabdi, S. (2016). *Task-free MRI predicts individual differences in brain activity during task performance*. Science, 352(6282), 216-220.

114. Teoh, A., Samad, S. A., & Hussain, A. (2004). *Nearest neighbourhood classifiers in biometric fusion*. International Journal of The Computer, the internet and management, 12(1), 23

115. Thalheim, L., Krissier J. & Zlegter P.M. (2004). *Body Check-Biometric Access Protection Devices and their Programs Put to the Test*. c't Magazine.

116. Thielen, J., van den Broek, P., Farquhar, J., & Desain, P. (2015). Broad-Band visually evoked potentials: re (con) volution in brain-computer interfacing. PloS one, 10(7), e0133797.

117. Tocan, M. C. (2012). *Knowledge based economy assessment*. Journal of Knowledge Management, Economics and Information Technology, 2(5), 1-13.

118. Torres, E. P., Torres, E. A., Hernández-Álvarez, M., & Yoo, S. G. (2020). *EEG-based BCI emotion recognition: a survey*. Sensors, 20(18), 5083.

119. Uludag, U., Ross, A., & Jain, A. (2004). *Biometric template selection and update: a case study in fingerprints*. Pattern recognition, 37(7), 1533-1542.

120. Urigüen, J. A., & Garcia-Zapirain, B. (2015). *EEG artifact removal—state-of-the-art and guidelines*. Journal of neural engineering, 12(3), 031001.

121. Van der Putte, T., & Keuning, J. (2000). *Biometrical fingerprint recognition: don't get your fingers burned*. In Smart Card Research and Advanced Applications (pp. 289-303). Springer, Boston, MA.

122. Van Erp, J., Lotte, F., & Tangermann, M. (2012). *Brain-computer interfaces: beyond medical applications*. Computer, 45(4), 26-34.

123. Van Gerven, M., Farquhar, J., Schaefer, R., Vlek, R., Geuze, J., Nijholt, A., ... & Desain, P. (2009). *The brain–computer interface cycle*. Journal of neural engineering, 6(4), 041001.

124. Velásquez, I., Caro, A., & Rodríguez, A. (2017). *Identifying Comparison and Selection Criteria for Authentication Schemes and Methods*. In Simposio Argentino de Ingeniería de Software (ASSE)-JAIIO 46 (Córdoba, 2017)..

125. Vidal, F., Burle, B., Spieser, L., Carbonnell, L., Meckler, C., Casini, L., & Hasbroucq, T. (2015). *Linking EEG signals, brain functions and mental operations: Advantages of the Laplacian transformation*. International Journal of Psychophysiology, 97(3), 221-232.

126. Wang, Y., & Jung, T. P. (2011). *A collaborative brain-computer interface for improving human performance*. PloS one, 6(5), e20422.

127. Waziri, A., Claassen, J., Stuart, R. M., Arif, H., Schmidt, J. M., Mayer, S. A., ... & Hirsch, L. J. (2009). *Intracortical electroencephalography in acute brain injury*. Annals of Neurology: Official Journal of the American Neurological Association and the Child Neurology Society, 66(3), 366-377.

128. Weaver, A. C. (2006). *Biometric authentication*. Computer, 39(2), 96-97.

129. Whaley III, D. L. (2005). *The interquartile range: Theory and estimation* (Doctoral dissertation, East Tennessee State University).

130. Wheless, J. W., Castillo, E., Maggio, V., Kim, H. L., Breier, J. I., Simos, P. G., & Papanicolaou, A. C. (2004). M*agnetoencephalography (MEG) and magnetic source imaging (MSI)*. The neurologist, 10(3), 138-153.

131. Wyczesany, M., Kaiser, J., & Coenen, A. M. (2008). *Subjective mood estimation co-varies with spectral power EEG characteristics*.

132. Wyłomańska, A., Iskander, D. R., & Burnecki, K. (2020). *Omnibus test for normality based on the Edgeworth expansion*. Plos one, 15(6), e0233901.

133. Xia, X., & O'Gorman, L. (2003). *Innovations in fingerprint capture devices*. Pattern Recognition, 36(2), 361-369.

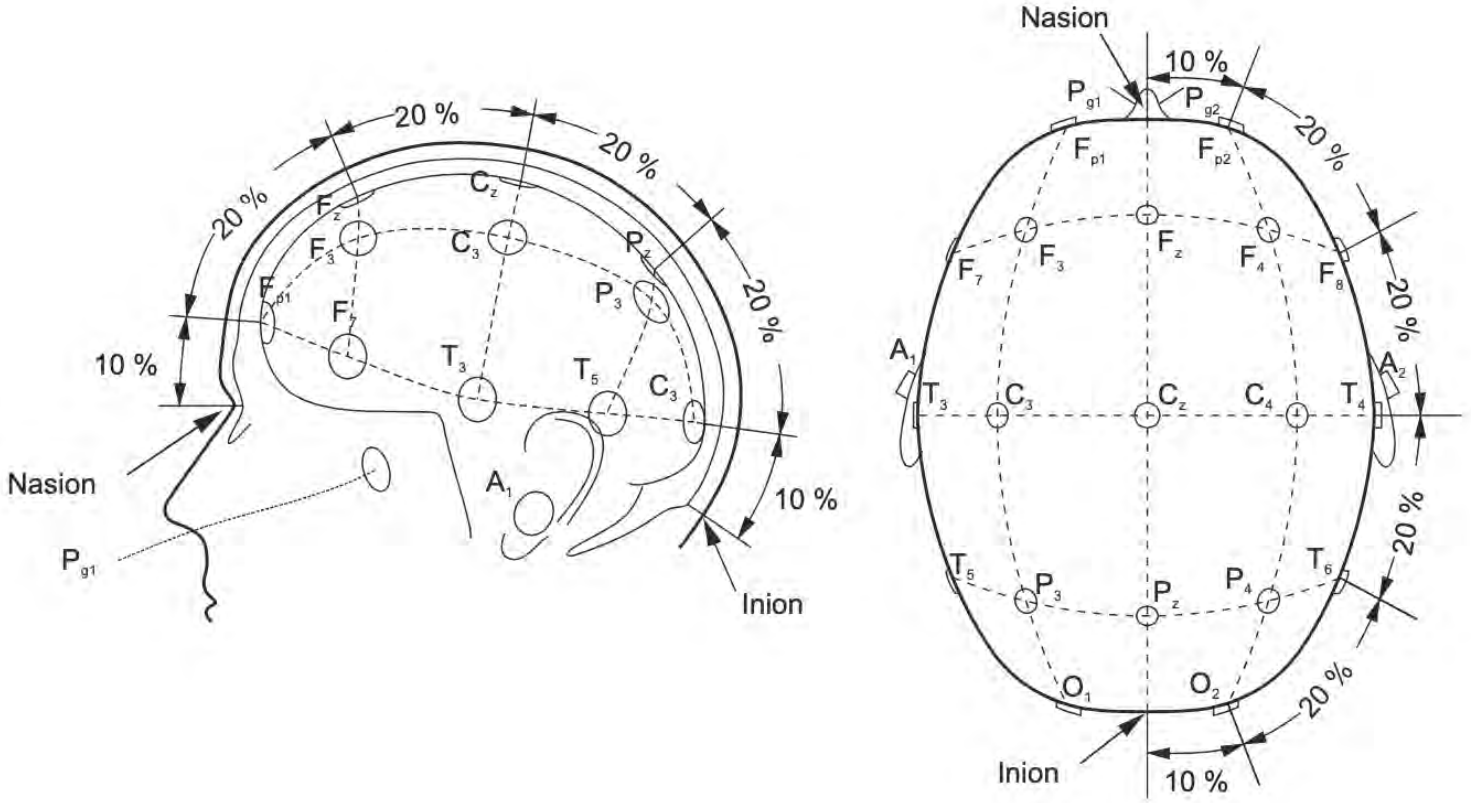
134. Yadav, S. K., & Saha, R. (2020). *Investigating non-Gaussianity in Cosmic Microwave Background Temperature Maps using Spherical Harmonic Phases*. arXiv preprint arXiv:2001.10960.

135. Yaghouby, F. (2015). *Experimental-computational analysis of vigilance dynamics for applications in sleep and epilepsy*. University of Kentucky.

136. Yong-suo, L. I. U., Qing-hua, M. E. N. G., Rong, C., Jian-song, W. A. N. G., Shu-min, J. I. A. N. G., & Yu-zhu, H. U. (2004). *Improvement of similarity measure: pearson product-moment correlation coefficient*. Journal of Chinese Pharmaceutical Sciences, 13(3), 180.

137. Zheng, W. L., Zhu, J. Y., & Lu, B. L. (2017). *Identifying stable patterns over time for emotion recognition from EEG*. IEEE Transactions on Affective Computing, 10(3), 417-429.

9. Anexos



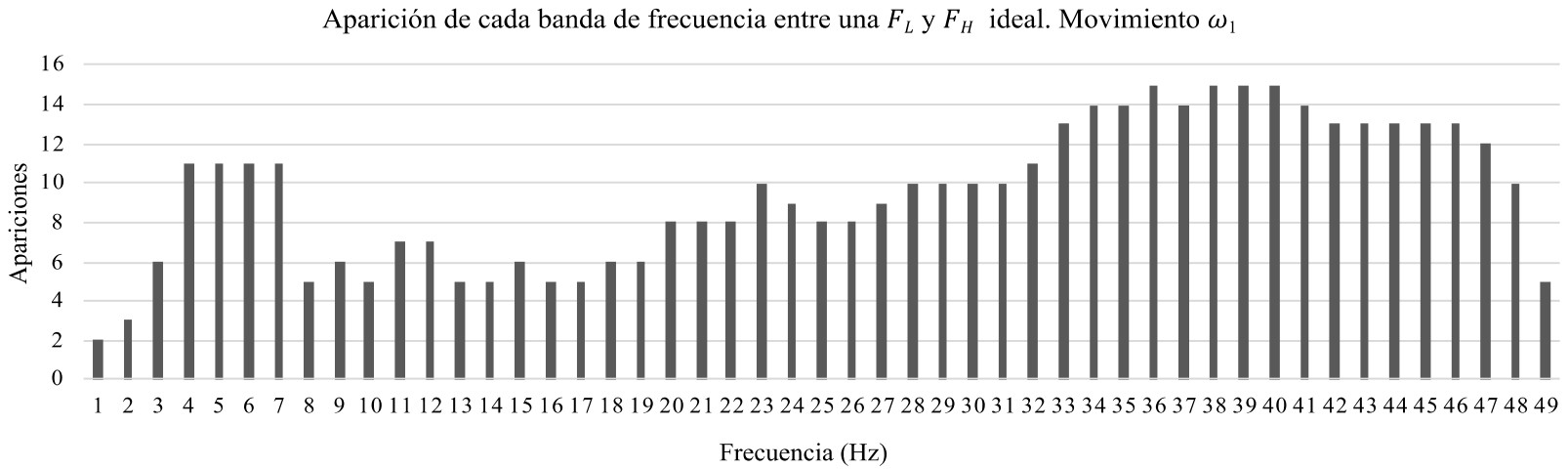
Anexo 1 (Figura 2). Posicionamiento de los electrodos bajo el sistema 10-20. Como es posible observar en el diagrama la leyenda "10-20" hace referencia a la distancia entre nodos adyacentes, i.e., 10 o 20% de la distancia craneal entre los puntos denominados *nasion* e *inion*. Como es posible vislumbrar en el elemento gráfico presentado, las letras asignadas a cada electrodo, permiten identificar el área de colocación en el cráneo e.g., FP hace referencia al área prefrontal, F corresponde al área frontal, T hace alusión al temporal, P al parietal y O al Occipital. C, por su parte, evoca al área central, mientras que A se reserva para los electrodos de referencia aludidos en la sección 4.3.2 de este documento. El diagrama presentado es provisto por (Nicolas-Alonso y Gomez-Gil, 2012) en su publicación para la revista *Sensors* titulada *Brain computer interfaces, a review*.

	Sujeto 2		Sujeto 3		Sujeto 4		Sujeto 5		Sujeto 6		Sujeto 7		Sujeto 8		Sujeto 9	
	Banda	Efect. %	Banda	Efect. %	Banda	Efect. %	Banda	Efect. %	Banda	Efect. %	Banda	Efect. %	Banda	Efect. %	Banda	Efect. %
Sujeto 1	23-34:	99.71%	3-9:	100.00%	33-47:	98.83%	20-48:	98.98%	4-9:	100.00%	36-48:	99.91%	34-40:	90.71%	39-48:	98.29%
Sujeto 2			28-49:	98.76%	11-14:	100.00%	9-12:	99.80%	1-48:	100.00%	38-46:	98.16%	10-36:	99.98%	41-47:	97.77%
Sujeto 3					32-41:	99.42%	15-49:	99.95%	23-30:	94.59%	4-7:	100.00%	31-49:	99.11%	35-48:	98.08%
Sujeto 4							11-15:	97.99%	4-7:	100.00%	3-9:	99.81%	23-38:	97.74%	10-12:	97.70%
Sujeto 5									15-49:	99.48%	4-9:	100.00%	18-24:	99.54%	1-7:	98.52%
Sujeto 6											4-7:	100.00%	3-7:	99.92%	2-7:	100.00%
Sujeto 7													27-49:	98.16%	33-49:	82.14%
Sujeto 8															20-23:	97.05%

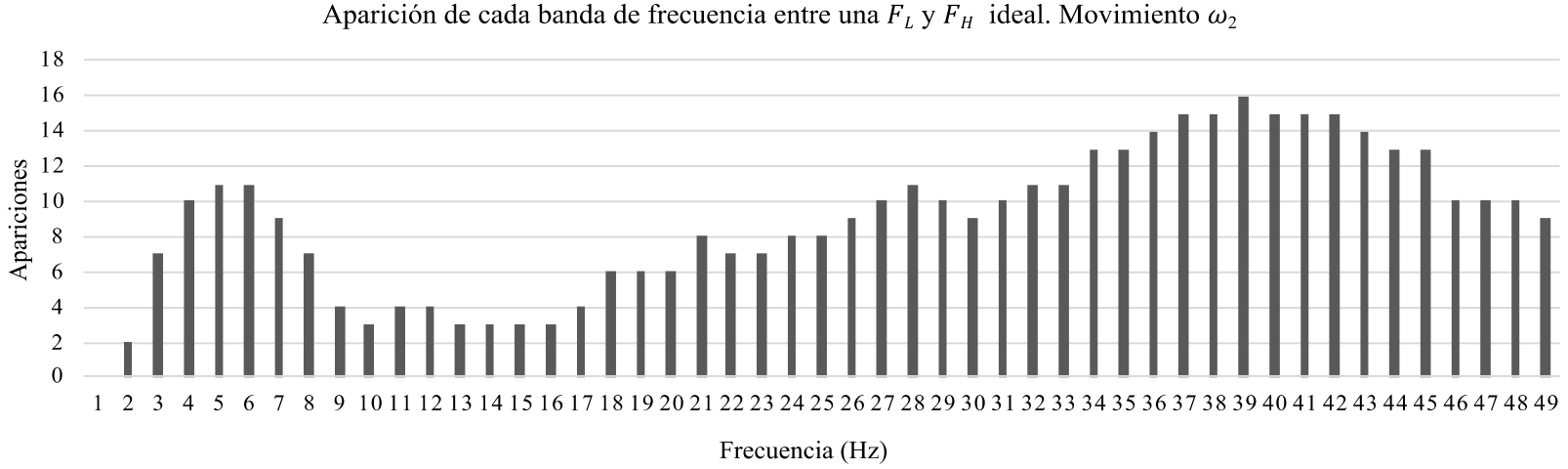
Anexo 2 (Tabla 1.1). Bandas de frecuencia ideales para ω_1. Bandas de frecuencia ideales para cada combinación binaria no-redundante de sujetos y su efectividad empleando la clase de movimiento ω_1. Las casillas en color gris corresponden a permutaciones de sujetos no relevantes.

	Sujeto 2		Sujeto 3		Sujeto 4		Sujeto 5		Sujeto 6		Sujeto 7		Sujeto 8		Sujeto 9	
	Banda	Efect. %	Banda	Efect. %	Banda	Efect. %	Banda	Efect. %	Banda	Efect. %	Banda	Efect. %	Banda	Efect. %	Banda	Efect. %
Sujeto 1	25-32:	99.22%	3-8:	100.00%	26-39:	99.44%	21-45:	99.17%	3-9:	100.00%	37-49:	99.66%	32-43:	92.13%	39-49:	97.58%
Sujeto 2			31-42:	98.41%	11-12:	98.76%	10-12:	99.36%	4-49:	100.00%	37-49:	98.96%	11-36:	99.88%	2-7:	99.41%
Sujeto 3					34-49:	98.88%	27-49:	99.33%	21-49:	97.86%	26-49:	100.00%	33-49:	99.53%	36-45:	98.88%
Sujeto 4							18-21:	94.61%	3-6:	99.95%	3-10:	99.92%	23-28:	96.64%	17-20:	96.62%
Sujeto 5									13-25:	99.88%	4-9:	99.98%	21-29:	99.46%	2-8:	99.03%
Sujeto 6											5-9:	100.00%	4-7:	99.98%	3-6:	100.00%
Sujeto 7													28-48:	97.66%	34-45:	87.44%
Sujeto 8															18-22:	98.73%

Anexo 3 (Tabla 1.2). Bandas de frecuencia ideales para ω_2. Bandas de frecuencia ideales para cada combinación binaria no-redundante de sujetos y su efectividad empleando la clase de movimiento ω_2. Las casillas en color gris corresponden a permutaciones de sujetos no relevantes.



Anexo 4 (Figura 5). Apariciones de cada frecuencia en el conjunto de ideales del movimiento ω_1 i.e., tabla 1.1. A partir de este elemento es posible determinar las bandas de frecuencia ideales para el filtrado.



Anexo 5 (Figura 6). Número de apariciones de cada frecuencia en el conjunto de ideales del movimiento ω_1 i.e., tabla 1.2. A partir de este elemento es posible determinar las bandas de frecuencia ideales para el filtrado.

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 93.29%	TR: 99.06%	TR: 99.58%	TR: 100.00%	TR: 99.53%	TR: 100.00%	TR: 100.00%	TR: 83.15%	TR: 96.24%
Sujeto 2	TR: 93.15%	TA: 95.59%	TR: 99.62%	TR: 96.29%	TR: 51.83%	TR: 100.00%	TR: 100.00%	TR: 99.81%	TR: 98.08%
Sujeto 3	TR: 100.00%	TR: 100.00%	TA: 97.84%	TR: 100.00%	TR: 100.00%	TR: 91.97%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 99.91%	TR: 99.48%	TR: 100.00%	TA: 93.05%	TR: 90.05%	TR: 100.00%	TR: 99.95%	TR: 68.31%	TR: 71.13%
Sujeto 5	TR: 97.93%	TR: 71.97%	TR: 100.00%	TR: 75.02%	TA: 89.91%	TR: 100.00%	TR: 100.00%	TR: 93.85%	TR: 96.48%
Sujeto 6	TR: 100.00%	TR: 100.00%	TR: 97.98%	TR: 100.00%	TR: 100.00%	TA: 99.01%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 7	TR: 100.00%	TR: 98.26%	TR: 100.00%	TR: 99.81%	TR: 100.00%	TR: 99.86%	TA: 98.31%	TR: 100.00%	TR: 80.80%
Sujeto 8	TR: 92.77%	TR: 100.00%	TR: 99.95%	TR: 94.37%	TR: 97.89%	TR: 100.00%	TR: 100.00%	TA: 89.53%	TR: 59.20%
Sujeto 9	TR: 97.00%	TR: 98.26%	TR: 99.86%	TR: 91.92%	TR: 95.12%	TR: 100.00%	TR: 91.31%	TR: 66.95%	TA: 90.00%
Promedio	TSR: 97.12%	TSR: 95.85%	TSR: 99.43%	TSR: 94.50%	TSR: 91.59%	TSR: 98.98%	TSR: 98.84%	TSR: 89.07%	TSR: 87.99%

Anexo 6 (Tabla 1.3). Efectividades en la etapa de autenticación (Fase I) empleando ω_1. El sujeto que encabeza cada fila es el cliente. El sujeto que encabeza cada columna pretende acceder. Se resaltan efectividades bajas $< 80.00\%$.

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 94.93%	TR: 98.53%	TR: 99.29%	TR: 99.82%	TR: 98.44%	TR: 100.00%	TR: 100.00%	TR: 81.29%	TR: 91.82%
Sujeto 2	TR: 93.91%	TA: 92.93%	TR: 99.02%	TR: 82.89%	TR: 51.33%	TR: 99.07%	TR: 99.87%	TR: 99.96%	TR: 97.91%
Sujeto 3	TR: 100.00%	TR: 100.00%	TA: 96.67%	TR: 100.00%	TR: 100.00%	TR: 93.82%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 98.53%	TR: 95.38%	TR: 100.00%	TA: 93.60%	TR: 71.07%	TR: 100.00%	TR: 99.87%	TR: 78.09%	TR: 67.69%
Sujeto 5	TR: 97.07%	TR: 72.27%	TR: 98.98%	TR: 61.56%	TA: 89.02%	TR: 99.56%	TR: 99.82%	TR: 97.38%	TR: 94.76%
Sujeto 6	TR: 100.00%	TR: 100.00%	TR: 98.44%	TR: 100.00%	TR: 100.00%	TA: 99.16%	TR: 100.00%	TR: 99.96%	TR: 100.00%
Sujeto 7	TR: 100.00%	TR: 99.29%	TR: 100.00%	TR: 98.27%	TR: 99.33%	TR: 99.56%	TA: 98.71%	TR: 100.00%	TR: 73.73%
Sujeto 8	TR: 88.22%	TR: 100.00%	TR: 100.00%	TR: 96.27%	TR: 98.40%	TR: 100.00%	TR: 100.00%	TA: 90.58%	TR: 67.38%
Sujeto 9	TR: 94.89%	TR: 98.04%	TR: 99.91%	TR: 83.20%	TR: 90.58%	TR: 99.96%	TR: 89.11%	TR: 80.04%	TA: 89.87%
Promedio	TSR: 96.39%	TSR: 95.16%	TSR: 99.15%	TSR: 90.62%	TSR: 88.69%	TSR: 99.01%	TSR: 98.60%	TSR: 91.92%	TSR: 87.02%

Anexo 7 (Tabla 1.4). Efectividades en la etapa de autenticación (Fase I) empleando ω_2. El sujeto que encabeza cada fila es el cliente. El sujeto que encabeza cada columna pretende acceder. Se resaltan efectividades bajas $< 80.00\%$.

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 98.25%	TR: 94.74%	TR: 100.00%	TR: 94.74%	TR: 98.25%	TR: 100.00%	TR: 100.00%	TR: 68.42%	TR: 100.00%
Sujeto 2	TR: 75.44%	TA: 98.36%	TR: 100.00%	TR: 5.71%	TR: 22.86%	TR: 100.00%	TR: 100.00%	TR: 89.55%	TR: 91.80%
Sujeto 3	TR: 100.00%	TR: 100.00%	TA: 87.04%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 94.74%	TR: 60.00%	TR: 100.00%	TA: 95.08%	TR: 28.77%	TR: 100.00%	TR: 100.00%	TR: 83.58%	TR: 63.93%
Sujeto 5	TR: 92.98%	TR: 24.29%	TR: 100.00%	TR: 27.40%	TA: 98.36%	TR: 100.00%	TR: 100.00%	TR: 79.10%	TR: 96.72%
Sujeto 6	TR: 100.00%	TR: 93.44%	TR: 100.00%	TR: 98.36%	TR: 91.80%	TA: 26.23%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 7	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 97.06%	TR: 100.00%	TR: 100.00%	TA: 67.21%	TR: 95.52%	TR: 45.90%
Sujeto 8	TR: 43.86%	TR: 73.13%	TR: 100.00%	TR: 41.79%	TR: 52.24%	TR: 100.00%	TR: 100.00%	TA: 95.08%	TR: 90.16%
Sujeto 9	TR: 77.19%	TR: 91.80%	TR: 100.00%	TR: 59.02%	TR: 77.05%	TR: 100.00%	TR: 93.44%	TR: 11.48%	TA: 90.16%
Promedio	TSR: 86.94%	TSR: 81.75%	TSR: 98.56%	TSR: 68.80%	TSR: 74.37%	TSR: 91.80%	TSR: 95.63%	TSR: 78.46%	TSR: 86.06%

Anexo 8 (Tabla 2.1). Efectividades en prueba piloto (Fase II) empleando ω_1. El sujeto que encabeza cada fila es el cliente. El sujeto que encabeza cada columna pretende acceder. Se resaltan efectividades bajas i.e., $< 80.00\%$.

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 95.24%	TR: 87.30%	TR: 100.00%	TR: 93.65%	TR: 90.48%	TR: 100.00%	TR: 100.00%	TR: 58.06%	TR: 100.00%
Sujeto 2	TR: 88.89%	TA: 95.38%	TR: 100.00%	TR: 21.54%	TR: 15.38%	TR: 100.00%	TR: 100.00%	TR: 98.39%	TR: 85.71%
Sujeto 3	TR: 100.00%	TR: 100.00%	TA: 96.36%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 90.48%	TR: 41.54%	TR: 100.00%	TA: 95.38%	TR: 18.84%	TR: 100.00%	TR: 97.26%	TR: 87.10%	TR: 74.60%
Sujeto 5	TR: 92.06%	TR: 26.15%	TR: 100.00%	TR: 28.99%	TA: 95.38%	TR: 100.00%	TR: 100.00%	TR: 87.10%	TR: 88.89%
Sujeto 6	TR: 100.00%	TR: 96.55%	TR: 100.00%	TR: 100.00%	TR: 94.83%	TA: 94.83%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 7	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 89.04%	TR: 98.55%	TR: 100.00%	TA: 95.38%	TR: 100.00%	TR: 26.98%
Sujeto 8	TR: 30.65%	TR: 75.81%	TR: 100.00%	TR: 45.16%	TR: 50.00%	TR: 100.00%	TR: 100.00%	TA: 95.16%	TR: 100.00%
Sujeto 9	TR: 65.08%	TR: 80.95%	TR: 100.00%	TR: 11.11%	TR: 60.32%	TR: 100.00%	TR: 90.48%	TR: 16.13%	TA: 95.24%
Promedio	TSR: 84.71%	TSR: 78.19%	TSR: 99.60%	TSR: 64.99%	TSR: 69.31%	TSR: 99.43%	TSR: 98.12%	TSR: 82.44%	TSR: 85.71%

Anexo 9 (Tabla 2.2). Efectividades en prueba piloto (Fase II) empleando ω_2. El sujeto que encabeza cada fila es el cliente. El sujeto que encabeza cada columna pretende acceder. Se resaltan efectividades bajas i.e., $< 80.00\%$.

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 96.49%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 80.70%	TR: 100.00%
Sujeto 2	TR: 100.00%	TA: 92.31%	TR: 100.00%	TR: 24.62%	TR: 29.23%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 98.36%
Sujeto 3	TR: 100.00%	TR: 100.00%	TA: 85.19%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 100.00%	TR: 70.77%	TR: 100.00%	TA: 94.59%	TR: 43.48%	TR: 100.00%	TR: 100.00%	TR: 96.77%	TR: 91.80%
Sujeto 5	TR: 100.00%	TR: 44.62%	TR: 100.00%	TR: 42.03%	TA: 98.55%	TR: 100.00%	TR: 100.00%	TR: 98.39%	TR: 98.36%
Sujeto 6	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 15.52%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 7	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 50.00%	TR: 100.00%	TR: 63.93%
Sujeto 8	TR: 59.65%	TR: 93.55%	TR: 100.00%	TR: 66.13%	TR: 77.42%	TR: 100.00%	TR: 100.00%	TA: 93.55%	TR: 100.00%
Sujeto 9	TR: 89.47%	TR: 96.72%	TR: 100.00%	TR: 63.93%	TR: 91.80%	TR: 100.00%	TR: 96.72%	TR: 24.59%	TA: 85.25%
Promedio	TSR: 93.96%	TSR: 88.66%	TSR: 98.35%	TSR: 76.81%	ACC: 82.28%	ACC: 90.61%	ACC: 94.08%	ACC: 88.22%	ACC: 93.08%

Anexo 10 (Tabla 2.3). Efectividades (Fase II) combinando ω_1 y ω_2 i.e., movimiento de mano izquierda y derecha. Se resaltan efectividades bajas i.e., < 80.00. El TSR promedio es de 89.56%.

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 86.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 96.00%	TR: 100.00%
Sujeto 2	TR: 98.00%	TA: 96.43%	TR: 100.00%	TR: 69.64%	TR: 21.43%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 3	TR: 100.00%	TR: 100.00%	TA: 91.49%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 98.00%	TR: 73.21%	TR: 100.00%	TA: 94.03%	TR: 65.08%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 5	TR: 98.00%	TR: 23.21%	TR: 100.00%	TR: 95.24%	TA: 98.41%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 85.45%
Sujeto 6	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 98.08%	TR: 100.00%	TA: 71.15%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 7	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 62.30%	TR: 100.00%	TR: 40.00%
Sujeto 8	TR: 76.00%	TR: 100.00%	TR: 100.00%	TR: 74.14%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 67.24%	TR: 100.00%
Sujeto 9	TR: 90.00%	TR: 87.27%	TR: 100.00%	TR: 89.09%	TR: 67.27%	TR: 100.00%	TR: 90.91%	TR: 100.00%	TA: 96.36%
Promedio	TSR: 94.00%	TSR: 86.68%	TSR: 99.05%	TSR: 91.14%	TSR: 83.58%	TSR: 96.79%	TSR: 94.80%	TSR: 95.92%	TSR: 91.31%

Anexo 11 (Tabla 2.4). Efectividades agregando bandas 20-23 y 18-22Hz. Efectividades en la fase II tras agregar las bandas de frecuencia 20-23 y 18-22Hz. Se resaltan efectividades bajas i.e., $< 80.00\%$. El TSR promedio es 91.01%.

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 90.32%	TR: 82.14%	TR: 96.00%	TR: 41.94%	TR: 74.19%	TR: 100.00%	TR: 77.42%	TR: 61.29%	TR: 30.77%
Sujeto 2	TR: 96.43%	TA: 100.00%	TR: 20.00%	TR: 35.71%	TR: 3.57%	TR: 0.00%	TR: 75.00%	TR: 92.86%	TR: 100.00%
Sujeto 3	TR: 100.00%	TR: 0.00%	TA: 96.00%	TR: 96.00%	TR: 44.00%	TR: 0.00%	TR: 96.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 96.77%	TR: 0.00%	TR: 96.00%	TA: 100.00%	TR: 4.88%	TR: 0.00%	TR: 81.58%	TR: 68.75%	TR: 100.00%
Sujeto 5	TR: 96.77%	TR: 0.00%	TR: 52.00%	TR: 51.22%	TA: 100.00%	TR: 4.55%	TR: 76.32%	TR: 100.00%	TR: 96.15%
Sujeto 6	TR: 100.00%	TR: 0.00%	TR: 40.91%	TR: 54.55%	TR: 4.55%	TA: 100.00%	TR: 81.82%	TR: 100.00%	TR: 100.00%
Sujeto 7	TR: 100.00%	TR: 92.86%	TR: 100.00%	TR: 52.63%	TR: 36.84%	TR: 100.00%	TA: 42.11%	TR: 75.00%	TR: 11.54%
Sujeto 8	TR: 61.29%	TR: 96.43%	TR: 100.00%	TR: 6.25%	TR: 71.88%	TR: 100.00%	TR: 78.12%	TA: 21.88%	TR: 73.08%
Sujeto 9	TR: 34.62%	TR: 80.77%	TR: 100.00%	TR: 100.00%	TR: 42.31%	TR: 100.00%	TR: 61.54%	TR: 80.77%	TA: 96.15%
Promedio	TSR: 86.24%	TSR: 50.24%	TSR: 77.88%	TSR: 59.81%	TSR: 42.47%	TSR: 56.06%	TSR: 74.43%	TSR: 77.84%	TSR: 78.63%

Anexo 12 (Tabla 2.5). Efectividades entrenando con δ_1 y accediendo con δ_2. Se resaltan efectividades bajas i.e., < 80.00. El TSR promedio es de 67.07%.

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 76.67%	TR: 93.33%	TR: 100.00%	TR: 30.00%	TR: 80.00%	TR: 100.00%	TR: 100.00%	TR: 96.67%	TR: 40.00%
Sujeto 2	TR: 40.00%	TA: 100.00%	TR: 8.57%	TR: 26.83%	TR: 0.00%	TR: 2.33%	TR: 100.00%	TR: 100.00%	TR: 41.86%
Sujeto 3	TR: 93.33%	TR: 2.86%	TA: 100.00%	TR: 77.14%	TR: 25.71%	TR: 0.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 40.00%	TR: 7.32%	TR: 68.57%	TA: 95.12%	TR: 4.88%	TR: 56.10%	TR: 100.00%	TR: 100.00%	TR: 60.98%
Sujeto 5	TR: 36.67%	TR: 0.00%	TR: 37.14%	TR: 26.83%	TA: 100.00%	TR: 91.11%	TR: 100.00%	TR: 100.00%	TR: 23.26%
Sujeto 6	TR: 60.00%	TR: 0.00%	TR: 2.86%	TR: 41.46%	TR: 0.00%	TA: 100.00%	TR: 100.00%	TR: 100.00%	TR: 55.81%
Sujeto 7	TR: 46.67%	TR: 84.62%	TR: 100.00%	TR: 53.85%	TR: 30.77%	TR: 100.00%	TA: 10.26%	TR: 96.77%	TR: 0.00%
Sujeto 8	TR: 23.33%	TR: 87.10%	TR: 100.00%	TR: 3.23%	TR: 90.32%	TR: 100.00%	TR: 100.00%	TA: 45.16%	TR: 64.52%
Sujeto 9	TR: 30.00%	TR: 95.35%	TR: 100.00%	TR: 68.29%	TR: 39.53%	TR: 100.00%	TR: 100.00%	TR: 40.00%	TA: 100.00%
Promedio	TSR: 49.63%	TSR: 52.29%	TSR: 68.57%	TSR: 46.97%	TSR: 41.25%	TSR: 72.17%	TSR: 90.03%	TSR: 86.51%	TSR: 54.05%

Anexo 13 (Tabla 2.6). Efectividades entrenando con δ_1 y accediendo con δ_3. Se resaltan efectividades bajas i.e., < 80.00. El TSR promedio es de 62.38%.

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 46.67%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 53.33%	TR: 96.67%
Sujeto 2	TR: 43.33%	TA: 100.00%	TR: 65.71%	TR: 31.71%	TR: 0.00%	TR: 97.67%	TR: 100.00%	TR: 100.00%	TR: 67.44%
Sujeto 3	TR: 86.67%	TR: 8.57%	TA: 100.00%	TR: 82.86%	TR: 51.43%	TR: 88.57%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 40.00%	TR: 4.88%	TR: 94.29%	TA: 95.12%	TR: 4.88%	TR: 70.73%	TR: 100.00%	TR: 100.00%	TR: 56.10%
Sujeto 5	TR: 36.67%	TR: 0.00%	TR: 48.57%	TR: 24.39%	TA: 100.00%	TR: 75.56%	TR: 100.00%	TR: 100.00%	TR: 16.28%
Sujeto 6	TR: 66.67%	TR: 0.00%	TR: 5.71%	TR: 53.66%	TR: 0.00%	TA: 100.00%	TR: 100.00%	TR: 100.00%	TR: 58.14%
Sujeto 7	TR: 93.33%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 46.15%	TR: 96.77%	TR: 64.10%
Sujeto 8	TR: 80.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 96.77%	TR: 96.77%
Sujeto 9	TR: 66.67%	TR: 100.00%	TR: 100.00%	TR: 97.56%	TR: 100.00%	TR: 100.00%	TR: 92.31%	TR: 90.32%	TA: 95.35%
Promedio	TSR: 62.22%	TSR: 57.05%	TSR: 79.36%	TSR: 76.14%	TSR: 61.81%	TSR: 92.50%	TSR: 93.16%	TSR: 93.02%	TSR: 72.32%

Anexo 14 (Tabla 2.7). Efectividades entrenando con δ_2 y accediendo con δ_2. Se resaltan efectividades bajas i.e., < 80.00. El TSR promedio es de 76.40%.

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 73.08%	TR: 76.92%	TR: 88.46%	TR: 38.46%	TR: 50.00%	TR: 95.65%	TR: 65.38%	TR: 42.31%	TR: 53.85%
Sujeto 2	TR: 100.00%	TA: 100.00%	TR: 24.14%	TR: 43.33%	TR: 0.00%	TR: 0.00%	TR: 80.00%	TR: 88.46%	TR: 96.30%
Sujeto 3	TR: 100.00%	TR: 3.45%	TA: 100.00%	TR: 100.00%	TR: 51.72%	TR: 13.04%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 100.00%	TR: 3.33%	TR: 79.31%	TA: 100.00%	TR: 11.36%	TR: 4.35%	TR: 88.24%	TR: 69.23%	TR: 92.59%
Sujeto 5	TR: 96.15%	TR: 0.00%	TR: 65.52%	TR: 61.36%	TA: 100.00%	TR: 0.00%	TR: 79.41%	TR: 92.31%	TR: 92.59%
Sujeto 6	TR: 100.00%	TR: 0.00%	TR: 56.52%	TR: 60.87%	TR: 0.00%	TA: 100.00%	TR: 91.30%	TR: 100.00%	TR: 100.00%
Sujeto 7	TR: 96.15%	TR: 93.33%	TR: 100.00%	TR: 47.06%	TR: 38.24%	TR: 100.00%	TA: 41.18%	TR: 69.23%	TR: 7.41%
Sujeto 8	TR: 53.85%	TR: 80.77%	TR: 100.00%	TR: 15.38%	TR: 34.62%	TR: 95.65%	TR: 73.08%	TA: 76.92%	TR: 73.08%
Sujeto 9	TR: 53.85%	TR: 85.19%	TR: 100.00%	TR: 100.00%	TR: 33.33%	TR: 100.00%	TR: 62.96%	TR: 53.85%	TA: 96.30%
Promedio	TSR: 85.90%	TSR: 49.22%	TSR: 79.33%	TSR: 62.94%	TSR: 35.47%	TSR: 56.52%	TSR: 75.73%	TSR: 76.92%	TSR: 79.12%

Anexo 15 (Tabla 2.8). Efectividades empleando rango intercuartil como característica. Entrenamiento con δ_1 y acceso con δ_2. Se resaltan efectividades bajas i.e., < 80.00. El TSR promedio es de 66.80%.

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 94.12%	TR: 76.47%	TR: 82.35%	TR: 20.59%	TR: 50.00%	TR: 97.06%	TR: 97.06%	TR: 82.35%	TR: 29.41%
Sujeto 2	TR: 35.29%	TA: 100.00%	TR: 2.78%	TR: 38.46%	TR: 0.00%	TR: 2.44%	TR: 100.00%	TR: 100.00%	TR: 41.03%
Sujeto 3	TR: 100.00%	TR: 5.56%	TA: 100.00%	TR: 83.33%	TR: 25.00%	TR: 2.78%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 55.88%	TR: 15.38%	TR: 50.00%	TA: 94.87%	TR: 7.69%	TR: 71.79%	TR: 97.37%	TR: 97.14%	TR: 79.49%
Sujeto 5	TR: 38.24%	TR: 0.00%	TR: 19.44%	TR: 38.46%	TA: 100.00%	TR: 68.29%	TR: 100.00%	TR: 100.00%	TR: 25.64%
Sujeto 6	TR: 61.76%	TR: 0.00%	TR: 5.56%	TR: 43.59%	TR: 0.00%	TA: 100.00%	TR: 100.00%	TR: 100.00%	TR: 61.54%
Sujeto 7	TR: 38.24%	TR: 84.21%	TR: 100.00%	TR: 57.89%	TR: 44.74%	TR: 100.00%	TA: 15.79%	TR: 88.57%	TR: 0.00%
Sujeto 8	TR: 14.71%	TR: 97.14%	TR: 100.00%	TR: 8.57%	TR: 34.29%	TR: 100.00%	TR: 97.14%	TA: 40.00%	TR: 40.00%
Sujeto 9	TR: 14.71%	TR: 82.05%	TR: 100.00%	TR: 74.36%	TR: 17.95%	TR: 100.00%	TR: 94.74%	TR: 91.43%	TA: 97.44%
Promedio	TSR: 50.33%	TSR: 51.20%	TSR: 62.24%	TSR: 51.12%	TSR: 31.07%	TSR: 71.37%	TSR: 89.12%	TSR: 88.83%	TSR: 52.73%

Anexo 16 (Tabla 2.9). Efectividades empleando rango intercuartil como característica. Entrenamiento con δ_1 y acceso con δ_3. Se resaltan efectividades bajas i.e., < 80.00. El TSR promedio es de 60.89%.

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 11.76%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 73.53%	TR: 97.06%
Sujeto 2	TR: 55.88%	TA: 100.00%	TR: 52.78%	TR: 38.46%	TR: 0.00%	TR: 92.68%	TR: 100.00%	TR: 100.00%	TR: 71.79%
Sujeto 3	TR: 100.00%	TR: 11.11%	TA: 100.00%	TR: 86.11%	TR: 44.44%	TR: 52.78%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 52.94%	TR: 7.69%	TR: 88.89%	TA: 94.87%	TR: 5.13%	TR: 28.21%	TR: 97.37%	TR: 94.29%	TR: 58.97%
Sujeto 5	TR: 32.35%	TR: 0.00%	TR: 16.67%	TR: 30.77%	TA: 100.00%	TR: 14.63%	TR: 97.37%	TR: 100.00%	TR: 17.95%
Sujeto 6	TR: 61.76%	TR: 2.44%	TR: 5.56%	TR: 43.59%	TR: 0.00%	TA: 100.00%	TR: 100.00%	TR: 100.00%	TR: 58.97%
Sujeto 7	TR: 85.29%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 31.58%	TR: 100.00%	TR: 36.84%
Sujeto 8	TR: 41.18%	TR: 100.00%	TR: 100.00%	TR: 62.86%	TR: 100.00%	TR: 100.00%	TR: 94.29%	TA: 82.86%	TR: 68.57%
Sujeto 9	TR: 47.06%	TR: 100.00%	TR: 100.00%	TR: 94.87%	TR: 100.00%	TR: 100.00%	TR: 94.74%	TR: 88.57%	TA: 92.31%
Promedio	TSR: 54.25%	TSR: 57.92%	TSR: 73.77%	TSR: 72.39%	TSR: 61.06%	TSR: 76.48%	TSR: 90.59%	TSR: 93.25%	TSR: 66.94%

Anexo 17 (Tabla 2.10). Efectividades empleando rango intercuartil como característica. Entrenamiento con δ_2 y acceso con δ_3. Se resaltan efectividades bajas i.e., < 80.00. El TSR promedio es de 71.85%

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 75.00%	TR: 75.00%	TR: 92.86%	TR: 46.43%	TR: 57.14%	TR: 100.00%	TR: 67.86%	TR: 45.45%	TR: 38.46%
Sujeto 2	TR: 100.00%	TA: 100.00%	TR: 20.69%	TR: 45.16%	TR: 0.00%	TR: 0.00%	TR: 80.65%	TR: 95.45%	TR: 96.15%
Sujeto 3	TR: 100.00%	TR: 3.45%	TA: 100.00%	TR: 100.00%	TR: 62.07%	TR: 7.41%	TR: 96.55%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 100.00%	TR: 9.68%	TR: 79.31%	TA: 100.00%	TR: 11.36%	TR: 11.11%	TR: 91.43%	TR: 72.73%	TR: 100.00%
Sujeto 5	TR: 100.00%	TR: 0.00%	TR: 62.07%	TR: 64.64%	TA: 100.00%	TR: 0.00%	TR: 80.00%	TR: 95.45%	TR: 92.31%
Sujeto 6	TR: 100.00%	TR: 0.00%	TR: 40.74%	TR: 51.85%	TR: 0.00%	TA: 100.00%	TR: 85.19%	TR: 95.45%	TR: 100.00%
Sujeto 7	TR: 100.00%	TR: 93.55%	TR: 100.00%	TR: 57.14%	TR: 13.14%	TR: 100.00%	TA: 42.86%	TR: 63.64%	TR: 7.69%
Sujeto 8	TR: 50.00%	TR: 77.27%	TR: 100.00%	TR: 18.18%	TR: 50.00%	TR: 95.45%	TR: 81.82%	TA: 77.27%	TR: 77.27%
Sujeto 9	TR: 50.00%	TR: 88.46%	TR: 100.00%	TR: 100.00%	TR: 34.62%	TR: 100.00%	TR: 65.38%	TR: 50.00%	TA: 96.15%
Promedio	TSR: 86.11%	TSR: 49.71%	TSR: 77.30%	TSR: 64.82%	TSR: 36.48%	TSR: 57.11%	TSR: 76.86%	TSR: 77.27%	TSR: 78.67%

Anexo 18 (Tabla 2.11). Efectividades empleando desviación de la mediana absoluta como característica. Entrenamiento con δ_1 y acceso con δ_2. Se resaltan efectividades bajas i.e., < 80.00. El TSR promedio es de 67.15%

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 91.43%	TR: 77.14%	TR: 85.71%	TR: 28.57%	TR: 34.29%	TR: 85.71%	TR: 94.29%	TR: 82.86%	TR: 20.00%
Sujeto 2	TR: 40.00%	TA: 100.00%	TR: 2.86%	TR: 33.33%	TR: 0.00%	TR: 0.00%	TR: 100.00%	TR: 100.00%	TR: 39.47%
Sujeto 3	TR: 94.29%	TR: 5.71%	TA: 100.00%	TR: 80.00%	TR: 40.00%	TR: 2.86%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 54.29%	TR: 17.95%	TR: 65.71%	TA: 94.87%	TR: 12.82%	TR: 61.54%	TR: 100.00%	TR: 97.22%	TR: 81.58%
Sujeto 5	TR: 37.14%	TR: 0.00%	TR: 8.57%	TR: 35.90%	TA: 100.00%	TR: 36.59%	TR: 100.00%	TR: 100.00%	TR: 31.58%
Sujeto 6	TR: 57.14%	TR: 0.00%	TR: 5.71%	TR: 43.59%	TR: 0.00%	TA: 100.00%	TR: 100.00%	TR: 100.00%	TR: 57.89%
Sujeto 7	TR: 37.14%	TR: 84.21%	TR: 100.00%	TR: 55.26%	TR: 34.21%	TR: 100.00%	TA: 15.79%	TR: 88.89%	TR: 0.00%
Sujeto 8	TR: 17.14%	TR: 88.89%	TR: 100.00%	TR: 2.78%	TR: 33.33%	TR: 97.22%	TR: 94.44%	TA: 41.67%	TR: 38.89%
Sujeto 9	TR: 17.14%	TR: 76.32%	TR: 100.00%	TR: 81.58%	TR: 21.05%	TR: 97.37%	TR: 92.11%	TR: 88.89%	TA: 97.37%
Promedio	TSR: 49.52%	TSR: 50.02%	TSR: 63.17%	TSR: 50.65%	TSR: 30.63%	TSR: 64.59%	TSR: 88.51%	TSR: 88.84%	TSR: 51.86%

Anexo 19 (Tabla 2.12). Efectividades empleando desviación de la mediana absoluta como característica. Entrenamiento con δ_1 y acceso con δ_3. Se resaltan efectividades bajas i.e., < 80.00. El TSR promedio es de 59.76%

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 31.43%	TR: 100.00%	TR: 100.00%	TR: 97.14%	TR: 100.00%	TR: 100.00%	TR: 97.14%	TR: 74.29%	TR: 91.43%
Sujeto 2	TR: 51.43%	TA: 100.00%	TR: 48.57%	TR: 38.46%	TR: 0.00%	TR: 87.80%	TR: 100.00%	TR: 100.00%	TR: 84.21%
Sujeto 3	TR: 91.43%	TR: 11.43%	TA: 100.00%	TR: 80.00%	TR: 57.14%	TR: 57.14%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 54.29%	TR: 17.95%	TR: 88.57%	TA: 97.44%	TR: 5.13%	TR: 30.77%	TR: 100.00%	TR: 97.22%	TR: 68.42%
Sujeto 5	TR: 37.14%	TR: 0.00%	TR: 14.29%	TR: 33.33%	TA: 100.00%	TR: 12.20%	TR: 100.00%	TR: 100.00%	TR: 23.68%
Sujeto 6	TR: 60.00%	TR: 2.44%	TR: 5.71%	TR: 41.03%	TR: 0.00%	TA: 100.00%	TR: 100.00%	TR: 100.00%	TR: 60.53%
Sujeto 7	TR: 80.00%	TR: 97.37%	TR: 100.00%	TR: 100.00%	TR: 97.37%	TR: 100.00%	TA: 28.95%	TR: 97.22%	TR: 28.95%
Sujeto 8	TR: 37.14%	TR: 100.00%	TR: 100.00%	TR: 69.44%	TR: 97.22%	TR: 100.00%	TR: 94.44%	TA: 72.22%	TR: 66.67%
Sujeto 9	TR: 45.71%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 97.37%	TR: 100.00%	TR: 89.47%	TR: 88.89%	TA: 86.84%
Promedio	TSR: 54.29%	TSR: 58.80%	TSR: 73.02%	TSR: 72.98%	TSR: 61.58%	TSR: 76.43%	TSR: 90.00%	TSR: 92.20%	TSR: 67.86%

Anexo 20 (Tabla 2.13). Efectividades empleando desviación de la mediana absoluta como característica. Entrenamiento con δ_2 y acceso con δ_3. Se resaltan efectividades bajas i.e., < 80.00. El TSR promedio es de 71.91%

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 100.00%	TR: 0.00%	TR: 95.24%	TR: 30.43%	TR: 0.00%	TR: 45.00%	TR: 73.91%	TR: 43.48%	TR: 0.00%
Sujeto 2	TR: 4.35%	TA: 100.00%	TR: 100.00%	TR: 33.33%	TR: 0.00%	TR: 20.00%	TR: 59.26%	TR: 56.00%	TR: 0.00%
Sujeto 3	TR: 100.00%	TR: 95.24%	TA: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 13.04%	TR: 66.67%	TR: 100.00%	TA: 97.37%	TR: 63.89%	TR: 85.00%	TR: 87.10%	TR: 12.00%	TR: 43.48%
Sujeto 5	TR: 60.87%	TR: 11.11%	TR: 100.00%	TR: 91.67%	TA: 100.00%	TR: 40.00%	TR: 58.06%	TR: 52.00%	TR: 0.00%
Sujeto 6	TR: 20.00%	TR: 20.00%	TR: 100.00%	TR: 25.00%	TR: 0.00%	TA: 95.00%	TR: 65.00%	TR: 60.00%	TR: 0.00%
Sujeto 7	TR: 100.00%	TR: 74.07%	TR: 100.00%	TR: 32.26%	TR: 22.58%	TR: 100.00%	TA: 70.97%	TR: 80.00%	TR: 17.39%
Sujeto 8	TR: 4.35%	TR: 68.00%	TR: 100.00%	TR: 8.00%	TR: 16.00%	TR: 85.00%	TR: 64.00%	TA: 88.00%	TR: 0.00%
Sujeto 9	TR: 0.00%	TR: 8.70%	TR: 100.00%	TR: 86.96%	TR: 4.35%	TR: 90.00%	TR: 65.22%	TR: 34.78%	TA: 100.00%
Promedio	TSR: 44.73%	TSR: 49.31%	TSR: 99.47%	TSR: 56.11%	TSR: 34.09%	TSR: 73.33%	TSR: 71.50%	TSR: 58.47%	TSR: 28.99%

Anexo 21 (Tabla 2.14). Efectividades empleando dimensión fractal de *Katz* como característica. Entrenamiento con δ_1 y acceso con δ_2. Se resaltan efectividades bajas i.e., < 80.00. El TSR promedio es de 57.33%

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 96.55%	TR: 0.00%	TR: 93.10%	TR: 13.79%	TR: 0.00%	TR: 93.10%	TR: 100.00%	TR: 80.00%	TR: 0.00%
Sujeto 2	TR: 10.34%	TA: 100.00%	TR: 100.00%	TR: 6.45%	TR: 0.00%	TR: 13.51%	TR: 78.38%	TR: 80.00%	TR: 0.00%
Sujeto 3	TR: 100.00%	TR: 100.00%	TA: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 20.69%	TR: 80.65%	TR: 100.00%	TA: 87.10%	TR: 90.32%	TR: 96.77%	TR: 100.00%	TR: 52.00%	TR: 77.42%
Sujeto 5	TR: 13.79%	TR: 0.00%	TR: 100.00%	TR: 25.81%	TA: 100.00%	TR: 100.00%	TR: 91.89%	TR: 80.00%	TR: 0.00%
Sujeto 6	TR: 17.24%	TR: 0.00%	TR: 100.00%	TR: 16.13%	TR: 0.00%	TA: 100.00%	TR: 86.49%	TR: 84.00%	TR: 0.00%
Sujeto 7	TR: 37.93%	TR: 5.41%	TR: 100.00%	TR: 25.81%	TR: 2.70%	TR: 100.00%	TA: 51.35%	TR: 88.00%	TR: 0.00%
Sujeto 8	TR: 0.00%	TR: 52.00%	TR: 100.00%	TR: 8.00%	TR: 28.00%	TR: 96.00%	TR: 96.00%	TA: 84.00%	TR: 0.00%
Sujeto 9	TR: 0.00%	TR: 2.70%	TR: 100.00%	TR: 19.35%	TR: 16.22%	TR: 100.00%	TR: 94.59%	TR: 72.00%	TA: 100.00%
Promedio	TSR: 32.95%	TSR: 37.86%	TSR: 99.23%	TSR: 33.60%	TSR: 37.47%	TSR: 88.82%	TSR: 88.74%	TSR: 80.00%	TSR: 30.82%

Anexo 22 (Tabla 2.15). Efectividades empleando dimensión fractal de *Katz* como característica. Entrenamiento con δ_1 y acceso con δ_3. Se resaltan efectividades bajas i.e., < 80.00. El TSR promedio es de 58.83%

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 100.00%	TR: 13.79%	TR: 100.00%	TR: 27.59%	TR: 48.28%	TR: 89.66%	TR: 100.00%	TR: 64.00%	TR: 24.14%
Sujeto 2	TR: 24.14%	TA: 100.00%	TR: 93.33%	TR: 22.58%	TR: 2.70%	TR: 100.00%	TR: 100.00%	TR: 84.00%	TR: 8.11%
Sujeto 3	TR: 100.00%	TR: 100.00%	TA: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 31.03%	TR: 67.74%	TR: 100.00%	TA: 93.55%	TR: 58.06%	TR: 100.00%	TR: 96.77%	TR: 76.00%	TR: 22.58%
Sujeto 5	TR: 3.45%	TR: 0.00%	TR: 100.00%	TR: 19.35%	TA: 100.00%	TR: 90.32%	TR: 89.19%	TR: 80.00%	TR: 0.00%
Sujeto 6	TR: 24.14%	TR: 10.81%	TR: 100.00%	TR: 35.48%	TR: 0.00%	TA: 97.37%	TR: 97.30%	TR: 92.00%	TR: 13.51%
Sujeto 7	TR: 79.31%	TR: 67.57%	TR: 100.00%	TR: 90.32%	TR: 83.78%	TR: 100.00%	TA: 83.78%	TR: 96.00%	TR: 32.43%
Sujeto 8	TR: 16.00%	TR: 84.00%	TR: 100.00%	TR: 20.00%	TR: 72.00%	TR: 100.00%	TR: 100.00%	TA: 100.00%	TR: 20.00%
Sujeto 9	TR: 3.45%	TR: 0.00%	TR: 100.00%	TR: 12.90%	TR: 0.00%	TR: 100.00%	TR: 83.78%	TR: 80.00%	TA: 100.00%
Promedio	TSR: 42.39%	TSR: 49.32%	TSR: 99.26%	TSR: 46.86%	TSR: 51.65%	TSR: 97.48%	TSR: 94.54%	TSR: 85.78%	TSR: 35.64%

Anexo 23 (Tabla 2.16). Efectividades empleando dimensión fractal de *Katz* como característica. Entrenamiento con δ_2 y acceso con δ_3. Se resaltan efectividades bajas i.e., < 80.00. El TSR promedio es de 66.99%

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 73.08%	TR: 82.14%	TR: 96.00%	TR: 46.43%	TR: 74.19%	TR: 100.00%	TR: 77.42%	TR: 61.29%	TR: 53.85%
Sujeto 2	TR: 100.00%	TA: 100.00%	TR: 100.00%	TR: 45.16%	TR: 3.57%	TR: 20.00%	TR: 80.65%	TR: 95.45%	TR: 100.00%
Sujeto 3	TR: 100.00%	TR: 95.24%	TA: 96.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 100.00%	TR: 66.67%	TR: 100.00%	TA: 97.37%	TR: 63.89%	TR: 85.00%	TR: 91.43%	TR: 72.73%	TR: 100.00%
Sujeto 5	TR: 100.00%	TR: 11.11%	TR: 100.00%	TR: 91.67%	TA: 100.00%	TR: 40.00%	TR: 80.00%	TR: 100.00%	TR: 96.15%
Sujeto 6	TR: 100.00%	TR: 20.00%	TR: 100.00%	TR: 60.87%	TR: 4.55%	TA: 95.00%	TR: 91.30%	TR: 100.00%	TR: 100.00%
Sujeto 7	TR: 100.00%	TR: 93.55%	TR: 100.00%	TR: 57.14%	TR: 38.24%	TR: 100.00%	TA: 41.18%	TR: 80.00%	TR: 17.39%
Sujeto 8	TR: 61.29%	TR: 96.43%	TR: 100.00%	TR: 18.18%	TR: 71.88%	TR: 100.00%	TR: 81.82%	TA: 21.88%	TR: 77.27%
Sujeto 9	TR: 53.85%	TR: 88.46%	TR: 100.00%	TR: 100.00%	TR: 42.31%	TR: 100.00%	TR: 65.38%	TR: 80.77%	TA: 96.15%
Promedio	TSR: 87.58%	TSR: 72.62%	TSR: 99.11%	TSR: 68.54%	TSR: 55.40%	TSR: 82.22%	TSR: 78.80%	TSR: 79.12%	TSR: 82.31%

Anexo 24 (Tabla 2.17). Efectividades combinando características i.e., $\sigma(\vec{x})$, $iqr(\vec{x})$, $MAD(\vec{x})$ y $katz(\vec{x})$. Entrenamiento con δ_1 y acceso con δ_2. Se resaltan efectividades bajas i.e., < 80.00. El TSR promedio es de 78.41%

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 76.67%	TR: 93.33%	TR: 100.00%	TR: 30.00%	TR: 80.00%	TR: 100.00%	TR: 100.00%	TR: 96.67%	TR: 40.00%
Sujeto 2	TR: 40.00%	TA: 100.00%	TR: 100.00%	TR: 38.46%	TR: 0.00%	TR: 13.51%	TR: 100.00%	TR: 100.00%	TR: 41.86%
Sujeto 3	TR: 100.00%	TR: 100.00%	TA: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 55.88%	TR: 80.65%	TR: 100.00%	TA: 87.10%	TR: 90.32%	TR: 96.77%	TR: 100.00%	TR: 100.00%	TR: 81.58%
Sujeto 5	TR: 38.24%	TR: 0.00%	TR: 100.00%	TR: 38.46%	TA: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 31.58%
Sujeto 6	TR: 61.76%	TR: 0.00%	TR: 100.00%	TR: 43.59%	TR: 0.00%	TA: 100.00%	TR: 100.00%	TR: 100.00%	TR: 61.54%
Sujeto 7	TR: 46.67%	TR: 84.62%	TR: 100.00%	TR: 57.89%	TR: 44.74%	TR: 100.00%	TA: 10.26%	TR: 96.77%	TR: 0.00%
Sujeto 8	TR: 23.33%	TR: 97.14%	TR: 100.00%	TR: 8.57%	TR: 90.32%	TR: 100.00%	TR: 100.00%	TA: 40.00%	TR: 64.52%
Sujeto 9	TR: 30.00%	TR: 95.35%	TR: 100.00%	TR: 81.58%	TR: 39.53%	TR: 100.00%	TR: 100.00%	TR: 91.43%	TA: 97.37%
Promedio	TSR: 52.51%	TSR: 72.34%	TSR: 100.0%	TSR: 53.96%	TSR: 60.55%	TSR: 90.03%	TSR: 90.03%	TSR: 91.65%	TSR: 57.61%

Anexo 25 (Tabla 2.18). Efectividades combinando características i.e., $\sigma(\vec{x})$, $iqr(\vec{x})$, $MAD(\vec{x})$ y $katz(\vec{x})$. Entrenamiento con δ_1 y acceso con δ_3. Se resaltan efectividades bajas i.e., < 80.00. El TSR promedio es de 74.30%

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 11.76%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 74.29%	TR: 97.06%
Sujeto 2	TR: 55.88%	TA: 100.00%	TR: 93.33%	TR: 38.46%	TR: 2.70%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 84.21%
Sujeto 3	TR: 100.00%	TR: 100.00%	TA: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 54.29%	TR: 67.74%	TR: 100.00%	TA: 93.55%	TR: 58.06%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 68.42%
Sujeto 5	TR: 37.14%	TR: 0.00%	TR: 100.00%	TR: 33.33%	TA: 100.00%	TR: 90.32%	TR: 100.00%	TR: 100.00%	TR: 23.68%
Sujeto 6	TR: 66.67%	TR: 10.81%	TR: 100.00%	TR: 53.66%	TR: 0.00%	TA: 97.37%	TR: 100.00%	TR: 100.00%	TR: 60.53%
Sujeto 7	TR: 93.33%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 28.95%	TR: 100.00%	TR: 64.10%
Sujeto 8	TR: 80.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 72.22%	TR: 96.77%
Sujeto 9	TR: 66.67%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 94.74%	TR: 90.32%	TA: 86.84%
Promedio	TSR: 62.86%	TSR: 75.39%	TSR: 99.26%	TSR: 79.89%	TSR: 73.42%	TSR: 98.63%	TSR: 91.52%	TSR: 92.98%	TSR: 75.73%

Anexo 26 (Tabla 2.19). Efectividades combinando características i.e., $\sigma(\vec{x})$, $iqr(\vec{x})$, $MAD(\vec{x})$ y $katz(\vec{x})$. Entrenamiento con δ_2 y acceso con δ_3. Se resaltan efectividades bajas i.e., < 80.00. El TSR promedio es de 83.30%

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 24.14%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 2	TR: 100.00%	TA: 96.97%	TR: 100.00%	TR: 100.00%	TR: 93.94%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 3	TR: 100.00%	TR: 100.00%	TA: 83.33%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 38.71%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 5	TR: 100.00%	TR: 59.46%	TR: 100.00%	TR: 100.00%	TA: 94.87%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 94.29%
Sujeto 6	TR: 100.00%	TR: 67.57%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 0.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 7	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 54.29%	TR: 100.00%	TR: 6.06%
Sujeto 8	TR: 70.83%	TR: 100.00%	TR: 100.00%	TR: 50.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 45.83%	TR: 91.67%
Sujeto 9	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 77.78%
Promedio	TSR: 88.33%	TSR: 91.56%	TSR: 98.15%	TSR: 87.63%	TSR: 98.76%	TSR: 88.89%	TSR: 94.92%	TSR: 93.98%	TSR: 85.53%

Anexo 27 (Tabla 2.21). Efectividades entrenando con δ_1, δ_2 y accediendo con δ_3. Se resaltan las efectividades bajas i.e., < 80.00. El TSR promedio es de 91.97%

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 0.00%	TR: 90.91%	TR: 100.00%	TR: 100.00%	TR: 77.27%	TR: 100.00%	TR: 100.00%	TR: 95.45%	TR: 90.91%
Sujeto 2	TR: 100.00%	TA: 55.56%	TR: 100.00%	TR: 100.00%	TR: 92.59%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 3	TR: 100.00%	TR: 100.00%	TA: 42.86%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 58.33%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 5	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 38.89%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 6	TR: 100.00%	TR: 85.00%	TR: 100.00%	TR: 100.00%	TR: 90.00%	TA: 45.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 7	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 38.46%	TR: 100.00%	TR: 100.00%
Sujeto 8	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 66.67%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 90.48%	TR: 95.24%
Sujeto 9	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 0.00%
Promedio	TSR: 88.89%	TSR: 92.39%	TSR: 93.65%	TSR: 91.67%	TSR: 88.75%	TSR: 93.89%	TSR: 93.16%	TSR: 98.44%	TSR: 87.35%

Anexo 28 (Tabla 2.22). Efectividades entrenando con δ_1, δ_3 y accediendo con δ_2. Se resaltan las efectividades bajas i.e., < 80.00. El TSR promedio es de 92.02%

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 75.00%	TR: 95.83%	TR: 100.00%	TR: 87.50%	TR: 66.67%	TR: 100.00%	TR: 100.00%	TR: 79.83%	TR: 18.18%
Sujeto 2	TR: 100.00%	TA: 23.08%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 3	TR: 100.00%	TR: 100.00%	TA: 21.05%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 12.12%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 5	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 48.39%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 6	TR: 100.00%	TR: 87.50%	TR: 100.00%	TR: 100.00%	TR: 81.25%	TA: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 7	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 80.77%	TR: 100.00%	TR: 100.00%
Sujeto 8	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 30.00%	TR: 100.00%
Sujeto 9	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 11.76%
Promedio	TSR: 97.22%	TSR: 89.60%	TSR: 91.23%	TSR: 88.85%	TSR: 88.48%	TSR: 100.0%	TSR: 97.86%	TSR: 89.98%	TSR: 81.10%

Anexo 29 (Tabla 2.23). Efectividades entrenando con δ_2, δ_3 y accediendo con δ_1. Se resaltan las efectividades bajas i.e., < 80.00. El TSR promedio es de 91.59%

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 30.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 2	TR: 93.33%	TA: 97.56%	TR: 100.00%	TR: 100.00%	TR: 53.66%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 94.74%
Sujeto 3	TR: 10.00%	TR: 100.00%	TA: 91.43%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 10.00%	TR: 100.00%	TR: 100.00%	TA: 66.70%	TR: 89.74%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 5	TR: 100.00%	TR: 26.83%	TR: 100.00%	TR: 97.44%	TA: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 86.84%
Sujeto 6	TR: 100.00%	TR: 58.54%	TR: 100.00%	TR: 100.00%	TR: 97.56%	TA: 2.44%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 7	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 97.37%	TR: 100.00%	TR: 100.00%	TA: 57.89%	TR: 100.00%	TR: 7.89%
Sujeto 8	TR: 50.00%	TR: 100.00%	TR: 100.00%	TR: 25.81%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 58.06%	TR: 93.55%
Sujeto 9	TR: 93.33%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 97.37%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 94.74%
Promedio	TSR: 85.18%	TSR: 86.99%	TSR: 99.05%	TSR: 87.48%	TSR: 93.15%	TSR: 89.16%	TSR: 95.32%	TSR: 95.34%	TSR: 86.42%

Anexo 30 (Tabla 2.24). Efectividades al suprimir la dimensión fractal como característica. Entrenamiento con δ_1, δ_2 y acceso con δ_3. Se resaltan efectividades bajas < 80.00. El TSR promedio es 90.90%

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 19.23%	TR: 73.08%	TR: 100.00%	TR: 65.38%	TR: 46.15%	TR: 100.00%	TR: 100.00%	TR: 90.91%	TR: 73.08%
Sujeto 2	TR: 100.00%	TA: 78.57%	TR: 100.00%	TR: 100.00%	TR: 82.14%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 3	TR: 100.00%	TR: 100.00%	TA: 44.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 84.09%	TR: 95.12%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 5	TR: 100.00%	TR: 89.29%	TR: 100.00%	TR: 100.00%	TA: 65.85%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 6	TR: 100.00%	TR: 86.36%	TR: 100.00%	TR: 100.00%	TR: 90.91%	TA: 59.09%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 7	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 97.06%	TR: 100.00%	TR: 100.00%	TA: 41.18%	TR: 100.00%	TR: 92.31%
Sujeto 8	TR: 95.45%	TR: 100.00%	TR: 100.00%	TR: 36.36%	TR: 86.36%	TR: 100.00%	TR: 100.00%	TA: 86.36%	TR: 68.18%
Sujeto 9	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 96.15%	TR: 100.00%	TA: 0.00%
Promedio	TSR: 90.52%	TSR: 91.92%	TSR: 93.78%	TSR: 86.99%	TSR: 85.17%	TSR: 95.45%	TSR: 93.04%	TSR: 97.47%	TSR: 81.51%

Anexo 31 (Tabla 2.25). Efectividades al suprimir la dimensión fractal como característica. Entrenamiento con δ_1, δ_3 y acceso con δ_2. Se resaltan efectividades bajas < 80.00. El TSR promedio es 90.65%

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sujeto 6	Sujeto 7	Sujeto 8	Sujeto 9
Sujeto 1	TA: 88.64%	TR: 76.92%	TR: 100.00%	TR: 53.85%	TR: 53.85%	TR: 100.00%	TR: 92.31%	TR: 34.62%	TR: 13.64%
Sujeto 2	TR: 100.00%	TA: 43.33%	TR: 100.00%	TR: 100.00%	TR: 83.33%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 3	TR: 100.00%	TR: 100.00%	TA: 31.82%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 4	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 54.05%	TR: 91.18%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 5	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 79.41%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 6	TR: 100.00%	TR: 75.00%	TR: 100.00%	TR: 100.00%	TR: 81.25%	TA: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 7	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 82.76%	TR: 100.00%	TR: 100.00%
Sujeto 8	TR: 91.67%	TR: 100.00%	TR: 100.00%	TR: 94.12%	TR: 100.00%	TR: 100.00%	TR: 93.10%	TA: 58.82%	TR: 81.82%
Sujeto 9	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%	TR: 95.45%	TR: 100.00%	TA: 31.82%
Promedio	TSR: 97.81%	TSR: 88.36%	TSR: 92.42%	TSR: 89.11%	TSR: 87.67%	TSR: 100.0%	TSR:95.96%	TSR: 88.16%	TSR: 80.81%

Anexo 32 (Tabla 2.26). Efectividades al suprimir la dimensión fractal como característica. Entrenamiento con δ_2, δ_3 y acceso con δ_1. Se resaltan las efectividades bajas i.e., ≤ 80.00. El TSR promedio es de 91.15%

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4
Sujeto 1	TA: 96.43%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 2	TR: 100.00%	TA: 94.74%	TR: 100.00%	TR: 100.00%
Sujeto 3	TR: 100.00%	TR: 100.00%	TA: 100.00%	TR: 100.00%
Sujeto 4	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 0.00%
Promedio	TSR: 99.11%	TSR: 98.69%	TSR: 100.0%	TSR: 75.00%

Anexo 33 (Tabla 2.27). Efectividades al aplicar el modelo en un nuevo *dataset* de 4 sujetos. Entrenamiento con δ_1, δ_2 y acceso con δ_1. Se evita el uso de experimentos de entrenamiento en la autenticación. Se resaltan las efectividades bajas i.e., ≤ 80.00. El TSR promedio es de 93.20%

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4
Sujeto 1	TA: 80.00%	TR: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 2	TR: 100.00%	TA: 100.00%	TR: 100.00%	TR: 100.00%
Sujeto 3	TR: 100.00%	TR: 100.00%	TA: 100.00%	TR: 100.00%
Sujeto 4	TR: 100.00%	TR: 100.00%	TR: 100.00%	TA: 100.00%
Promedio	TSR: 95.00%	TSR: 100.0%	TSR: 100.0%	TSR: 100.0%

Anexo 34 (Tabla 2.28). Efectividades al aplicar el modelo en un nuevo *dataset* de 4 sujetos. Entrenamiento con δ_1, δ_2 y acceso con δ_2. Se evita el uso de experimentos de entrenamiento en la autenticación. El TSR promedio es de 98.75%

Anexo 34 y 35 (Figuras 10 y 11). Visualización de las GUI programadas en *ViewPrincipal* y *ViewIniciado.* La primera de ellas i.e., *ViewPrincipal* proporciona un selector que permite indicar el usuario que se pretende autenticar, así como la metodología a utilizar e.g., por contraseña, empleando un archivo de MATLAB con la señal electroencefalográfica o bien mediante un escaneo EEG en tiempo real. Como se mencionó, estas opciones se han proporcionado temporalmente por cuestiones de evaluación. El segundo gráfico i.e., *ViewIniciado* muestra a la pantalla desplegada al usuario tras un inicio de sesión exitoso. En éste, se permite la alteración de ciertos parámetros de la cuenta e.g., el nivel de seguridad o bien su eliminación Adicionalmente, esta pantalla permite visualizar información estadística sobre los experimentos de un usuario e.g., el número de muestras disponibles.

Anexo 36 (Figura 12). Visualización de la GUI programada en *ViewCrearUsuario*. Esta, permite la recopilación de datos de un usuario e.g., su nombre y contraseña, nivel de seguridad preferido, imagen y datos de autenticación. Como es posible observar, para esto último, la GUI brinda dos opciones: "Registrar EEG" y "Grabación MAT". La primera se encarga de efectuar una invocación al recopilador, mientras que, el segundo, inicia un selector de archivo del sistema operativo que permite seleccionar los datos de entrenamiento

Anexo 37 (Figura 13). Visualización de la GUI programada en *ViewRecopilador*. Esta, presenta una actividad mental al usuario, que deberá ser realizada mientras Lector.py recopila los datos EEG.

Anexo 38. Distribución del código fabricado

El sistema de autenticación desarrollado en esta tesis se encuentra disponible en el siguiente repositorio: https://github.com/diegofariasc/Sistema-autenticacion-BCI