Seguridad en las interfaces cerebro-ordenador: Estado del arte, oportunidades y retos futuros

SERGIO LÓPEZ BERNAL, Universidad de Murcia, Departamento de Ingeniería de la Información y las Comunicaciones
ALBERTO HUERTAS CELDRÁN, Instituto Tecnológico de Waterford, Software de Telecomunicación y Sistemas y Grupo de Sistemas de Comunicación CSG, Departamento de Informática IfI, Universidad de Zúrich UZH
GREGORIO MARTÍNEZ PÉREZ, Universidad de Murcia, Departamento de Ingeniería de la Información y las Comunicaciones
MICHAEL TAYNNAN BARROS, Universidad de Essex, Facultad de Informática e Ingeniería Electrónica y Universidad de Tampere, CBIG/BioMediTech en la Facultad de Medicina y Tecnología Sanitaria SASITHARAN BALASUBRAMANIAM, Instituto Tecnológico de Waterford, Grupo de Software y Sistemas de Telecomunicación y Universidad RCSI de Medicina y Ciencias de la Salud, FutureNeuro, Centro de Investigación de Enfermedades Neurológicas Crónicas y Raras del SFI

Las interfaces cerebro-ordenador (BCI) han mejorado notablemente la calidad de vida de los pacientes al devolverles las capacidades auditivas, visuales y motrices dañadas. Tras la evolución de sus escenarios de aplicación, la tendencia actual de las BCI es permitir nuevos paradigmas innovadores de comunicación cerebro-cerebro y cerebro-internet. Este avance tecnológico genera oportunidades para los atacantes, ya que la información personal y la integridad física de los usuarios podrían correr un tremendo riesgo. Este trabajo presenta las versiones existentes del ciclo de vida de la ICB y las homogeneiza en un nuevo enfoque que supera las limitaciones actuales. Después, ofrecemos una caracterización cualitativa de los ataques a la seguridad que afectan a cada fase del ciclo de la ICB para analizar sus impactos y las contramedidas documentadas en la literatura. Por último, reflexionamos sobre las lecciones aprendidas, destacando las tendencias de investigación y los retos futuros en materia de seguridad de las ICB.

Este trabajo ha sido apoyado por el Irish Research Council bajo la beca postdoctoral del gobierno de Irlanda (Grant No. GOIPD/2018/466), por la Science Foundation Ireland (SFI) bajo Grant No. 16/RC/3948 y cofinanciado bajo el Euro- pean Regional Development Fund y por FutureNeuro industry partners, por el Programa de Investigación e Innovación Horizonte 2020 de la Unión Europea a través del Marie Skłodowska-Curie bajo Grant Agreement No. 839553, por Armasuisse S+T con el proyecto CYD-C-2020003, por la Universidad de Zürich UZH, y por el Programa de Investigación e Innovación Horizonte 2020 de la Unión Europea bajo el acuerdo de subvención nº 830927, concretamente el Proyecto Concordia H2020.
Direcciones de los autores: S. L. Bernal y G. M. Perez, Universidad de Murcia, Departamento de Ingeniería de la Información y las Comunicaciones, Murcia, España; emails: {slopez, gregorio}@um.es; A. H. Celdrán, Waterford Institute of Technol- ogy, Telecommunication Software and Systems Group, Waterford, Ireland and Communication Systems Group CSG, De- partment of Informatics IfI, University of Zurich UZH, CH 8050 Zürich, Switzerland; email: ahuertas@tssg.org; M. T. Barros, Universidad de Essex, Escuela de Informática e Ingeniería Electrónica, Essex, Reino Unido, Universidad de Tampere, CBIG/BioMediTech en la Facultad de Medicina y Tecnología Sanitaria, Tampere, Finlandia; correo electrónico: michael.barros@tuni.fi;
S. Balasubramaniam, Waterford Institute of Technology, Telecommunication Software and Systems Group, Waterford, Irlanda, RCSI University of Medicine and Health Sciences, FutureNeuro, the SFI Research Centre for Chronic and Rare Neu- rological Diseases, Dublín, Irlanda; correo electrónico: sasib@tssg.org.

0300/2020/12-ART11 $15.00
https://doi.org/10.1145/3427376

Conceptos CCS: - **Seguridad y privacidad→ Arquitecturas de seguridad y privacidad específicas de cada dominio**; Palabras y frases clave adicionales: Interfaces cerebro-ordenador, BCI, ciberseguridad, privacidad, seguridad **Formato de referencia ACM:**
Sergio López Bernal, Alberto Huertas Celdrán, Gregorio Martínez Pérez, Michael Taynnan Barros y Sasitharan Balasubramaniam. 2020. Seguridad en las interfaces cerebro-ordenador: Estado del arte, oportunidades y retos futuros. *ACM Comput. Surv.* 54, 1, Artículo 11 (diciembre de 2020), 35 páginas. https://doi.org/10.1145/3427376

1 INTRODUCCIÓN

Las interfaces cerebro-ordenador (BCI) surgieron en los años setenta con la intención de adquirir y procesar la actividad cerebral de los usuarios para realizar posteriormente acciones específicas sobre máquinas o dispositivos externos [87]. Tras varias décadas de investigación, esta funcionalidad se ha ampliado al permitir no sólo el registro de la actividad neuronal, sino también la estimulación [167]. La Figura 1 describe una simplificación de los componentes y procesos generales que definen un ciclo BCI común encargado de registrar y estimular neuronas [1, 26, 59], presentado posteriormente en la Sección 2. Es importante señalar que estas fases no son estándar, por lo que incluimos las más comunes utilizadas en la literatura. El sentido de las agujas del reloj, indicado en azul, muestra el proceso de adquisición de datos neuronales, y el sentido contrario representa el de estimulación, que se resalta en rojo. En cuanto a la adquisición de datos neuronales, las neuronas interactúan entre sí, produciendo actividad neuronal, ya sea basada en acciones previamente acordadas, como controlar un joystick, o generada espontáneamente (fase 1 de la Figura 1). Esta actividad es adquirida por la BCI y transformada en datos digitales (fase 2). A continuación, el sistema de procesamiento de datos de la BCI analiza los datos para deducir la acción que pretende realizar el usuario (fase 3). Por último, las aplicaciones ejecutan la acción prevista, permitiendo el control de dispositivos externos. Estas aplicaciones pueden presentar retroalimentación operativa a los usuarios, lo que permite la generación de nueva actividad neuronal. Sin embargo, el sentido antihorario de la Figura 1 comienza en la fase 4, en la que las aplicaciones definen las acciones de estimulación que se pretende realizar. La fase 3 procesa esta acción para determinar un patrón de disparo que contenga todos los parámetros esenciales que necesita la BCI para estimular el cerebro. Por último, el patrón de disparo se envía al BCI, que se encarga de estimular neuronas específicas pertenecientes a una o varias regiones cerebrales y depende de la tecnología utilizada. En pocas palabras, una BCI puede ser un sistema de comunicación unidireccional o bidireccional entre el cerebro y dispositivos computacionales externos. Las comunicaciones unidireccionales se dan cuando adquieren datos o estimulan neuronas, mientras que las bidireccionales se dan cuando realizan ambas tareas [139].

Desde el punto de vista de la seguridad, las BCI se encuentran en una fase temprana e inmadura. La literatura no ha considerado la seguridad como un aspecto crítico de las BCI hasta hace pocos años, cuando han surgido términos como neuroseguridad, neuroprivacidad, neuroconfidencialidad, piratería cerebral o neuroética [31, 58, 59]. Los trabajos existentes en la literatura han detectado ataques de seguridad específicos que afectan a la integridad, confidencialidad, disponibilidad y seguridad de las ICB, pero no realizan un análisis exhaustivo y pasan por alto problemas relevantes [17, 87, 96, 163, 165]. Más concretamente, el uso de ICB de neuroestimulación en entornos clínicos introduce graves vulnerabilidades que pueden tener un impacto significativo en el estado de salud del usuario [136]. Las BCI ya existentes en el mercado se beneficiarían de la implementación de soluciones de seguridad ro- bustas, reduciendo su impacto, especialmente en entornos clínicos. Además, la expansión de las BCI a nuevos mercados, por ejemplo, los videojuegos o el entretenimiento, genera riesgos considerables en términos de confidencialidad de los datos [87, 96, 163, 165]. En este , la información personal de los usuarios, como pensamientos, emociones, orientación sexual o creencias religiosas, está amenazada si no se adoptan medidas de seguridad [59, 96, 165]. Además, los enfoques contemporáneos de la BCI, como el uso de interfaces basadas en silicio, introducen nuevos retos de seguridad debido al aumento del volumen de datos adquiridos y al uso de tecnología potencialmente vulnerable [121]. La revolución tecnológica

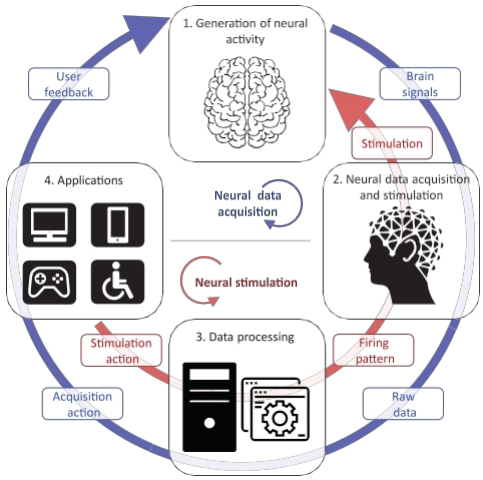

Fig. 1. Funcionamiento general de una ICB bidireccional. El flujo en sentido horario indicado con una flecha azul representa el proceso de adquisición de datos neuronales, mientras que el flujo en sentido antihorario representado con una flecha roja modela la estimulación cerebral.

de los últimos , combinada con movimientos como el Internet de las Cosas (IoT), trae consigo una aceleración en la creación de nuevos dispositivos carentes de estándares de seguridad y soluciones basadas en los conceptos de *security-by-design* y *privacy-by-design* [17, 60, 137, 163, 165]. Esta revolución también trae a la realidad escenarios prospectivos y disruptivos, donde destacamos como ejemplos las comunicaciones directas entre cerebros, conocidas como Brain-to-Brain (BtB) o Brainets [67, 126, 127, 184], y cerebros conectados a Internet (Brain-to-Internet (BtI)), que requerirán importantes esfuerzos desde el prisma de la seguridad.

Una vez resumido el funcionamiento de las BCI y su estado de seguridad, el objetivo de este artículo es analizar los problemas de seguridad de los componentes de software que intervienen en los procesos, las fases de trabajo y las comunicaciones de las BCI. Además, este trabajo considera los problemas de seguridad de las infraestructuras, como ordenadores, smartphones y plataformas en la nube, en las que se despliegan diferentes arquitecturas de BCI. También es importante señalar que, a pesar de que este artículo indica los impactos globales sobre el cerebro y la seguridad física del usuario, el enfoque principal de este trabajo es realizar un análisis de seguridad desde un punto de vista tecnológico. En línea con estos aspectos, y hasta donde sabemos, este artículo es el primer trabajo que revisa y analiza exhaustivamente el campo de la BCI desde el punto de vista de la seguridad. Dado que estos aspectos no han sido estudiados en profundidad con anterioridad y que las tecnologías BCI son todavía inmaduras, esta línea de trabajo tiene un especial interés a medio y largo plazo. Sin embargo, esta área de conocimiento es relevante en la actualidad, ya que es necesario proteger los dispositivos ya disponibles en el mercado contra los ataques.

En este contexto, la Sección 2 se centra en el análisis de los problemas de seguridad relacionados con el diseño del ciclo de vida de la ICB. Unificamos los heterogéneos ciclos de vida BCI existentes en un enfoque novedoso y común que integra los procesos de grabación y estimulación. Una vez propuesto el nuevo enfoque de diseño del ciclo de vida, revisamos los ataques aplicables a cada fase del ciclo, el impacto generado por los ataques y las contramedidas para mitigarlos, tanto documentadas en la literatura como detectadas por nosotros. Tras destacar los problemas de seguridad relacionados con el diseño de la ICB, la Sección 3 revisa los ciberataques, impactos y contramedidas actuales que afectan a los escenarios de despliegue de la ICB. Esta sección identifica los problemas de seguridad generados por los dispositivos que implementan las responsabilidades de cada fase del ciclo de vida, así como los mecanismos de comunicación y los escenarios de aplicación. La última contribución principal de este artículo es la Sección 4, donde damos nuestra visión respecto a la tendencia

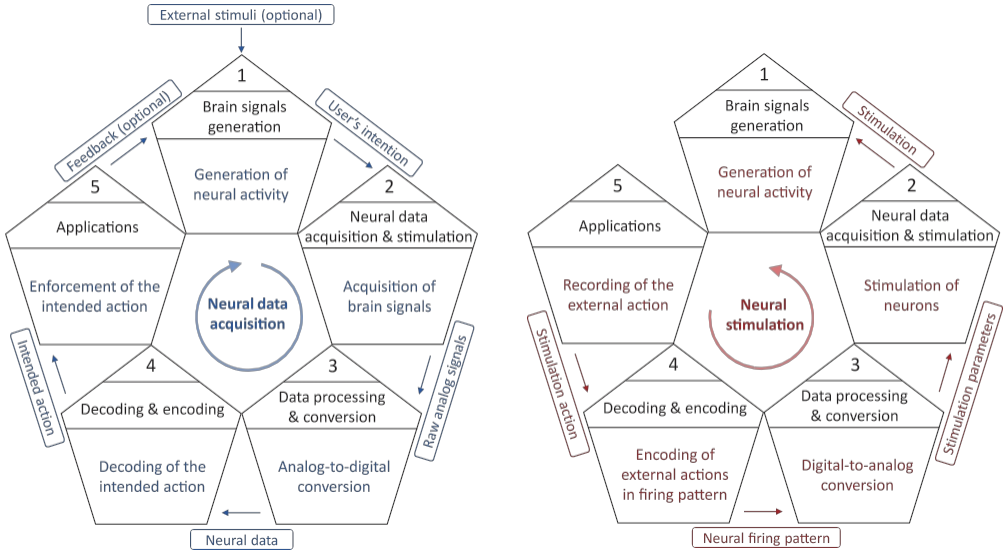

Fig. 2. Ciclo de funcionamiento bidireccional de la BCI que representa, en negro, las fases comunes para la adquisición de datos neuronales y la estimulación cerebral. (Izquierda) Representación, en azul, de los procesos realizados y los datos transferidos por cada fase del proceso de adquisición de datos neuronales. Este ciclo puede considerarse un proceso de bucle cerrado, ya que comienza y termina en la misma fase. (Lado derecho) Representación, en rojo, de los procesos y transiciones de cada fase que componen el proceso estimulación.

de la ICB y los retos de seguridad que esta evolución generará en el futuro. Por último, la sección 5 presenta algunas conclusiones y trabajos futuros.

2 CIBERATAQUES QUE AFECTAN AL CICLO BCI, IMPACTOS, Y CONTRAMEDIDAS

Esta sección revisa las diferentes fases operativas de las ICB detectadas en la literatura, conocidas como el ciclo de las ICB, y las homogeneiza en un nuevo enfoque que se muestra en la Figura 2. A continuación, analizamos los ataques a la seguridad que afectan a cada fase del ciclo, sus repercusiones y las contramedidas documentadas en la bibliografía. También presentamos oportunidades inexploradas en términos de ciberataques y contramedidas que afectan a cada fase.

La literatura ha propuesto diferentes configuraciones del ciclo BCI. Sin embargo, las versiones existentes sólo consideran el proceso de adquisición de señales, omitiendo la estimulación de las neuronas. Estas soluciones presentan varias clasificaciones del ciclo BCI, ya que algunas no consideran la generación señales cerebrales como una fase, o agrupan varias fases en una sola, sin proporcionar información sobre sus roles [26, 59]. Otras soluciones, como las propuestas en las referencias [6, 59, 87, 172], son confusas debido a que definen como nuevas fases, las transiciones y los datos intercambiados entre las diferentes etapas. En cuanto a las aplicaciones, algunos autores definen una etapa genérica de aplicaciones [1, 26, 87, 148], mientras que otros tratan el concepto de *comandos* enviados a dispositivos externos [10, 17, 18, 25, 54, 163, 171]. Además, unos pocos
trabajos definen la retroalimentación enviada por las aplicaciones a los usuarios [10, 17, 18, 25, 59, 87, 163, 171, 172]. Para homogeneizar el ciclo BCI y abordar los puntos que antes faltaban o eran confusos, presentamos una nueva versión del ciclo BCI con cinco fases (con tareas, entradas y salidas claramente definidas) que consideran tanto las capacidades de adquisición como las de estimulación. La figura 2 representa nuestra propuesta, en la que la dirección de las agujas del reloj corresponde al proceso de adquisición de la señal cerebral. La información y las tareas relativas a este funcionamiento se indican en azul. En cambio, el proceso de estimulación se indica

en el sentido contrario a las agujas del reloj, a partir de la fase 5, y, en cada fase, la información y las tareas se identifican en rojo.

Según el proceso de adquisición neuronal (sentido horario en la Figura 2), la fase 1 se centra en la generación de señales cerebrales. Los datos generados contienen la intención del usuario de realizar determinadas tareas; por ejemplo, controlar un dispositivo externo. Esta fase puede verse influida por estímulos externos, produciendo modificaciones en la actividad neuronal habitual. En la fase 2, las ondas cerebrales son captadas por electrodos utilizando una amplia variedad de tecnologías, como la electroencefalografía (EEG) o la resonancia magnética funcional (fMRI). A continuación, las señales analógicas en bruto que contienen la intención del usuario se transmiten a la fase 3, en la que es necesario procesar y convertir los datos. En concreto, esta fase lleva a cabo un procedimiento de conversión analógico-digital para permitir el procesamiento posterior de los datos. Uno de los principales objetivos de esta fase es maximizar la relación señal-ruido (SNR), que compara el nivel de la señal objetivo con el nivel de ruido de fondo para obtener la señal original con la precisión posible. La fase 4 procesa los datos neuronales digitales para descodificar la acción prevista del usuario, donde se calculan y seleccionan las características relevantes a partir de los datos neuronales. , distintos modelos (por ejemplo, clasificadores, predictores, regresores) o sistemas basados en reglas determinan la acción prevista [25, 148]. Finalmente, la acción llega a las aplicaciones en la fase 5, que la ejecutan. Las aplicaciones también pueden enviar feedback opcional al usuario para generar señales cerebrales y, por tanto, nuevas iteraciones del ciclo. En cuanto al proceso de estimulación (sentido antihorario en la Figura 2), el bucle comienza en la fase 5, donde se especifica la acción de estimulación de forma general (por ejemplo, estimular una región cerebral concreta para tratar la enfermedad de Alzheimer). Esta acción prevista se transmite a la fase 4, donde esta entrada se procesa mediante diferentes técnicas, como el aprendizaje automático (Machine Learning, ML), para generar un patrón de disparo que contiene información de alto nivel sobre los dispositivos de estimulación que se van a activar, las frecuencias utilizadas y la planificación temporal. La Fase 3 pretende transformar el patrón de disparo recibido, indicado de general, en parámetros específicos relacionados con la tecnología BCI utilizada. Por ejemplo, la identificación de las neuronas a estimular o la potencia y el voltaje necesarios para el proceso. La fase 2 transmite estos parámetros de estimulación al sistema de estimulación, que se encarga de la estimulación física del cerebro. Tras este , el cerebro genera actividad neuronal como respuesta, que también puede ser adquirida por el BCI para medir el estado del cerebro tras cada proceso de estimulación. En este , se produce una alternancia entre la estimulación cerebral y la adquisición de señales es posible, pasando de una de la figura 2 a la otra.

Antes de revisar los ataques, impactos y contramedidas de cada fase del ciclo de la ICM, es esencial definir con precisión el concepto de *seguridad*, que se refiere a la "protección de la información y los sistemas de información frente al acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados para proporcionar integridad, confidencialidad y disponibilidad" [149]. Los conceptos de integridad, confidencialidad y disponibilidad, junto con el concepto de *seguridad*, se utilizan en esta sección como métricas para evaluar el impacto de los ataques de seguridad contra los sistemas BCI. Las definiciones estándar de estos conceptos son las siguientes:

- **Integridad:** "Protección contra la modificación o destrucción no autorizada de la información. Estado en el que la información ha permanecido inalterada desde el momento en que fue producida por una fuente, durante su transmisión, almacenamiento y eventual recepción por el destino" [76].
- **Confidencialidad:** "preservación de las restricciones autorizadas de acceso y divulgación, incluidos los medios para proteger la intimidad personal y la información privada" [149].
- **Disponibilidad:** "propiedad de que los datos o la información sean accesibles y utilizables a petición de una persona autorizada" [149].
- **Seguridad:** "ausencia de condiciones que puedan causar la muerte, lesiones, enfermedades profesionales, daños o pérdidas de equipos o bienes, o daños al medio ambiente" [143]. Este trabajo considera el concepto de seguridad desde las perspectivas fisiológica, psiquiátrica y psicológica.

Tabla 1. Definición de los ANacks detectados para el ciclo BCI

Ataque	Descripción
Ataques adversarios [38, 90]	Presentación de entradas creadas intencionadamente a un sistema de LD para perturbar su funcionamiento y rendimiento normales.
Ataques de estímulos engañosos [40, 79, 96]	Presentación de estímulos sensoriales o motores malintencionados a los usuarios con el objetivo de generar una respuesta neuronal específica.
Ataques de desbordamiento del búfer [16, 109, 147]	Acceso a espacios de memoria fuera de límites debido a implementaciones de software inseguras. Se aprovechan de operaciones sobre búferes de memoria cuyos límites no están bien gestionados.
Ataques criptográficos [58, 59]	Explotar vulnerabilidades en los elementos que definen un sistema, como algoritmos, protocolos o herramientas. Una variedad de técnicas centradas en evadir las medidas de seguridad de los sistemas criptográficos.
Ataques al firmware [13, 173]	Extraer o modificar el firmware de un dispositivo, una pieza crítica del software que controla su hardware.
Ataques contra el agotamiento de la batería [24, 135]	Consumir la batería de un dispositivo, reduciendo su rendimiento o incluso haciéndolo permanentemente inaccesible.
Ataques de inyección [105, 134]	Presentar una entrada a un intérprete que contenga elementos particulares que puedan modificar cómo se analiza, aprovechando la falta de verificación de la entrada.
Ataques de malware [77, 154, 177]	Uso de hardware, software o firmware con el objetivo de obtener acceso a dispositivos informáticos para realizar acciones maliciosas de forma intencionada.
Ataques de ransomware [2, 37]	Cifrar los datos de los usuarios y exigir después un rescate económico para descifrarlos.
Ataques de botnets [4, 92]	Uso de botnets, redes de dispositivos infectados controlados y coordinados por un atacante, para realizar ataques particulares dirigidos a objetivos específicos.
Ataques de sniffing [5]	Obtención de información privada escuchando un canal de comunicación. Cuando los datos no están cifrados, los atacantes tienen acceso al contenido de toda la comunicación.
Ataques Man-in-the-middle [163]	Alteración de la comunicación entre dos entidades, haciendo creer a los extremos que se comunican directamente entre sí.
Ataques de repetición [77, 166]	Retransmisión de datos adquiridos previamente para realizar una acción maliciosa, como la suplantación de uno de los participantes legítimos de la comunicación.
Ataques de ingeniería social [47, 49]	Manipulación psicológica para obtener acceso a recursos restringidos. Un ejemplo son los ataques de phishing, basados en la suplantación de una entidad legítima en la comunicación digital.
Ataques de suplantación de identidad [159, 166]	Enmascarar una entidad de la comunicación, transmitiendo datos maliciosos. Los ataques de suplantación de identidad más frecuentes en las comunicaciones de red son, entre otros, la suplantación de IP y la suplantación de MAC.

Llegados a este punto, es esencial señalar que en este documento el concepto de seguridad se refiere a la preservación de la integridad física de los usuarios de BCI, sin centrarse en la conservación de los objetos o del entorno. Para comprender mejor los ataques y las contramedidas que se exponen más adelante en esta sección, la Tabla 1 ofrece una breve descripción de los ataques que afectan a la ICM, mientras que la Tabla 2 describe sus contramedidas. Para cada fase del ciclo BCI, detallamos las particularidades de estos ataques y contramedidas.

La figura 3 indica los ataques, impactos y contramedidas descritos en esta sección. Como puede verse, cada ataque está representado por un color que asocia los impactos que genera y las contramedidas para mitigarlo. Para cada impacto incluido en la figura, se incluye una versión simplificada del ciclo ICB. Las fases del ciclo marcadas en rojo indican los impactos detectados en la literatura para esa fase específica, mientras que el color azul indica nuestra contribución. Además, los ataques, impactos y contramedidas marcados con referencias han sido propuestos en la literatura, mientras que los que no tienen referencias son nuestra contribución. Es importante señalar que esta figura pone de manifiesto las limitaciones expuestas por la literatura, como puede apreciarse por el volumen de nuestras contribuciones. Para simplificar la imagen, hemos sintetizado la mayoría de los impactos sobre la seguridad en una entrada general "Causar daños físicos", describiendo detalladamente los impactos específicos sobre la salud de los usuarios a lo largo de la sección.

Tabla 2. Definición de las contramedidas detectadas para el ciclo BCI

Contramedida	Descripción
Sesiones de formación, demostraciones y juegos serios [59].	Iniciativas para concienciar a los usuarios sobre los riesgos de la tecnología.
Notificaciones a los usuarios [24]	Alerta a los usuarios en caso de que se detecte un ataque, para que participen en la defensa (por ejemplo, dejando de utilizar el dispositivo).
Antenas direccionales [186]	Antenas que irradian o reciben la energía principalmente en determinadas direcciones, con el fin de reducir las interferencias.
Análisis del medio [59]	Detección del medio de comunicación para detectar comportamientos anómalos.
Baja potencia de transmisión [170]	Reducción de la potencia de transmisión para evitar la interceptación de la comunicación por entidades maliciosas.
Salto de frecuencia y de canal [46, 186]	Modelos de comunicación inalámbrica basados en patrones de salto pseudoaleatorios previamente conocidos por emisor y receptor.
Espectro ensanchado [166, 170, 186]	Transmisión de la información en ancho de banda más amplio para evitar interferencias en el medio inalámbrico.
Mecanismos de control de acceso [24, 164, 165]	Medios para detectar e impedir el acceso no autorizado a determinados recursos.
Gestión de privilegios [110-112]	Asigne privilegios a distintos grupos de usuarios en función de sus funciones.
Listas blancas y listas negras [106]	Lista de entidades, como sistemas o usuarios, que tienen permitido o prohibido, respectivamente, realizar acciones específicas.
Mecanismos criptográficos [8]	Uso de técnicas de cifrado y descifrado para proteger la privacidad de los datos, ya que los atacantes pueden acceder a la información desprotegida y modificarla.
Privacidad diferencial [60, 90]	Mecanismo criptográfico basado en la adición de ruido a los datos con el objetivo de suprimir los aspectos sensibles, accesibles cuando se combinan con una gran cantidad de datos de un usuario.
Cifrado homomórfico [90]	Mecanismo criptográfico que permite el cálculo de operaciones matemáticas sobre datos cifrados, generando un resultado cifrado.
Cifrado funcional [164, 165]	Mecanismo criptográfico en el que disponer de una clave secreta permite conocer una función de los datos cifrados sin revelar los propios datos.
Verificación de autenticidad [8]	Garantizar que los datos a los que accedemos, o el punto final con el que nos comunicamos, es quien dice ser.
Verificación de la legitimidad [8]	Compruebe si una aplicación maliciosa ha sustituido a una legítima.
Limitación de funciones [123]	Asegúrese de que cualquier software sólo implementa la funcionalidad específica para la que fue concebido.
Actualizaciones periódicas [37]	Corrigen las vulnerabilidades detectadas e incluyen nuevas funcionalidades para reforzar las contramedidas existentes.
Lenguajes de programación robustos [110]	Elija las lenguas más adecuadas teniendo en cuenta sus puntos fuertes y débiles.
Técnicas y opciones de compilación [111]	Capacidades específicas de los compiladores para proteger los accesos fuera de límites a la memoria del dispositivo o a los registros de la CPU.
Endurecimiento de la aplicación [50]	Modificación de una aplicación para hacerla más resistente a los ataques, como la ofuscación del código de la aplicación.
Arquitecturas de aplicaciones segmentadas [147]	Aislamiento de arquitecturas y sistemas, estableciendo diferentes contenedores y grupos de seguridad para comunicarse entre sí.
Sandboxing [104]	Aísla la ejecución de diferentes programas, permitiendo su protección frente a ataques.
Antivirus [159]	Software centrado en la prevención, detección y eliminación de ataques de malware. Los antivirus modernos ofrecen protección frente a una amplia variedad de amenazas.
Visualización de malware [41]	Técnica centrada en el análisis de binarios de software de forma gráfica para detectar patrones anómalos de malware.

(Continuación)

Tabla 2. Continuación

Contramedida	Descripción
Cuarentena de dispositivos [4]	Aislamiento del software infectado o potencialmente infectado, para evitar su propagación e infección.
Planes de copia de seguridad [3]	Copia recurrente de datos almacenados en una ubicación diferente para permitir su recuperación en caso de pérdida de datos.
Destilación de defensa [90]	Creación de un segundo modelo ML basado en el original, con menos sensibilidad respecto a las perturbaciones de entrada y que ofrece resultados más suaves y generales.
Saneamiento de datos [66]	Rechazo de muestras que puedan producir un impacto negativo en el modelo, preprocesamiento y validación de todas las entradas que contengan información adversa.
Entrenamiento adversarial [44]	Inclusión de muestras adversarias en el proceso de entrenamiento para permitir el reconocimiento de ataques en el futuro.
Sistemas de supervisión [15]	Capturan y analizan el comportamiento de las entidades de un sistema y sus comunicaciones.
Detección de anomalías [24]	Detección de comportamientos extraños en los sistemas que pueden corresponder potencialmente a una situación de ataque.
Cortafuegos [159]	Sistema de ciberseguridad que sólo permite la entrada o salida de comunicaciones de red previamente autorizadas.
IDS [159]	Análisis de la actividad de la red para identificar comunicaciones potencialmente dañinas destinadas a perturbar el sistema.
Interrupción de la comunicación [73]	Detención de una comunicación activa para mitigar el impacto de un ataque si hay pruebas de su presencia.
Validación de entradas [134]	Análisis y preprocesamiento de las entradas presentadas a un sistema para suprimir posibles causas de fallo.
Aleatorización [165]	Cambio de los datos existentes de forma que no sigan un patrón determinista y eviten la fuga de privacidad.
Anonimizador BCI [17]	Anonimización de las señales cerebrales adquiridas del cerebro para compartirlas sin exponer información sensible de los usuarios.

2.1 Fase 1. Generación de señales cerebrales

2.1.1 Ataques. Teniendo en cuenta el flujo de adquisición de datos neuronales, esta primera fase se centra en los procesos cerebrales que generan la actividad neuronal, que pueden verse influidos por estímulos externos. La literatura ha detectado *ataques de estímulos engañosos* [40, 79, 96], un mecanismo para alterar la generación de señales cerebrales mediante la presentación de estímulos intencionadamente diseñados a los usuarios de BCI. Para entender estos , es importante introducir algunos conceptos. *Los potenciales relacionados con eventos (ERP)* son respuestas neurofisiológicas a un estímulo cognitivo, sensorial o motor, detectadas como un patrón de variación de voltaje [26]. Dentro de los diferentes tipos de Potenciales Relacionados con Eventos (PRE), los Potenciales Evocados (PE) se centran en los estímulos sensoriales y pueden dividirse en dos categorías, los Potenciales Evocados Visuales (PEV) y los Potenciales Evocados Auditivos (PEA), relacionados, respectivamente, con estímulos externos visuales y auditivos. En concreto, *el P300* es un Potencial Evocado Visual (PEV) que se detecta como un pico de amplitud en la señal de Electroencefalografía (EEG) unos 300 ms después de un estímulo, muy utilizado debido a su rápida respuesta [158].

Por un lado, Martinovic et al. [96] utilizaron el potencial P300 para obtener información privada de los sujetos de prueba y demostraron ataques de estímulos engañosos. Los estímulos visuales se presentaron en forma de imágenes, agrupadas de la siguiente manera: códigos PIN de cuatro dígitos, cajeros automáticos de bancos y tarjetas de crédito, el mes de nacimiento y fotos de personas. El objetivo del experimento era demostrar que los usuarios generan un pico más alto en el potencial P300 cuando se enfrentan a un estímulo conocido y, por tanto, ser capaces de extraer información privada. Los autores utilizaron los auriculares Emotiv EPOC de 14 canales [36], un dispositivo BCI EEG comercial, y demostraron que la fuga de información, medida en entropía de la información, era del 10%-20% de la información global, y podía incrementarse hasta aproximadamente el 43%. Por otro lado, Frank et al. [40] demostraron la posibilidad de realizar *engaños* subliminales

ataques de estímulos. Para realizar los experimentos, se utilizó el mismo concepto de ERP con potenciales P300. En este trabajo, los autores mostraron información oculta en el contenido visual proyectado a 29 sujetos, en forma de estímulos con una duración de 13,3 milisegundos, imperceptibles para el ojo humano. En el estudio se utilizaron dispositivos EEG de las marcas NeuroSky [118] y Emotiv [34]. Consideramos que los trabajos anteriores son relevantes para resaltar la importancia de la seguridad en BCI, y se requieren experimentos adicionales con un mayor número de usuarios.

La literatura ha documentado algunos métodos bien conocidos para presentar estímulos a los usuarios y ana- lizar sus respuestas neuronales [17, 96, 163]. Por ejemplo, para estudiar la actividad neuronal generada tras una pregunta en una prueba de detección de mentiras [79]. Aunque estos métodos no representan ataques en sí mismos, son una oportunidad para desarrollar nuevos ataques con estímulos engañosos contra las BCI, definidos como sigue:

- *Paradigma Oddball*: estímulos diana específicos, ocultos entre una secuencia de estímulos no diana comunes, generarían picos en la ERP. Por ejemplo, para diferenciar una cara conocida entre varias desconocidas.
- *Prueba de conocimiento de culpabilidad*: la respuesta generada por estímulos familiares puede diferenciarse de la generada por elementos desconocidos. Este principio se ha utilizado para la detección de mentiras.
- *Priming*: un estímulo puede generar un efecto de memoria implícito que influye posteriormente en otros estímulos.

A pesar del amplio estudio en la literatura sobre potenciales evocados auditivos (PEA), no hay trabajos específicos, hasta donde sabemos, que describan ataques sobre estímulos auditivos. Sin embargo, Fukushima et al. [42] describieron que los sonidos inaudibles de alta frecuencia podían afectar a la activi- dad cerebral. Detectamos que este escenario genera nuevas oportunidades para los atacantes, ya que la generación de estímulos auditivos inaudibles no requiere una interacción cercana con la víctima, lo que ayuda al atacante a pasar desapercibido.

En cuanto a la neuroestimulación, esta fase representa el resultado del proceso de estimulación dentro del cerebro. Basándonos en la falta de literatura que defina taxonomías de ataques sobre el cerebro, identificamos dos categorías principales de ataque durante la neuroestimulación. La primera categoría consiste en tomar el control del proceso de estimulación para causar daños en el tejido neural. Estos ataques pueden reproducir o empeorar los efectos secundarios a menudo presentes durante el tratamiento de afecciones neurológicas, como la enfermedad de Parkinson, ya sea mediante acciones de sobreestimulación o impidiendo el tratamiento. La fea- sibilidad de estos ataques es apoyada por las referencias [48, 128], quienes indicaron que los efectos adversos de la neuroestimulación están relacionados con los parámetros y patrones de la estimulación. Además, identificamos otra modalidad de ataque en esta categoría, basada en recrear condiciones neurológicas conocidas si existe un dispositivo de neuroestimulación con acceso a las regiones naturalmente afectadas por esas enfermedades. Como ejemplo, identificamos la posibilidad de recrear enfermedades neurodegenerativas, como las de Parkinson y Alzheimer, basadas en el deterioro del tejido cerebral, y ataques epilépticos. Aunque estos ataques son hoy en día sólo teóricos [11], el avance de las tecnologías BCI en prospección, como Neuralink [116], podría dar lugar a sistemas de neuroestimulación que puedan abarcar varias partes del cerebro, introduciendo así estas amenazas.

La segunda categoría de ataques se centra en inducir un efecto o percepción en el usuario. Es bien sabido que la neuroestimulación puede provocar múltiples efectos psiquiátricos y psicológicos, como variaciones del estado de ánimo, depresión, ansiedad o pensamientos suicidas, como se indica más adelante en la sección 2.1.2. Un atacante podría magnificar estos efectos con parámetros de estimulación maliciosos para aprovecharse del usuario. Por ejemplo, el ataque podría tener como objetivo reducir la inhibición del paciente para facilitar la extracción de información privada. Esta situación introduce la posibilidad de *ataques de ingeniería social* a la BCI, en los que el atacante no necesitaría técnicas sociales sofisticadas para manipular psicológicamente a sus víctimas.

Tabla 3. Resumen de los efectos secundarios más comunes durante la neuroestimulación aprobada por la FDA

Tecnología	Condición	Región del cerebro	Efectos secundarios neurológicos	Efectos secundarios psiquiátricos/psicológicos
EPC	Enfermedad de Parkinson	STN	Acinesia, calambres en la cara o en la mano, disartria, disfagia, apraxia de los párpados, trastornos de la marcha, hipersalivación, trastornos de la visión, incontinencia, dificultades de aprendizaje y de memoria, parestesia, inestabilidad postural, trastornos del habla, falta de fluidez verbal, síntomas vegetativos, debilidad [23, 30, 33, 48, 157].	Ansiedad, apatía, trastornos cognitivos, confusión, depresión, alucinaciones, estado submaníaco [23, 33, 48]
		GPI	Similar al STN [48]	Ansiedad, depresión, pensamientos suicidas [33, 48]
		VIM	Disfagia, trastornos de la motricidad fina, trastornos del habla [157].	
	Temblor esencial	VIM	Disestesia, disartria, trastornos de la marcha, parestesia, trastornos del habla [23, 33].	
	Distonía	GPI	Alteración de la marcha, paresia, alteración del habla, contracciones musculares tetánicas, déficit visual [23, 33].	Ansiedad, trastornos cognitivos, confusión, alucinaciones [23].
	Trastorno obsesivo-compulsivo	VC/VS, NAc		Depresión, condicionamiento operante, alteración del procesamiento de la recompensa, pensamientos suicidas, suicidio [102]
RNS	Epilepsia	Origen del ataque	Muerte, cambio en las convulsiones, hemorragia, infección [117].	Ansiedad, depresión, suicidio, pensamientos suicidas [117]

2.1.2 Impactos. Es importante señalar que los *ataques con estímulos engañosos* detallados para esta fase sólo se han realizado contra la confidencialidad de los datos [40, 79], con el objetivo de extraer datos sensibles de los usuarios de BCI. Sin embargo, consideramos que también pueden afectar a la integridad, disponibilidad y seguridad de la ICB. Estos estímulos pueden alterar el funcionamiento normal de esta fase, generando entradas maliciosas para las siguientes etapas que pueden derivar en interrupciones del servicio o acciones incorrectas con el objetivo de causar daños físicos a los usuarios. Específicamente, Landau et al. [79] identificaron que ataques de estímulos engañosos realizados durante un diagnóstico médico, como una prueba de epilepsia fotosensible en la que se presentan diferentes estímulos visuales, pueden derivar en un diagnóstico erróneo, afectando la seguridad de los usuarios. También identificamos como factible que los estímulos maliciosos, tanto perceptibles como subliminales, puedan afectar al estado de ánimo de los usuarios.

Desde la perspectiva de la neuroestimulación, los ataques mencionados pueden afectar a la salud de los usuarios de forma diferente según las enfermedades que padezcan previamente, repercutiendo en su seguridad física y psicológica. Los problemas relacionados con las distintas tecnologías de BCI se detallan en la Sección 2.2, indicando los im- pactos generales sobre el cerebro en esta . La Tabla 3 presenta los efectos secundarios más comunes durante determinadas terapias de neuroestimulación. Como puede observarse, la realización de un ataque durante el proceso de estimulación puede agravar o incluso generar una amplia gama de impactos negativos en los pacientes de BCI. Además, los autores de las referencias [135, 136] destacaron problemas comunes a las enfermedades neurológicas, como el daño tisular, los efectos rebote y la negación de la estimulación (que también afecta a la disponibilidad del servicio). Además, identificaron que una alteración del voltaje, la frecuencia, la anchura del pulso o el contacto del electrodo utilizado para estimular el cerebro podría modificar el volumen de tejido cerebral activado, induciendo efectos no deseados en las estructuras circundantes en función de la ubicación del electrodo y la técnica de estimulación. Pycroft et al. [135] también indicaron que un ataque a la neuroestimulación podría inducir los pensamientos y el comportamiento del paciente. En la Referencia [95], los autores destacaron que los ataques a la neuroestimulación pueden impedir que los pacientes hablen o se muevan, causar daños cerebrales o incluso poner en peligro su vida, mientras que los autores de la Referencia [79] indicaron la frustración del usuario si el resultado del proceso no es el adecuado.

Pycroft et al. [136] indicaron posibles agresiones y daños contra los pacientes de neuroestimulación. En primer lugar, detectaron que un procedimiento de sobreestimulación podría causar daños en los tejidos, independientemente del tipo de estimulación y de la afección médica. En el caso de la enfermedad de

Parkinson, un atacante podría aplicar

una estimulación de ~10Hz sobre la región del STN para producir hipocinesia o acinesia. En pacientes con temblor esencial, en los que se estimula el núcleo intermedio ventral (NIM), tanto un aumento del voltaje como una disminución de la frecuencia podrían derivar peligrosamente en un temblor exacerbado. Por último, una variación de los parámetros de estimulación durante el tratamiento del trastorno obsesivo-compulsivo podría generar alteraciones del procesamiento de la recompensa o del condicionamiento operante.

De acuerdo con lo anterior, los impactos sobre la seguridad son los más perjudiciales en esta fase, ya que presentan un riesgo de problemas físicos y psiquiátricos irreversibles. Además, aprovechando el estado psico- lógico de la víctima, podría facilitar también los ataques de ingeniería social. El atacante podría tener como objetivo reducir o inhibir los mecanismos de defensa mental del paciente, adquiriendo información sensible, lo que afectaría a la confidencialidad de los datos. Sin embargo, más preocupante sería aprovecharse del estado mental de la víctima, en el que el paciente accede inconscientemente a actos no deseados, como apostar dinero, comprar productos innecesarios, cometer un delito o participar en relaciones sexuales no consentidas.

2.1.3 Contramedidas. Centrándonos en las contramedidas para mitigar los estímulos engañosos, múltiples trabajos [24, 79, 135, 136] identificaron medidas generales para concienciar a los usuarios de BCI, como la difusión de los riesgos de estas tecnologías entre clínicos y pacientes y la educación de los usuarios en estas tecnologías. Esto es especialmente interesante, ya que los humanos suelen ser el elemento más débil de un sistema de seguridad. En concreto, Ienca et al. [59] indicaron que las sesiones de formación específicas podrían ser beneficiosas para proteger a los usuarios frente a estímulos potencialmente inseguros relacionados con los métodos de autenticación y la información bancaria. Además, la inclusión de demos y juegos serios en los dispositivos BCI comerciales puede educarles sobre los riesgos de estas tecnologías. Sin embargo, estas contramedidas sólo pueden aplicarse cuando el usuario es consciente de los estímulos. Por ello, consideramos que *los ataques por estímulos engañosos* pueden reducirse si las BCI se complementan con sistemas externos que monitoricen los estímulos presentados y den a los usuarios la posibilidad de evaluar si el contenido es apropiado. Por ejemplo, analizando si los contenidos multimedia mostrados a los usuarios, como imágenes o vídeos, han sido modificados maliciosamente [15, 175], aunque sean subliminales. Además, proponemos utilizar modelos predictivos basados en sistemas de detección de anomalías, con el objetivo de detectar un ataque en su fase inicial y desplegar mecanismos para mitigarlos.

2.2 Fase 2. Adquisición de datos neuronales y estimulación

2.2.1 Ataques. Esta segunda fase se centra en la interacción de los dispositivos BCI con el cerebro para adquirir datos neuronales o realizar su estimulación. En cuanto a la adquisición de datos, los autores de Refer- ences [79, 87] identificaron el uso de una combinación de *ataques de repetición y suplantación* en los que señales previas del usuario de BCI, señales de otros usuarios o señales sintéticas pueden suplantar las ondas cerebrales le- gítimas. Detectamos la aplicabilidad de estos ataques a los sistemas de estimulación, en los que un atacante puede forzar comportamientos de estimulación específicos basándose en acciones anteriores. Un posible resultado de este control puede ser un aumento del voltaje suministrado al cerebro del paciente [95]. Además, los autores de las referencias [59, 79] detectaron el uso de *ataques de interferencia* contra el proceso de ac- quisición de datos neuronales, transmitiendo ruido electromagnético al medio. Basándonos en Vadlamani et al. [170], también identificamos este problema en la estimulación neural, donde *los ataques de interferencia* pueden anular las señales legítimas emitidas por los electrodos de la BCI si se transmiten con suficiente potencia.

2.2.2 Impactos. En cuanto a los impactos producidos por los ataques anteriores, Li et al. [87] identificaron que *los ataques de repetición y suplantación* afectan tanto a la integridad como a la disponibilidad de los datos, pudiendo interrumpir el proceso de adquisición. Landau et al. [79] destacaron que estos ataques podrían interferir en los procedimientos de diagnóstico clínico, sustituyendo las señales cerebrales legítimas por otras maliciosas, concluyendo en diagnósticos erróneos, y produciendo la ausencia de tratamiento o uno innecesario en pacientes sanos. Identificamos que estos , aplicados al escenario de la estimulación, pueden perturbar el

proceso de estimulación o adquirir y modificar el patrón de estimulación utilizado por la BCI para estimular maliciosamente las neuronas, afectando a la integridad de los datos, la disponibilidad de datos y servicios, y la seguridad del paciente. Centrándonos en los *ataques de interferencia*, un atacante puede tener como objetivo impedir que los electrodos capten las señales cerebrales debido al ruido transmitido [59, 79], afectando a su disponibilidad y seguridad. Detectamos que los ataques de interferencia también pueden afectar a los escenarios de neuroestimulación, donde las señales con suficiente potencia pueden anular a las legítimas, afectando a la integridad y disponibilidad de los datos, así como a la seguridad del paciente durante las acciones de estimulación.

Aparte de los impactos derivados de los ataques anteriores, es importante señalar que cada tecnología BCI concreta presenta riesgos específicos en función de su invasividad y funcionamiento, por lo que el impacto generado por un ataque difiere. Para analizar esta situación, seleccionamos algunas de las tecnologías BCI más utilizadas para adquirir datos neuronales o estimular el cerebro. Para cada una de ellas, abordamos consideraciones específicas para evaluar su impacto.

En cuanto a las cuestiones relacionadas con las tecnologías de adquisición, es necesario considerar tanto su resolución temporal como espacial. Hemos observado que una baja resolución temporal en las tecnologías de adquisición plantea problemas de disponibilidad de datos y servicios, ya que los dispositivos transmiten una cantidad reducida de datos que pueden verse afectados más fácilmente por interferencias electromagnéticas y, sobre todo, por *ataques de interferencia*. Además, esta situación también puede ser beneficiosa para los *ataques de repetición y suplantación de identidad*, ya que los atacantes disponen de más tiempo para preparar y enviar datos maliciosos. Una resolución espacial elevada puede afectar a la confidencialidad de los datos, ya que permite a los atacantes acceder a datos neuronales más sensibles. Es importante señalar que los ataques a tecnologías como la Resonancia Magnética Funcional (fMRI) o la Magnetoencefalografía (MEG) pueden tener un mayor impacto económico debido al alto coste de estas tecnologías en comparación con otras como la EEG [82, 137]. No obstante, la EEG es la tecnología de adquisición más estudiada desde el punto de vista de la seguridad, debido a su amplia disponibilidad fuera de los entornos clínicos, lo que pone de manifiesto la viabilidad de ataques como *los ataques por estímulos engañosos* o *los ataques de interferencia*.

Aunque la bibliografía ha documentado algunas posibles repercusiones en la seguridad de las tecnologías de adquisición, el impacto de las tecnologías de neuroestimulación en la salud de los pacientes se ha estudiado de forma más detallada, concretamente en el campo de los dispositivos médicos implantables (IMD). Por ello, presentamos en primer lugar las tecnologías de estimulación más comunes en la actualidad para revisar posteriormente su impacto específico, abordando principalmente cuestiones de seguridad.

Centrándonos en los efectos específicos de las tecnologías de neuroestimulación, la estimulación cerebral profunda (ECP) es la más estudiada debido a su carácter invasivo, siendo Medtronic una de las marcas más populares que comercializa dispositivos de ECP de circuito abierto [128]. Los efectos secundarios de este método han sido ampliamente estudiados en la literatura, donde algunos de ellos han sido previamente presentados en la Tabla 3 para el tratamiento de condiciones particulares. Según Pycroft et al. [136], el uso de Estimulación Cerebral Profunda (ECP) con altas densidades de carga puede causar daños en los tejidos. Además, un aumento o disminución de la frecuencia de estimulación puede tener un impacto considerable en su eficacia, llegando incluso a invertir el efecto de la estimulación. Por último, durante la ECP puede producirse una alteración del procesamiento de las emociones y los afectos en forma de efectos secundarios, como el llanto patológico o la risa inapropiada, que tienen un impacto angustioso.

Pasando a la Estimulación Magnética Transcraneal (EMT), Polanía et al. [129] indicaron que los pulsos aplicados a zonas concretas podrían inducir la supresión de la percepción visual o la detención del habla, lo que sirve de oportunidad para los agresores. León et al. [84] destacaron que la Estimulación Magnética Transcraneal (EMT) podría producir efectos secundarios como dolor de cabeza y de cuello, siendo posibles pero improbables los ataques epilépticos. Los efectos secundarios de la Estimulación Eléctrica Transcraneal (EETT) suelen ser leves, como hormigueo, picor y enrojecimiento de la piel [114]. Sin embargo, esta técnica puede tener efectos indirectos en la estimulación de elementos no neuronales, como nervios periféricos, nervios craneales o retina. Por ello, la estimulación se limita a dosis máximas tolerables [89].

Además, en pacientes con depresión, la Estimulación por Corriente Directa (tDCS) puede derivar en casos de manía e hipomanía [99]. Cabe señalar que los efectos secundarios descritos anteriormente pueden surgir de forma natural en entornos controlados en los que los clínicos tienen un control estricto del procedimiento. Sin embargo, si los atacantes alteran la terapia, podrían recrear o amplificar las condiciones maliciosas, generando un claro impacto en la salud de los pacientes.

El Neuropace RNS es un sistema de neuroestimulación de bucle cerrado para el tratamiento de la epilepsia farmacorresistente, que realiza tanto procedimientos de adquisición de datos neuronales como de neuroestimulación. Presenta la ventaja de administrar la estimulación sólo cuando detecta el inicio de la actividad convulsiva, lo que reduce los efectos secundarios. Sin embargo, introduce retos potenciales que pueden ser utilizados por un atacante para afectar a la seguridad de sus usuarios [128]. En primer lugar, identificamos que el comportamiento en bucle cerrado podría inducir, tanto en los médicos como en los pacientes, una reducción de la percepción de los riesgos, asumiendo que el dispositivo funciona correctamente. Además, dado que el dispositivo presenta capacidades autónomas, un atacante podría alterar su , sin el conocimiento del usuario, para generar un impacto en la confidencialidad de los datos, la disponibilidad del servicio y la seguridad.

2.2.3 Contramedidas. En cuanto a las contramedidas para detectar y mitigar los ataques de repetición y suplantación de identidad, Landau et al. [79] propusieron, para la adquisición de datos, el uso de mecanismos de detección de anomalías para detectar entradas modificadas, así como la mejora de la precisión de los dispositivos de adquisición. Además, proponemos un mecanismo capaz de desactivar los electrodos no necesarios para el uso de la aplicación actual y evitar riesgos potenciales, como la adquisición de P300 en señales cerebrales. Esta acción podría ser realizada automáticamente por el sistema BCI o basarse en la decisión del paciente o del médico. Teniendo en cuenta la estimulación neural, y específicamente para las BCIs, se pueden utilizar dispositivos externos para au- torizar y autorizar las acciones de estimulación [24]. Los autores de las referencias [46, 170, 186] documentaron varios mecanismos de detección y contramedidas relacionados con la mitigación de ataques de interferencia. Todos los procedimientos de detección se basan en un análisis del medio para detectar comportamientos anómalos, como los identificados para la adquisición de datos neuronales por Ienca et al. [59]. En concreto, Landau et al. [79] propusieron utilizar un conjunto de clasificadores para detectar la adición de ruido a la entrada benigna. Como contramedidas propuestas, Vadlamani et al. [170] identificaron el uso de baja potencia de transmisión como posible solución para endurecer la detección de la transmisión legítima, y el uso de antenas direccionales orientadas al cerebro para evitar la interferencia. El uso de saltos de frecuencia
[186] y el salto de canal [46] tras un periodo de tiempo determinado también pretenden reducir el impacto de estos ataques. Detectamos que el uso de antenas direccionales es también una posible solución para *los ataques de replay y spoofing*. Por último, cabe destacar que la mitigación de los impactos anteriores centrados en la seguridad del usuario es consecuencia de la mitigación de los ataques detectados contra los dispositivos BCI. En el escenario de los sistemas de neuroestimulación de bucle cerrado, identificamos como esencial disponer de información sobre el comportamiento del dispositivo, tanto de los procedimientos de adquisición como de estimulación. Estos mecanismos de retroalimentación permitirían analizar externamente el estado del cerebro y las decisiones de estimulación. Otra propuesta es el uso de sistemas de detección de anomalías, incluidos en el dispositivo, para identificar parámetros de estimulación inusuales, o una ausencia de tratamiento cuando se produce una convulsión, no- tificando al usuario. Este segundo enfoque podría preservar más la energía, y la elección del
La estrategia dependería del caso de uso.

2.3 Fase 3. Tratamiento y conversión de datos

2.3.1 Ataques. En esta fase se realizan las tareas de procesamiento y conversión de datos necesarias para que los datos neuronales y las acciones de estimulación estén listos para las fases posteriores. Aunque la literatura no ha detectado problemas de seguridad en esta , de acuerdo con los aspectos indicados por Bonaci et al. en las Referencias [17, 18], identificamos como posibles ataques *de malware* contra esta fase, tomando el control sobre la BCI. Estos ataques son candidatos a afectar tanto a los procesos de adquisición como a los de estimulación,

que afectan a las tareas realizadas en esta . En concreto, identificamos que el malware puede perturbar la conversión analógico-digital que se produce durante la adquisición de datos neuronales, así como la traslación de los patrones de disparo a dispositivos de estimulación concretos. También detectamos que *los ataques de interferencia* aplicados a la fase anterior para la adquisición de datos pueden afectar a esta fase, ya que una señal de entrada distorsionada con suficiente ruido puede ser difícil de filtrar y, por tanto, propagar esta señal a las fases posteriores.

2.3.2 Impactos. En este contexto, identificamos que *los ataques de malware* tienen un impacto tanto en la adquisición de datos neuronales como en la estimulación, donde los atacantes alteran o anulan los datos recibidos de fases anteriores, generando datos maliciosos enviados a fases posteriores. Es decir, los datos analógicos registrados durante la adquisición de datos neuronales o el patrón de disparo utilizado en los procesos de neuroestimulación. Estos ataques pueden recoger los datos sensibles gestionados en esta , tanto analógicos como digitales, y enviarlos a los atacantes, afectando a la confidencialidad de los datos. Por ejemplo, información sobre pensamientos privados o tratamientos neurológicos. En cuanto a la disponibilidad de datos y servicios, tanto la adquisición como la estimulación son potencialmente vulnerables a malware que evite la transmisión de datos a fases posteriores del ciclo. El malware que afecta a la integridad y la disponibilidad también es una amenaza contra la seguridad física de los usuarios, ya que genera patrones de estimulación perjudiciales o acciones peligrosas enviadas a las aplicaciones. Además, los impactos y contramedidas descritos en la primera fase del flujo de adquisición para los ataques de interferencia también son aplicables a la fase actual.

2.3.3 Contramedidas. En cuanto a las contramedidas para mitigar los ataques que afectan a la confidencialidad de los datos, Chizeck et al. [26] definieron una solicitud de patente estadounidense titulada "Brain-Computer Interface Anonymize" que propone una tecnología capaz de procesar las señales neuronales para eliminar toda la información privada no esencial [17, 165]. Como resultado, la información sensible nunca se almacena en el dispositivo BCI ni se transmite al exterior. Identificamos este método como especialmente relevante en esta fase ya que se trata de la primera etapa tras el proceso de adquisición de la BCI. Aunque los autores no proporcionan detalles sobre técnicas o algoritmos para entender cómo se procesan las señales en bruto, indican que este proceso sólo puede realizarse en hardware o software dentro del propio dispositivo, y no en redes o plataformas informáticas externas, como forma de garantizar la privacidad de la información. Además, Ienca et al. [60] propusieron el uso de la *privacidad diferencial* para mejorar la seguridad y la transparencia del procesamiento de datos.

Las contramedidas para mitigar el malware dependen de su tipo y comportamiento. Consideramos el uso de software antivirus y Sistemas de Detección de Intrusiones (IDS) como alternativas para la de dispositivos individuales, basándonos en la Referencia [79]. Además, los autores de las Referencias [159, 177] consideran mecanismos de seguridad perimetral, como *cortafuegos*, responsables de analizar todas las comunicaciones entrantes y salientes del dispositivo. También se propone el uso de sistemas de detección de anomalías de aprendizaje automático (ML) para identificar posibles amenazas de malware [24, 141]. Por último, Chakkaravarty et al. [154] revisaron las técnicas actuales de malware persistente capaces de eludir los contramedidas habituales y propusieron técnicas de mitigación, como *el sandboxing* [104], *el endurecimiento de aplicaciones* [50] y la *visualización de malware* [41]. Es esencial destacar que las contramedidas aplicables a esta fase dependen en gran medida de las restricciones del dispositivo que la implementa, que suele ser el dispositivo BCI (véase la Sección 3).

2.4 Fase 4. Descodificación y codificación

2.4.1 Ataques. La decodificación y codificación es la fase centrada en la identificación de la acción pretendida por los usuarios en la adquisición de datos neuronales o la especificación del patrón de disparo neuronal en la neuroestimulación. Los ataques *de malware* han sido identificados en la literatura por Bonaci et al. [17, 18] desde la perspectiva de la adquisición de señales. En concreto, identificaron que los atacantes podrían utilizar *malware* para anular el funcionamiento de esta fase o para implementar algoritmos maliciosos adicionales. Además, identificamos que los ataques de malware también pueden aplicarse al flujo de estimulación, evitando o

interrumpir la generación de un patrón de disparo. Además, identificamos que *los ataques adversarios* también pueden aplicarse a esta fase tanto para tareas de adquisición como de estimulación, aprovechando los algoritmos de clasificación utilizados. Estos ataques afectan a todo tipo de modelos ML y, por ello, son actualmente un reto abierto [38]. Liu et al. [90] detectaron la posibilidad de *ataques de envenenamiento*, en los que los atacantes introducen muestras adversas manipuladas en los datos, con el objetivo de cambiar su distribución. *Los ataques de evasión* pretenden crear muestras que evadan los sistemas de detección, mientras que *los ataques de suplantación* se centran en muestras adversarias que derivan en una clasificación incorrecta de las legítimas. Por último, existen dos modelos de ataque en función del conocimiento sobre el modelo [44]. En los *ataques de caja blanca*, los adversarios conocen el modelo, mientras que en los *ataques de caja negra*, sólo tienen acceso al modelo a través de una interfaz limitada.

2.4.2 Impactos. Los ataques descritos anteriormente generan impactos particulares en la ICB. Por lado, *el malware* tiene un impacto en la integridad y disponibilidad de los datos, ya que puede alterar o ignorar los datos re- cibidos de fases anteriores, y anular la salida de la actual. Es decir, interrumpir la acción prevista enviada a las aplicaciones BCI en el proceso de adquisición, como impedir el control de una silla de ruedas o cambiar su dirección, o el patrón de disparo en la estimulación neuronal, permitiendo una amplia variedad de ataques, como se describe en la sección 2.1. Además, el *malware* afecta a la disponibilidad proceso de ML mediante la alteración del modelo entrenado o del algoritmo de ML. Desde el punto de vista de la confidencialidad de los datos, *el malware* puede acceder a las características utilizadas en la fase de entrenamiento del ML, así como recabar información sobre el modelo y el algoritmo utilizados. *El malware* también afecta a la seguridad de los usuarios, ya que los impactos anteriores sobre la integridad y la disponibilidad derivan en acciones maliciosas y patrones de disparo que afectan a la integridad de los usuarios, como causar daños neuronales o inducir determinados estados psicológicos. Por otro lado, *los ataques adversarios* también afectan a la integridad y disponibilidad de los datos, ya que la introducción de muestras maliciosas con el objetivo de perturbar el modelo puede alterar o evitar la generación de acciones y patrones de disparo. Shokri et al. [153] demostraron que los modelos ML son sensibles a *los ataques de adversarios*, con el objetivo de detectar si existe una muestra en el conjunto de datos de entrenamiento del modelo. Basándose en ello, un atacante puede extraer datos sensibles de los usuarios, como acciones previas previstas o patrones utilizados durante las acciones de estimulación. Teniendo en cuenta la confidencialidad de los datos, Landau et al. [79] detectaron que una entidad maliciosa que tomara el control del resultado de esta fase podría acceder a la intención del usuario. Por último, el uso de muestras maliciosas, como es el caso de *los ataques de envenenamiento*, alteran el sistema ML, derivando en impactos de seguridad para ambos sentidos del ciclo.

2.4.3 Contramedidas. Para mitigar los ataques a la fase de entrenamiento del ML que afectan a la integridad y disponibilidad, hemos identificado varias técnicas propuestas en la literatura para *ataques adversariales* genéricos, que pueden servir como oportunidad para mejorar la seguridad de la BCI. En primer lugar, *la higienización de datos* es útil para rechazar muestras que contengan información adversarial, perturbando así el modelo. Jagielski et al. [66] propusieron un enfoque similar contra los ataques de envenenamiento aplicados a técnicas de regresión, donde el ruido y los *valores atípicos* se suprimen del conjunto de datos de entrenamiento. Sin embargo, no impide que los atacantes elaboren muestras similares a las generadas por la distribución legítima. En este se han presentado contramedidas como el *entrenamiento adversarial* o la *destilación de defensas*. Sin embargo, ambas tienen limitaciones, ya que dependen de las muestras utilizadas durante el entrenamiento y romperse utilizando *ataques de caja negra* y ataques computacionalmente costosos basados en la op- timización iterativa [44, 90]. Goodfellow et al. [44] también propusieron *modificaciones en la arquitectura*, basadas en la mejora de los modelos ML para ser más robustos, pero esto deriva en modelos difíciles de entrenar que presentan degradación en el rendimiento cuando se utilizan en situaciones no adversariales. Liu et al. [90] documentaron la integración de técnicas para mitigar los ataques, llamado *método ensemble*. También indicaron dos métodos que pueden aplicarse tanto en la fase de entrenamiento como en la de prueba: *la privacidad diferencial* y *el cifrado homomórfico* [56, 90, 165]. Por último, cabe destacar que las contramedidas para mitigar *los ataques de malware* en la fase anterior pueden aplicarse a la actual.

2.5 Fase 5. Solicitudes

2.5.1 Ataques. Desde el contexto de la adquisición de datos, las aplicaciones ejecutan en el mundo físico las acciones pretendidas por los usuarios a través de su actividad neuronal. Estas acciones pueden ir desde la interacción con un ordenador o un smartphone hasta el control de un miembro robótico. Desde el de vista de la estimulación neuronal, las aplicaciones son el punto de entrada de la información transmitida al cerebro, como los estímulos sensoriales en prótesis o la mejora cognitiva. En esta sección, consideramos las aplicaciones, sin analizar su comunicación con sistemas externos, que se aborda en la Sección 3.1.

Teniendo en cuenta los problemas de esta fase, se han detectado en la literatura *ataques de suplantación de identidad* en BCI, en los que un atacante crea aplicaciones maliciosas idénticas a la original y las pone a disposición en tiendas de aplicaciones [8]. Los autores de las referencias [17, 18, 87] identificaron *los ataques de malware* como una amenaza en BCI. Además, Pycroft et al. [136] identificaron que el uso de dispositivos de consumo, como los smartphones, genera nuevos riesgos y problemas de seguridad. Las consideraciones específicas sobre el malware son las mismas que se detallan en las secciones 2.3 y 2.4. Además, hemos encontrado varias oportunidades relacionadas con ciberataques realizados contra aplicaciones. En particulardetectamos problemas de desconfiguración de la seguridad, ataques de desbordamiento del búfer (BO) y ataques de inyección sobre las aplicaciones. Sin embargo, el análisis detallado de estos ataques concretos queda fuera del alcance de este trabajo, y sólo abordamos aspectos generales relacionados con la ICB.

2.5.2 Impactos. Landau et al. [79] identificaron múltiples riesgos en las aplicaciones BCI con la independencia de cualquier ataque. Detectaron que un atacante podría interferir en la capacidad del usuario para utilizar el dispositivo, impactando en su disponibilidad. También detectaron problemas de confidencialidad en relación con la identificación de usuarios por sus datos neuronales, ilustrando un escenario en el que un atacante extrae datos de EEG de la aplicación y los compara con la base de datos de EEG de un , identificando al usuario y accediendo a su historial médico. Esta identificación puede derivar en una situación de discriminación basada en la pertenencia a determinados grupos, como las creencias religiosas. Además, la mayoría de las APIs de desarrollo de BCI ofrecen acceso total sobre la información y no implementan limitaciones sobre los estímulos presentados a los usuarios, generando problemas de confidencialidad [17, 40, 87, 96, 163, 165]. Por último, todos los ataques que afectan a esta fase pueden forzar a las aplicaciones a enviar estímulos o acciones maliciosas, causando daños físicos [8].

Teniendo en cuenta el impacto de los ataques anteriores, las aplicaciones creadas mediante *ataques de suplantación de identidad* afectan tanto a la integridad como a la confidencialidad de los datos, ya que pueden presentar estímulos maliciosos para obtener información neuronal sensible, como pensamientos o creencias [8]. En escenarios de neuroestimulación, identificamos que estas aplicaciones fraudulentas podrían modificar por completo los patrones de disparo utilizados para estimular al paciente, generando un alto impacto sobre la seguridad. Más concretamente, estas aplicaciones podrían inducir estados psicológicos en la víctima, haciéndola más dispuesta a apostar, o incluso generar efectos adversos como ansiedad y depresión. En base a ello, el atacante podría aprovecharse de estos estados , inyectando publicidad in-app para ganar dinero de la .

Los ataques de malware afectan a la integridad de las aplicaciones alterando sus servicios y capacidades, por ejemplo inutilizando el cifrado de la información. Además, pueden comprometer la confidencialidad de las aplicaciones, accediendo a información sensible como historiales médicos y perfiles de usuario utilizados durante los tratamientos de neuroestimulación. En cuanto a la disponibilidad de la aplicación, *los ataques de malware* pueden derivar en una denegación de servicio sobre la aplicación, afectando a procesos como el control de prótesis o sillas de ruedas.

Detectamos que *los ataques de desconfiguración* presentan problemas de integridad de datos, en los que los atacantes se aprovechan del sistema para obtener acceso no autorizado, como mecanismos de control de acceso débiles. Los problemas de confidencialidad de los datos también están presentes, por ejemplo, en los archivos de configuración que tienen contraseñas estáticas predefinidas, lo que permite a los atacantes acceder a los datos privados de los usuarios. Disponibilidad de las aplicaciones

También es posible que se produzcan problemas, ya que un problema de configuración errónea puede servir como primer paso para alterar el comportamiento normal de la aplicación BCI.

Pasando a *los ataques de inyección*, pueden producir pérdida, modificación y corrupción de datos, afectando a la integridad de las aplicaciones [105, 134]. En cuanto a la confidencialidad, pueden producir la revelación de información sensible a partes no autorizadas [105, 134], como es el caso de las compañías de seguros que seleccionar a los mejores candidatos para sus productos [8]. La disponibilidad puede verse afectada por una denegación de acceso sobre un sistema de autenticación, o produciendo acciones de crash, salida o reinicio de las aplicaciones, interrumpiendo procesos vitales como la neuroestimulación clínica [107, 134].

Los ataques de desbordamiento de búfer (BO) pueden derivar en la ejecución de código o comandos no autorizados, donde un atacante puede alterar el funcionamiento normal de la aplicación o acceder a información sensible [110]. Además, también pueden tener como objetivo eludir los mecanismos de protección mediante la ejecución de código fuera del alcance de la política de seguridad del programa. Estas acciones pueden afectar a la integridad, confidencialidad y disponibilidad de los datos de la aplicación [111].

2.5.3 Contramedidas. Es necesario verificar la legitimidad de las aplicaciones y garantizar un control suficiente de las tiendas de aplicaciones para mitigar *los ataques de suplantación* [8]. A este respecto, Landau et al.
[79] proponen el uso de aplicaciones desarrolladas por organizaciones autorizadas para garantizar su fiabilidad. En cuanto a *los ataques de malware*, las mismas contramedidas propuestas para la fase de *procesamiento y conversión de datos* se aplican también a las aplicaciones. Es decir, el uso de antivirus, cortafuegos, sistemas de detección de intrusiones (IDS) y sistemas de detección de anomalías para identificar y mitigar los ataques. Además, Takabi et al. [164, 165] propusieron el uso de mecanismos de control de acceso sobre la información para restringir su acceso y mitigar así los impactos sobre la confidencialidad. También indicaron el uso de la aleatorización y la privacidad diferencial. Además, propusieron la integración de la *encriptación homomórfica* para operar con la información encriptada combinada con *la encriptación funcional* para acceder sólo a un subconjunto de la información.

Como oportunidad para BCI, identificamos algunas acciones preventivas contra los *errores de configuración* definidas por el Open Web Application Security Project (OWASP) [123], como el uso de plataformas mínimas con sólo las características, componentes, librerías y software necesarios para reducir la probabilidad de problemas de configuración. Además, una revisión y actualización periódicas de los parámetros de configuración también son beneficiosas como parte del proceso de gestión de aplicaciones. También es necesario crear arquitecturas de aplicaciones segmentadas que ofrezcan una división entre componentes y definan diferentes grupos de seguridad, utilizando listas de control de acceso (ACL).

En cuanto *al BO*, es importante utilizar lenguajes de programación que protejan contra estos at- tacks, así como el uso de compiladores con mecanismos de detección. [147]. Los desarrolladores deben validar todas las entradas y seguir reglas de buenas prácticas al utilizar la memoria (por ejemplo, verificación de los límites de los búferes). Además, las aplicaciones sensibles deben ejecutarse con los menores privilegios posibles e incluso aislarse mediante técnicas de sandbox [110-112]. Para detectar *los ataques de inyección*, se han propuesto análisis estáticos y dinámicos del código fuente de las aplicaciones [134]. Para mitigarlos, es necesario escapar todos los caracteres especiales incluidos en la entrada [107, 134]. Se han propuesto múltiples soluciones, como el uso de listas blancas y listas negras [106], el uso de lenguajes seguros y APIs que contengan mecanismos de detección automática [105, 134], el uso de técnicas de sandboxing para definir límites estrictos entre procesos [107], la definición de diferentes permisos en el sistema [106] y mensajes de error con detalles mínimos pero descriptivos.

3 PROBLEMAS DE SEGURIDAD QUE AFECTAN A LAS IMPLANTACIONES DE BCI

Esta sección revisa las diferentes implementaciones arquitectónicas del ciclo BCI encontradas en la literatura. A continuación, las agrupamos en dos familias principales, caracterizadas por la implementación del ciclo BCI y su escenario de aplicación. A diferencia de la Sección 2, donde el análisis de seguridad

es independiente del despliegue, esta sección revisa el estado del arte de los ataques existentes que afectan a los dispositivos que implementan cada fase del ciclo BCI, así como sus impactos y contramedidas. En esta sección también se destacan las nuevas oportunidades, en términos de ataques y contramedidas, que la literatura no ha detectado. La Figura 4 representa los dos despliegues arquitectónicos definidos, BCI Locales y BCI Globales, indicando la comunicación entre sus elementos y las fases del ciclo BCI que cada elemento implementa según el tipo de despliegue.

3.1 ICB local

3.1.1 Descripción de la arquitectura. Los despliegues BCI locales destacan por la gestión de los procesos de adquisición de datos neuronales y estimulación de usuarios individuales. Esta arquitectura suele desplegar las fases BCI entre dos dispositivos físicos, tal y como se representa en la Figura 4. El primero, identificado como *dispositivo BCI*, se centra en los procedimientos de adquisición y estimulación neuronal (fases 1 y 2 del ciclo BCI). En cambio, las aplicaciones BCI (fase 5) se ejecutan en un Dispositivo de Control Cercano (NCD), un PC o teléfono inteligente que controla el dispositivo BCI mediante un enlace de comunicación por cable o inalámbrico. Las fases 3 y 4 del ciclo pueden aplicarse por igual en ambos dispositivos, donde los fabricantes toman la decisión final. En este punto, es esencial señalar que pueden surgir diseños alternativos debido a requisitos específicos de los despliegues, como la presencia de múltiples usuarios. Además, consideramos los BCI totalmente implantables dentro de esta arquitectura, ya que requieren un dispositivo externo para su con- figuración y verificación.

3.1.2 Ejemplos de implementación. Este tipo de despliegue arquitectónico es el más comúnmente implementado para BCIs de consumo, donde marcas comerciales como NeuroSky o Emotiv se centran en escenarios como el juego y el entretenimiento [1, 96, 100]. Los escenarios neuromédicos también utilizan este enfoque, en los que un Dispositivo de Control Cercano (NCD) situado en el entorno clínico gestiona los procesos de adquisición y estimulación. Esta sección aborda específicamente los problemas detectados en los dispositivos BCI físicos, los problemas inherentes al NCD y los relacionados con la comunicación entre el BCI y el NCD. En este , es importante señalar que los ataques, impactos y contramedidas detectados para el ciclo BCI también son aplicables.

3.1.3 Ataques. Centrándose en los dispositivos BCI, Ballarin et al. [8] identificaron ataques que afectaban al *firmware* de- vice lanzar un enlace de configuración (por ejemplo, puertos USB), teniendo un impacto en la integridad y confidencialidad de los datos, generando también interrupciones en el sistema. Pycroft et al. [136] identificaron la posibilidad de inyectar actualizaciones de firmware maliciosas. Además, identificamos que estos ataques pueden servir para generar problemas de seguridad. Ienca et al. [58, 59] documentaron *ataques criptográficos*, indicando que el proyecto Emokit de Cody fue capaz de crackear el cifrado de datos directamente desde el Emotiv EPOC, un BCI de consumo. Detectaron que estos ataques afectan a la integridad y confidencialidad de los datos. Marin et al. [95] detectaron que los actuales dispositivos médicos implantables IMD) carecen de mecanismos de seguridad robustos. Yaqoob et al. [178] identificaron que los dispositivos de neuroestimulación carecen de cifrado y suelen definir contraseñas por defecto, lo que afecta a la integridad y la confidencialidad, facilitando el acceso no autorizado a datos sensibles. También identificamos que producen problemas de disponibilidad y seguridad del servicio si pueden modificar los datos.

Los autores de las referencias [24, 135] destacaron que los atacantes podrían centrarse en agotar la batería del dispositivo y afectar así tanto a la disponibilidad del servicio como a la seguridad física de los usuarios. En los sistemas de neuroestimulación, perder la capacidad de la batería supondría una pérdida del tratamiento, en el que reaparecerían los síntomas de la enfermedad. Debido a esto, algunos IMD incluyen baterías recargables, reduciendo los riesgos de agotarlas, y definiendo así soluciones más robustas. También esencial tener en cuenta que, en los sistemas no recargables, es necesario intervenir quirúrgicamente para sustituir las baterías, lo que aumenta el riesgo de problemas de seguridad tanto física como psicológica.

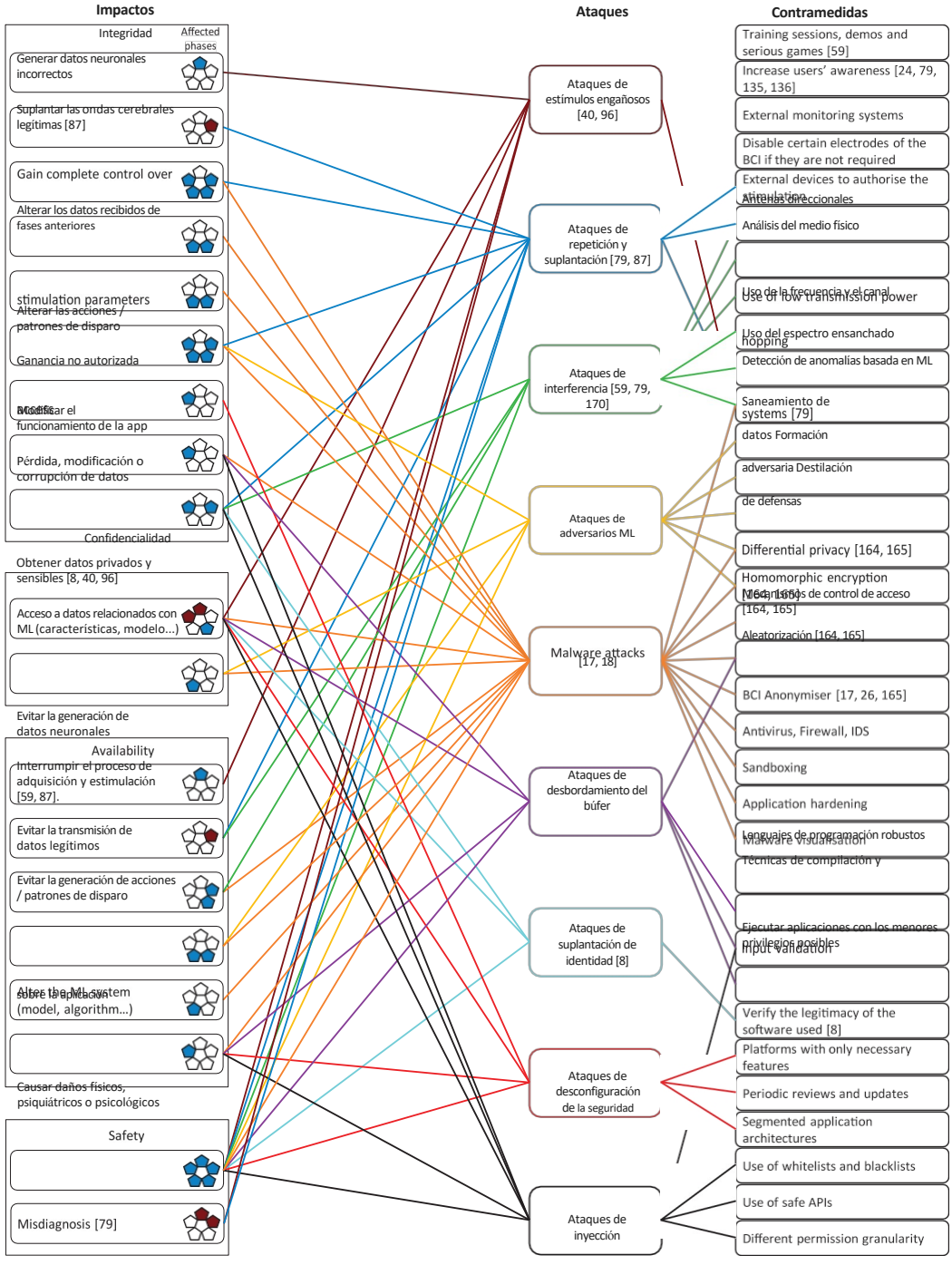

Fig. 3. Relación entre los aNacks, los impactos y las contramedidas a lo largo del ciclo BCI. Las fases del ciclo coloreadas en rojo para cada impacto representan cuestiones documentadas en la literatura, mientras que las marcadas en azul son nuestra contribución. Los aNacks, impactos y contramedidas seguidos de referencias han sido documentados en la literatura, y aquellos sin cita representan nuestra contribución.

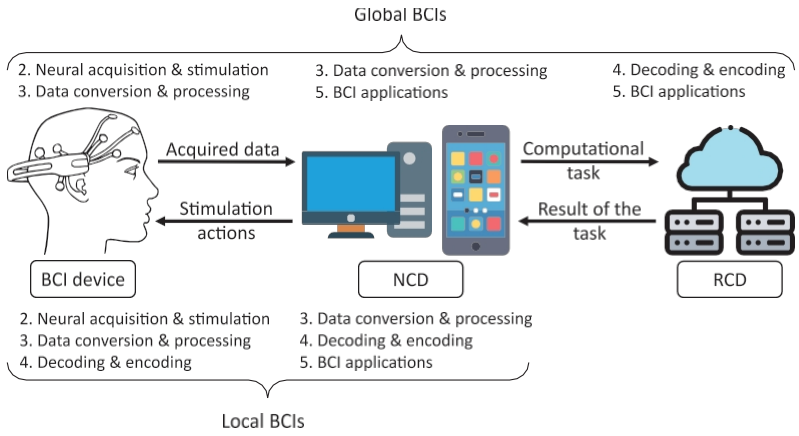

Fig. 4. Representación de los despliegues BCI Local y BCI Global, indicando la comunicación entre sus elementos y las etapas del ciclo BCI que cada elemento implementa según el despliegue arquitectónico.

Los autores de las referencias [17, 136] describieron la posibilidad de *ataques de secuestro*, denominados *brainjacking*, en los que el atacante adquiere acceso completo sobre el dispositivo por cualquier medio. Estos ataques generan un impacto en las cuatro métricas de impacto en la seguridad. Por último, Pycroft et al. [135] identificaron impactos generales sobre la confidencialidad que pueden ser compartidos por múltiples ataques. Identificaron que los IMD de bucle cerrado utilizan datos fisiológicos adquiridos por la BCI para mejorar los procedimientos de estimulación o la administración de fármacos. Sin embargo, estos datos sensibles pueden ser utilizados por los atacantes para adquirir información sobre el estado de salud del paciente. Además, un atacante puede adquirir información sensible almacenada en el dispositivo, como ajustes de estimulación, datos personales o estado de la batería, útil para realizar nuevos ataques.

Considerando las NCD, Ballarin et al. [8] identificaron *ataques de ingeniería social y phishing* contra las BCI, centrados en la adquisición de las credenciales de autenticación de los usuarios, afectando a la confidencialidad de los datos. Aunque las aplicaciones BCI no requieren conexión a Internet, los NCD sí pueden conectarse. Por ello, detectamos que estos sistemas pueden sufrir *ataques de malware* y, en concreto, *ransomware*
[2] y las basadas en *botnets* [74, 77, 159], con un impacto en la integridad y disponibilidad de los datos y aplicaciones contenidos en el DCN, así como en la seguridad de los usuarios. En particular, las *botnets* también generan problemas de confidencialidad de los datos, ya que los atacantes tienen el control del sistema. Además, detectamos *ataques de sniffing* en NCDs que se aprovechan de la configuración y protocolos de red, como MAC flooding, ataques DHCP, ARP spoofing o DNS poisoning [5], afectando a la integridad, confidencialidad y disponibilidad de servicios y datos.

Centrándose en la comunicación entre dispositivos BCI y NCD, Sundararajan et al. [163] estudiaron la seguridad del Emotiv Insight comercial, que implementaba Bluetooth Low Energy (BLE) en su versión 4.0 para comunicarse con un smartphone que contuviera la aplicación ofertada por Emotiv. Realizaron con éxito *ataques man-in-the-middle* a través del enlace Bluetooth Low Energy (BLE), pudiendo interceptar y modificar información, forzar al BCI a realizar tareas no deseadas y llevar a cabo *ataques de repetición* que afectaban, por tanto, a la integridad, confidencialidad y disponibilidad de datos sensibles. La literatura ha documentado otros impactos sobre la integridad y la confidencialidad, en los que los atacantes pueden interceptar y modificar datos sensibles incluso utilizando cifrado [8, 79, 87, 95, 135, 163, 164]. Estos ataques están relacionados con los *ataques criptográficos* descritos anteriormente, en los que un cifrado débil de los datos almacenados en el dispositivo puede derivar en *ataques man-in-the-middle*. Por último,

es importante señalar que los ataques relacionados con los datos de usuario y las credenciales tienen un mayor impacto si varios usuarios utilizan el sistema.

3.1.4 Contramedidas. Para algunos de los ataques anteriores, han propuesto diferentes contramedidas. En relación con los *ataques al firmware*, Ballarin et al. [8] indicaron el cifrado del firmware, así como una verificación de autenticidad mediante hash o firma. Pycroft et al. [136] destacaron las actualizaciones periódicas del firmware y el uso de mecanismos de autorización para estas actualizaciones. Los autores de las referencias [24, 135, 136] identificaron el uso de mecanismos de control de acceso colocados en de- vicios externos con proximidad al paciente y sistemas de detección de anomalías sobre el uso del dispositivo BCI para hacer frente a amenazas potenciales como *los ataques por agotamiento de la batería*. En particular, para estos ataques, se recomienda el uso de baterías recargables para evitar una sustitución quirúrgica. Los autores de la Referencia [79] proponen, como contramedidas generales, la regulación de la neurotecnología como forma de estandarizar sus procesos de fabricación, así como una reducción del proceso de entrenamiento de la BCI, que tiende a frustrar a los usuarios, mostrándose menos dispuestos a cooperar. Estas medidas son complementarias a las documentadas por la Referencia [135], que considera que los dispositivos BCI deben mantener registros y eventos de acceso, incluyendo mecanismos para informar de errores.

El uso de mecanismos criptográficos robustos y las últimas versiones del protocolo son determinantes para evitar *ataques criptográficos*, *ataques man-in-the-middle* y *ataques de sniffing* [8, 163]. Además, la anonimización de la información transmitida de BCI a NCD también es recomendable contra ataques que afecten a la confidencialidad, por ejemplo, utilizando el BCI Anonymizer [17, 18, 164]. Los *ataques de ingeniería social y phishing* centrados en el robo de credenciales pueden reducirse implementando un segundo factor de autenticación para acceder a la BCI y mecanismos adecuados de control de acceso [8, 135, 165]. La aplicación de las contramedidas *de malware* indicadas en la Sección 2.3 puede eludir las amenazas globales *de malware* que afectan a las ENT, actualizando todo el software a la última versión e implementando planes periódicos de copias de seguridad. Además, el uso de técnicas de ML, como las propuestas por Fernández-Maimó et al. [37] para los sistemas ciberfísicos médicos (MCPS), también puede utilizarse para detectar, clasificar y mitigar *los ataques de ran- somware*. En cuanto a *las botnets*, hemos detectado una gran variedad de técnicas de detección para el campo BCI, como el uso de detección de anomalías basada en ML y firmas, la cuarentena de dispositivos infectados y la interrupción de determinados flujos de comunicación [4, 73, 92]. Por último, consideramos que las recomendaciones de la U.S. Food and Drug Administration (FDA) para la gestión previa y posterior a la comercialización de la seguridad en dispositivos médicos son aplicables a la BCI [150, 168, 169].

3.2 ICB mundial

3.2.1 Descripción de la arquitectura. Las arquitecturas BCI globales se centran en la gestión de la adquisición de datos neuronales y la estimulación neuronal de múltiples usuarios a través de una conexión a Internet. Esta arquitectura considera tres dispositivos para desplegar las fases que componen el ciclo BCI, como puede verse en la Figura 4. En esta familia, el dispositivo BCI permanece centrado en la adquisición de datos y estimulación (fase 2), mientras que el NCD se encarga de la ejecución de las aplicaciones (fase 5), así como de las acciones de con- versión y procesamiento (fase 3). Por último, el nuevo elemento introducido en esta arquitectura es el Dispositivo de Control Remoto (RCD), que representa uno o más recursos o servicios externos accesibles a través de Internet, como la computación en nube y el almacenamiento. Normalmente implementa las fases 4 y 5 del ciclo BCI, ya que dispone de recursos para ejecutar aplicaciones más complejas y análisis de información. La principal diferencia entre esta arquitectura y la descrita para las BCI locales en la sección 3.1 es que, en las BCI locales, la NCD no envía información del usuario a servicios externos (por ejemplo, la nube). Por último, esta sección se centra en los problemas asociados a la comunicación entre el NCD y el RCD, y en los ataques relacionados con las BCI que pueden aplicarse a los RCD. Sin embargo, estos últimos ataques se abordan de general, ya que los ataques específicos de la computación en nube quedan fuera del ámbito de este artículo.

3.2.2 Ejemplos de despliegues. Este despliegue arquitectónico es el más innovador, ya que permite la comunicación de múltiples usuarios con servicios externos y la creación de despliegues complejos, donde los datos e información de cada usuario se almacenan y gestionan en una infraestructura compartida. Desde un punto de vista comercial, Emotiv permite a los usuarios contrastar sus datos con los datos almacenados por otros usuarios, así como mantener las grabaciones neuronales de los usuarios en la nube para visualizarlas y manipularlas, ofreciendo además una API llamada Emotiv Cortex [35]. Además, varias empresas de todo el mundo proporcionan servicios BCI distribuidos, como es el caso de Lifelines Neuro [88], que ofrece una adquisición, almacenamiento y visualización continua de EEG en su plataforma en la nube. Estos escenarios son especialmente relevantes en el contexto de la medicina personalizada y el diagnóstico precoz.

3.2.3 Ataques y contramedidas. Considerando los ataques a este despliegue, los problemas documentados en la Sección 3.1 para las BCI Locales son también aplicables en esta arquitectura. Sin embargo, las BCI globales presentan mayores riesgos, ya que estos despliegues son una oportunidad para ataques remotos contra dispositivos BCI interconectados, que derivan en daños físicos para sus usuarios. Además, Takabi et al. [165] detectaron que las aplicaciones BCI podrían enviar señales cerebrales en bruto a servicios en la nube que ejecutan técnicas de ML para extraer información sensible y, por tanto, afectar a la confidencialidad. Identificamos que este problema también puede estar presente en las BCI locales si el NCD dispone de conexión a Internet. Ballarin et al. [8] identificaron que podrían producirse *ataques man-in-the-middle* en el canal de comunicación entre el NCD y el RCD, afectando a la integridad y confidencialidad de los datos transmitidos, así como a la disponibilidad del servicio. También detectaron que los ataques a los RCD podrían tener un mayor impacto en la confidencialidad que en los BCI locales, ya que estas plataformas almacenan información sensible de múltiples usuarios, que puede ser robada o vendida a . Ienca et al. [60] detectaron diferentes problemas en las BCI Globales en cuanto a su uso. En primer lugar, destacaron que las marcas actuales, como Emotiv [34], indican en su política de privacidad que pueden recopilar datos personales, información de uso e interacciones con otras aplicaciones, y que pueden inferir información de estas fuentes, con posibles problemas de confidencialidad. Los autores identificaron como posible el uso de big data para extraer asociaciones y compartir los datos con . Además, detectaron que el uso de servicios en la nube podría derivar en un robo masivo de bases de datos con datos sensibles, una responsabilidad legal poco clara en caso de infracciones.

Identificamos que esta arquitectura es bastante similar a las definidas e implementadas para escenarios de Internet de las Cosas (IoT), donde dispositivos limitados se comunican con servicios externos a través de sistemas in- termedios, especialmente cuando interactúan múltiples dispositivos. Detectamos que la mayoría de los ataques e impactos de seguridad definidos por Stellios et al. [160] también son aplicables en esta . Además, consideramos que las cuestiones destacadas por el OWASP en sus proyectos IoT son aspectos críticos de las ICB globales [125]. Esta relación entre IoT y servicios externos ha sido estudiada previamente en escenarios de computación en nube [19]. A pesar de las ventajas, los ataques a la computación en nube pueden afectar a la integridad, confidencialidad y disponibilidad en diferentes niveles de la arquitectura de la nube, como la infraestructura, la red, el almacenamiento y el software [9, 155]. La evolución de los NCD deriva en dispositivos móviles con mayores capacidades de computación, integrados en sistemas móviles de computación en nube. Sin embargo, también repercuten en la seguridad de los despliegues [113]. Asimismo, detectamos que la mejora de las capacidades de las NCDs también puede permitir la introducción de la computación de niebla en las BCIs globales, donde las NCDs realizan parte del cómputo, generando nuevos problemas de seguridad y confianza [93, 142, 183]. *Los ataques de malware* también están presentes en los entornos de nube, donde el ransomware y las botnets son amenazas comunes [155].

Centrándose en las contramedidas generales de la computación en nube, Amara et al. [3] identificaron las amenazas y ataques a la seguridad, así como las técnicas de mitigación contra ellos. El uso de honeypots, fire walls e IDS en escenarios de nube es conveniente para reducir el impacto de los *ataques de malware* [142].

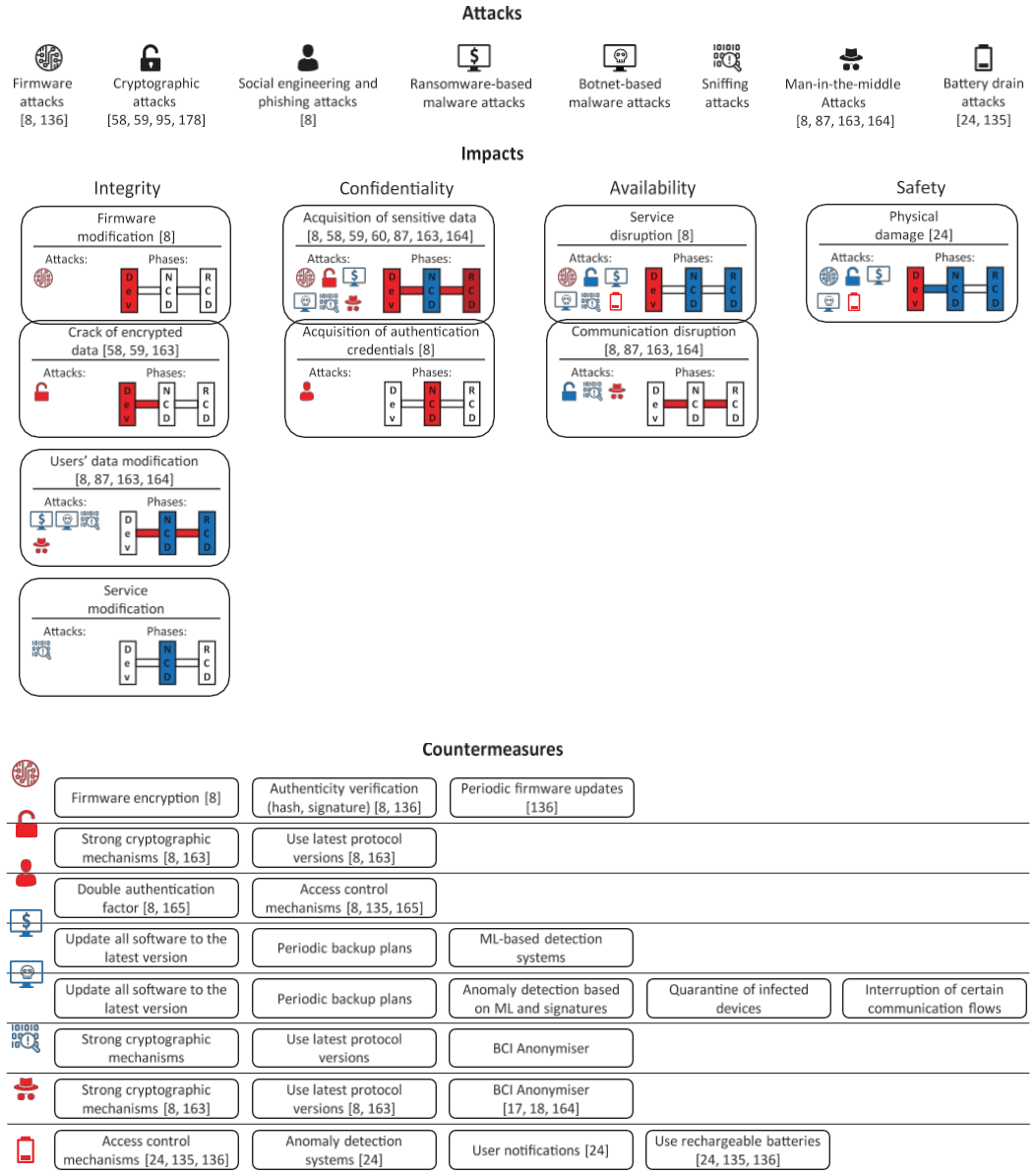

Fig. 5. Anacks, impactos y contramedidas asociados a los despliegues arquitectónicos de la ICB. Los elementos indicados en rojo representan información detectada en la literatura, mientras que el azul representa nuestra contribución.

La figura 5 resume los ataques, impactos y contramedidas anteriores. Esta figura muestra en primer lugar la lista de ataques considerados en esta , asociados a un único icono, donde aquellos ataques con referencias indican que han sido detectados en la literatura, mientras que los que no tienen referencias representan nuestra contribución. A continuación, mostramos los impactos que generan los ataques anteriores, organizados por categorías. Para cada impacto, indicamos los ataques concretos que lo provocan y qué elementos de los despliegues arquitectónicos presentados en la Figura 4 se ven afectados. Además, consideramos los problemas en los enlaces de comunicación entre estos elementos. En concreto, los ataques y elementos identificados en rojo representan problemas detectados en la bibliografía, mientras que los que aparecen en azul son

nuestras contribuciones. Por último, esta figura enumera las contramedidas detectadas tanto en la literatura como por nosotros, asociando a cada ataque una lista de contramedidas. Los criterios de color y referencia utilizados antes para los impactos se aplican también a las contramedidas, donde un ataque representado con un color determinado indica que todas sus contramedidas tienen el mismo color.

4 TENDENCIAS Y RETOS DE LAS CIB

Una de las primeras soluciones BCI se desarrolló a finales de los años noventa. Supuso un avance significativo en la industria médica, concretamente en la neurorrehabilitación, haciendo realidad el control mental de prótesis y sillas de ruedas [119]. Durante la década de 2000, se desarrolló una nueva generación de dispositivos neuroprotésicos para restaurar la movilidad de pacientes con parálisis severa, creando enlaces de comunicación entre el cerebro y una amplia variedad de actuadores, como exoesqueletos robóticos [82]. Esta tendencia en el campo de la BCI ha dado lugar a nuevos paradigmas y escenarios en la última década, en los que los procedimientos de adquisición y estimulación se utilizan conjuntamente para adquirir la actividad cerebral y proporcionar retroalimentación al cerebro o a los nervios periféricos, definiendo el concepto de BCI bidireccional o de bucle cerrado. Centrándonos en estos sistemas, NeuroPace RNS es la única tecnología aprobada clínicamente para el tratamiento en bucle cerrado [33]. La ECP se considera hoy en día un sistema BCI unidireccional, o de bucle abierto, que sólo realiza acciones de estimulación. Sin embargo, la investigación actual pretende desarrollar sistemas de ECP de bucle cerrado capaces de identificar automáticamente los mejores parámetros de estimulación en función del estado del cerebro [52]. Esta evolución también es aplicable a las neuroprótesis, en las que los usuarios pueden controlar mentalmente las prótesis mientras reciben estimulación para recuperar las capacidades motoras [85].

Esta evolución permitió definir formas de interacción prospectivas en las que la ICB actúa como elemento de comunicación en línea con otros sistemas y usuarios, basándose en arquitecturas de ICB globales. A continuación presentamos varios ejemplos de sistemas futuristas para destacar la importancia de la seguridad en el progreso de las tecnologías BCI. Zhang et al. [182] definieron el concepto de Internet del Cerebro, también conocido como Brain-to-Internet (BtI), en el que la BCI utiliza una NCD para acceder a servicios de Internet, como resultados de búsqueda o medios sociales. Lebedev et al. [82] también describieron experimentos en los que monos controlaban brazos robóticos remotos utilizando dispositivos BCI. Más recientemente, Saad et al.
[144] identificaron que las tecnologías 6G podrían permitir la interconexión de las BCI con Internet. Además, Martins et al. [97] documentaron una fusión entre la neuronorobótica y los servicios en la nube para adquirir conocimientos, definiendo el concepto de Human Brain/Cloud Interface (B/CI). Otro enfoque futurístico, Brain-to-Brain (BtB), permite la comunicación directa entre dos cerebros, conocido como BtB [127, 184], donde Pais-Vieira et al. [127] documentaron el intercambio de información en tiempo real entre el cerebro de dos ratas. Estos sistemas también se han ampliado para crear redes de cerebros interconectados, conocidas como Brainet, que pueden realizar tareas colaborativas entre usuarios y compartir conocimientos, recuerdos o pensamientos a través de cerebros remotos [67, 126]. Aunque estos sistemas se encuentran en una fase temprana de investigación, podrían ser una realidad en las próximas décadas, en las que los aspectos de seguridad cobrarán una enorme importancia. Para representar esta tendencia, la Figura 6 ilustra esta evolución de la literatura, indicando los años de publicación y los enfoques. Además, las innovaciones actuales, como el uso de chips basados en silicio, podrían aumentar la cantidad de información que podemos adquirir del cerebro y facilitar el desarrollo de dispositivos electrónicos para mejorar la resolución de la adquisición neuronal y la sensibilidad del proceso [121].

El campo de investigación de la ICB ha cobrado relevancia en los últimos años, en los que distintos gobiernos han financiado y promovido iniciativas de ICB. En Estados Unidos, la DARPA apoya la iniciativa BRAIN (Brain Research through Advancing Innovative Neurotechnologies) [64]. Canadá ha lanzado su línea de investigación, denominada Canadian Brain Research Strategy [63, 162]. Al otro lado del océano Atlántico, la Unión Europea también ha apoyado diferentes proyectos, como el Human Brain Project (HBP) [133] o el Brain/Neural Computer Interaction (BNCI)

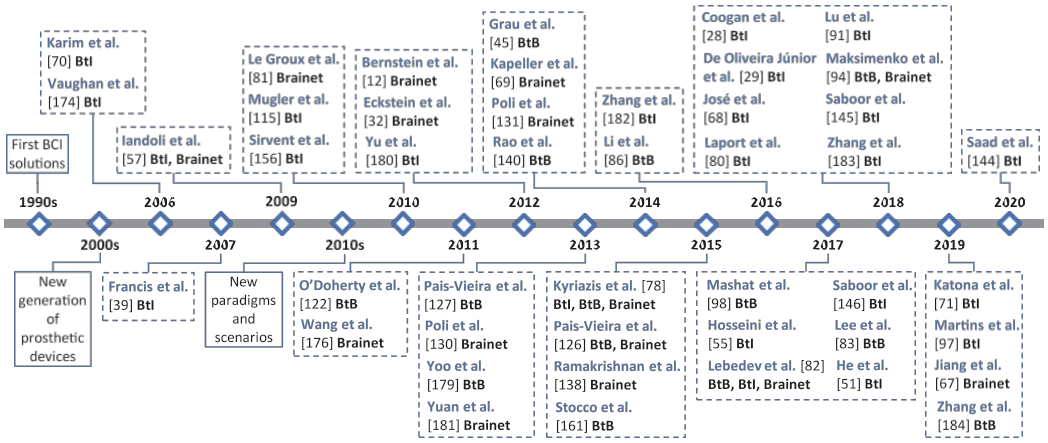

Fig. 6. Cronología de la evolución de la investigación en ICB, vista desde la perspectiva de los enfoques BtI, BtB y Brainet.

[21, 22]. Asia también ha promovido varias iniciativas, como el proyecto China Brain [132] o el proyecto Brain/MINDS en Japón [20]. Todas las iniciativas y proyectos anteriores pretenden avanzar en conocimiento del cerebro humano mediante el uso de tecnologías innovadoras. Como consecuencia, las tecnologías emergentes ofrecen capacidades precisas de adquisición y estimulación que permiten nuevos escenarios de aplicación de la BCI. El interés común en el estudio del cerebro humano y, en particular, en la BCI, conduce a nuevas oportunidades para los fabricantes, que pueden aumentar su competitividad produciendo servicios BCI revolucionarios basados en paradigmas crecientes como el IoT, la computación en la nube y los big data. Este desarrollo deriva en la mejora de la usabilidad, precisión y seguridad de los productos, junto con su expansión a sectores económicos no médicos como el entretenimiento. El resultado de lo anterior es una tendencia de la BCI hacia despliegues de arquitecturas BCI Globales, donde múltiples dispositivos BCI pueden comunicarse entre ellos para realizar tareas colaborativas, basadas en los enfoques de BtI, BtB y Brainet. Una vez resumida la evolución de la BCI y su tendencia, a continuación, destacamos los retos actuales y futuros más relevantes en materia de seguridad en BCI.

4.1 Interoperabilidad entre implantaciones de ICB

Los despliegues de BCI existentes consideran dispositivos aislados sin estándares que proporcionen interoperabilidad en términos de comunicación y representación de datos. Este es el caso de las marcas y dispositivos BCI comerciales, que han sido diseñados para resolver problemas particulares y no son compatibles entre sí [137]. Además, los despliegues que integran la comunicación entre varias BCI son ad hoc; es decir, los fabricantes los diseñan e implementan teniendo en cuenta únicamente los requisitos de un escenario concreto. En este contexto, la tendencia actual de las BCI hacia paradigmas como el IoT y la computación en nube requerirá una mejora de la interoperabilidad, ya que es esencial para garantizar la futura expansión de las tecnologías BCI. Además, la falta de interoperabilidad limita la definición de sistemas y mecanismos globales de ciberseguridad que puedan aplicarse. En este sentido, las soluciones BCI actuales están orientadas a dispositivos y no ofrecen mecanismos de colaboración contra ciberataques. Detectamos como una oportunidad de futuro el uso de APIs, tecnologías de comunicación y protocolos estandarizados bien conocidos para ofrecer una protección sin fisuras en BCI. También proponemos el uso de ontologías para representar la información neuronal de manera formal y estandarizada. Diferentes empresas y productos utilizarían una representación conjunta para facilitar la interpretación, el procesamiento y la puesta en común de los datos. Esta homogeneización tendría un impacto positivo en la ciberseguridad, permitiendo la

diseño y despliegue de nuevos protocolos y mecanismos para el intercambio seguro de determinados datos sensibles entre soluciones BCI independientes. En particular, el intercambio de información médica entre distintas organizaciones puede realizarse utilizando estándares bien conocidos, como es el caso del estándar HL7 [53].

4.2 Extensibilidad de los diseños BCI

La extensibilidad se refiere a la capacidad de los dispositivos BCI para añadir nuevas funcionalidades y escenarios de aplicación de forma dinámica. En la actualidad, los dispositivos BCI adolecen de falta de extensibilidad, ya que las empresas los fabrican para prestar servicios concretos en escenarios de aplicación fijos. El procesamiento de datos neuronales se realiza de forma fija y de acuerdo con unas premisas predefinidas. Esto significa que cada capa que compone las arquitecturas BCI realiza tareas de procesamiento particulares, que no pueden cambiarse ni modificarse bajo demanda [163]. Dado que cada escenario de aplicación tiene sus requisitos y restricciones, la tendencia hacia la ICB Global necesitará nuevas arquitecturas y mecanismos de procesamiento automáticos y flexibles sobre los datos neuronales adquiridos. Estos aspectos también afectan a las soluciones de seguridad que se pueden aplicar, ya que las restricciones actuales de los sistemas BCI impiden el uso de mecanismos de defensa reactivos y adaptativos para hacer frente a las amenazas descritas en las secciones anteriores. Junto con la falta de interoperabilidad, las responsabilidades de seguridad de cada fase de la arquitectura están predefinidas y no pueden ampliarse dentro de ese elemento, ni delegarse para que se realicen en otros sistemas. Como fu- tura línea de trabajo, destacamos el diseño de despliegues BCI que permitan la implementación de la mayoría de las operaciones realizadas en software, en lugar de hardware, permitiendo a los desarrolladores cambiar el comportamiento del sistema. Otra posible solución es un diseño modular de , incluyendo módulos suplementarios, según los requisitos. Sin embargo, estas modificaciones introducen nuevos retos de seguridad, ya que los desarrollos de software son más propensos a errores y ataques, y los nuevos sistemas modulares abordarán retos específicos, como la verificación de su autenticidad.

4.3 Protección de datos

Las arquitecturas y despliegues actuales de BCI no tienen en cuenta la protección de los datos neuronales y la información personal, como se ha detectado en la literatura [137, 152, 164]. La evolución de las BCI hacia escenarios distribuidos con características heterogéneas y ubicuas, como los enfoques BtB, requerirá el almacenamiento y la gestión de datos personales y sensibles de múltiples usuarios. Por ello, los futuros despliegues deberán garantizar que esta información crítica se transmita y procese de forma segura. En concreto, es necesario aplicar mecanismos criptográficos robustos a la comunicación y almacenamiento de datos, mientras que técnicas como la privacidad diferencial o el cifrado homomórfico ayudarían a garantizar el anonimato de los datos. Además, los usuarios no tienen control sobre sus preferencias de privacidad para definir quién tiene acceso a la información y en qué circunstancias concretas. Por ello, no existen normas de privacidad específicas que garanticen que las aplicaciones y los servicios externos sólo puedan acceder a la información neuronal aceptada por los usuarios, ni ninguna limitación que los fabricantes o terceros impidan el tratamiento de datos neuronales sensibles sin la autorización de los usuarios. Para mejorar esta situación, proponemos soluciones basadas en políticas que permitan a los usuarios definir sus preferencias de privacidad en función de su contexto particular. Además, proponemos el uso de sistemas fáciles de usar que también ayuden a los usuarios proponiendo recomendaciones que preserven la privacidad. Estas iniciativas también deben ajustarse a la legislación sobre protección de datos aplicable en cada país.

4.4 Amenazas físicas y arquitectónicas para la ICB

En la actualidad, una cantidad considerable de diseños e implantaciones de ICB no tienen en cuenta cuestiones de ciberseguridad como la protección de las comunicaciones, el procesamiento, el almacenamiento y las aplicaciones. Aunque algunas soluciones incluyen mecanismos de seguridad,

como los productos Medtronic DBS, algunos aspectos deben mejorarse. En concreto, estos dispositivos utilizan protocolos de telemetría propietarios [101], que recientemente

ha dado lugar a vulnerabilidades [27]. No obstante, empresas como Medtronic o Boston Scientific publican boletines de seguridad cuando se detecta una vulnerabilidad que afecta a sus dispositivos [103, 151], lo que pone de manifiesto el interés de las empresas por la seguridad. Además, la falta de estándares de ICB y, en concreto, de ciberseguridad, impide la homogeneización de las soluciones de seguridad implementadas [17, 137, 163, 165]. La expansión de la ICB requerirá mecanismos de ciberseguridad dinámicos y robustos para hacer frente a futuros retos. Además, el desarrollo de dispositivos BCI más precisos y la integración de un gran número de dispositivos y sistemas, daría lugar a una producción masiva de datos sensibles. En nuestra opinión, este contexto podría favorecer el aumento de sistemas y enlaces de comunicación vulnerables. Para hacer frente a estos retos, los fabricantes deberían evaluar alternativas para la mitigación de ciberataques desde múltiples perspectivas, con el objetivo de implementar soluciones de ciberseguridad sin fisuras. Basándonos en ello, proponemos utilizar tecnologías de red 5G, ya que han sido diseñadas para soportar un número significativo de dispositivos, necesarios para los escenarios BtB y Brainet. En particular, identificamos que técnicas y paradigmas asociados al 5G, como la Virtualización de Funciones de Red (NFV) y las Redes Definidas por Software (SDN) para la virtualización y gestión dinámica de las comunicaciones de red, son útiles para el desarrollo de soluciones de ciberseguridad reactivas. Asimismo, tecnologías como Blockchain pueden proporcionar el seguimiento de la información y asegurar que no ha sido modificada, garantizando la integridad de los datos. Además, identificamos la protección de las comunicaciones en red mediante el uso de protocolos como TLS
[62] o IPsec [61], que ofrecen mecanismos robustos contra los ciberataques. Además, detectamos que la aplicación de normas de gestión de riesgos de la información, como la ISO 27000 [65] y el Marco de Ciberseguridad del NIST [120], podría beneficiar la creación de soluciones homogéneas y robustas. Por último, identificamos que la teoría de juegos aplicada a las estrategias de seguridad de las ICB puede ser útil para implementar sistemas que evolucionan regularmente. En particular, pueden ser útiles para modelar cómo establecer las contramedidas más apropiadas contra ataques que cambian de forma continua y automática, específicamente en escenarios distribuidos como BtB [7].

5 CONCLUSIÓN

En este artículo se realiza un análisis global y exhaustivo de la literatura sobre las ICB en términos de . Principalmente, hemos evaluado los ataques, impactos y contramedidas que sufren las so- luciones BCI desde las perspectivas del diseño arquitectónico y la implementación del software. Inicialmente, propusimos una versión unificada del ciclo BCI para incluir los procesos de adquisición de datos neuronales y de estimulación. Una vez que dispusimos de un diseño homogéneo del ciclo BCI, identificamos los ataques a la seguridad, los impactos y las contramedidas que afectan a cada fase del ciclo. Esto sirvió como punto de partida para determinar qué procesos y fases de funcionamiento de las BCI son más propensos a sufrir ataques. También se han analizado los despliegues arquitectónicos de las soluciones BCI actuales para destacar los ataques a la seguridad y las contramedidas relacionadas con cada enfoque para comprender los problemas de estas tecnologías en términos de comunicaciones de red. Por último, aportamos nuestra visión sobre las tendencias de las BCI y de- pectamos que la evolución actual de las BCI hacia dispositivos interconectados está generando enormes problemas y retos de seguridad, que aumentarán en un futuro próximo.

Entre las lecciones aprendidas, destacamos las cinco siguientes: (1) el campo de la seguridad orientada a las tecnologías BCI aún no está maduro, lo que genera oportunidades para los atacantes; (2) incluso los ataques no sofisticados pueden tener un impacto significativo tanto en las tecnologías BCI como en la seguridad de los usuarios;
(3) existe una oportunidad actual para que las iniciativas de normalización unifiquen las ICB en términos de seguridad de la información; (4) los campos bien estudiados, como las IMD y la IO, pueden definir una guía para desarrollar mecanismos de seguridad sólidos para las ICB; (5) la concienciación de los usuarios sobre los problemas de seguridad de las ICB es vital.

Como trabajo futuro, planeamos centrar nuestros esfuerzos en el diseño e implementación de soluciones capaces de detectar y mitigar ataques que afecten al proceso de estimulación en tiempo real.

En este contexto, estamos considerando la posibilidad de utilizar técnicas de inteligencia artificial para detectar anomalías en los patrones de disparo y

actividad neuronal controlada por soluciones BCI encargadas de estimular el . Además, también planeamos contribuir mejorando la interoperabilidad y los mecanismos de protección de datos de las arquitecturas BCI existentes. Finalmente, otro trabajo futuro es el desarrollo de sistemas dinámicos y proactivos como una oportunidad para mitigar los impactos de los ataques documentados en este trabajo.

ACUSE DE RECIBO

Agradecemos a Mattia Zago sus consejos durante el desarrollo del soporte visual del trabajo.

REFERENCIAS

[1] Minkyu Ahn, Mijin Lee, Jinyoung Choi, Sung Jun, Minkyu Ahn, Mijin Lee, Jinyoung Choi y Sung Chan Jun. 2014. Una revisión de los juegos de interfaz cerebro-ordenador y una encuesta de opinión de investigadores, desarrolladores y usuarios. *Sensors* 14, 8 (agosto de 2014), 14601-14633.

[2] Bander Ali Saleh Al-rimy, Mohd Aizaini Maarof y Syed Zainudeen Mohd Shaid. 2018. Factores de éxito de la amenaza ransomware, taxonomía y contramedidas: Una encuesta y direcciones de investigación. *Comput. Secur.* 74 (mayo de 2018), 144-166.

[3] Naseer Amara, Huang Zhiqui y Awais Ali. 2017. Cloud computing security threats and attacks with their mitiga- tion techniques. En *Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowl- edge Discovery (CyberC'17)*. IEEE, 244-251.

[4] Pedram Amini, Muhammad Amin Araghizadeh y Reza Azmi. 2015. Un estudio sobre Botnet: Clasificación, detección y defensa. En *Actas del Simposio Internacional de Electrónica (IES'15)*. IEEE, 233-238.

[5] P. Anu y S. Vimala. 2017. A survey on sniffing attacks on computer . En *Actas de la Conferencia Internacional sobre Computación Inteligente y Control (I2C2'17)*. IEEE, 5.

[6] P. Arico, G. Borghini, G. Di Flumeri, N. Sciaraffa y F. Babiloni. 2018. BCI pasiva más allá del laboratorio: Tendencias actuales y direcciones futuras. *Physiol. Measure.* 39, 8 (ago. 2018), 08TR02.

[7] A. Attiah, M. Chatterjee y C. C. Zou. 2018. A game theoretic approach to model cyber attack and defense strate- gies. En *Actas de la Conferencia Internacional del IEEE sobre Comunicaciones (ICC'18)*. IEEE, 1-7.

[8] Pablo Ballarín Usieto y Javier Mínguez. 2018. Evitar el hackeo del cerebro-Retos de ciberseguridad y pri- vacidad en las interfaces cerebro-ordenador. Recuperado de https://www.bitbrain.com/blog/cybersecurity-brain-computer- interface.

[9] Srijita Basu, Arjun Bardhan, Koyal Gupta, Payel Saha, Mahasweta Pal, Manjima Bose, Kaushik Basu, Saunak Chaudhury y Pritika Sarkar. 2018. Cloud computing security challenges & solutions-A survey. En *Actas del 8º Taller y Conferencia Anual de Computación y Comunicación del IEEE (CCWC'18)*. IEEE, 347-356.

[10] Nebia Bentabet y Nasr Eddine Berrached. 2016. BCI sincrónica basada en P300 para controlar electrodomésticos. En *Actas de la 8ª Conferencia Internacional sobre Modelización, Identificación y Control (ICMIC'16)*. IEEE, 835-838.

[11] S. López Bernal, A. Huertas Celdrán, L. Fernández Maimó, M. T. Barros, S. Balasubramaniam y G. Martínez Pérez. 2020. Ciberataques a implantes cerebrales en miniatura para interrumpir la señalización neuronal espontánea. *IEEE Access* 8 (2020), 152204-152222.

[12] Abraham Bernstein, Mark Klein y Thomas W. Malone. 2012. Programando el cerebro global. *Commun. ACM* 55, 5 (mayo de 2012), 41.

[13] Meriem Bettayeb, Qassim Nasir y Manar Abu Talib. 2019. Ataques de actualización de firmware y seguridad para dispositivos IoT. En *Actas de la sexta conferencia internacional anual ArabWIC Research Track*. ACM Press, 6.

[14] Marom Bikson, Andre R. Brunoni, Leigh E. Charvet, Vincent P. Clark, Leonardo G. Cohen, Zhi-De Deng, Jacek Dmochowski, Dylan J. Edwards, Flavio Frohlich, Emily S. Kappenman, Kelvin O. Lim, Colleen Loo, Antonio Mantovani, David P. McMullen, Lucas C. Parra, Michele Pearson, Jessica D. Richardson, Judith M. Rumsey, Pejman Sehatpour, David Sommers, Gozde Unal, Eric M. Wassermann, Adam J. Woods y Sarah H. Lisanby. 2018. Rigor y reproducibilidad en la investigación con estimulación eléctrica transcraneal: Un taller patrocinado por el NIMH. *Brain Stimul.* 11, 3 (2018), 465-480.

[15] Gajanan K. Birajdar y Vijay H. Mankar. 2013. Detección de falsificación de imágenes digitales mediante técnicas pasivas: A survey.
Dig. Investigat. 10, 3 (oct. 2013), 226-245.

[16] Paul E. Black e Irena Bojanova. 2016. Derrotando el desbordamiento del búfer: Un fallo trivial pero peligroso. *IT Profess.* 18, 6 (Nov 2016), 58-61.

[17] Tamara Bonaci, Ryan Calo y Howard Jay Chizeck. 2015. Tiendas de aplicaciones para el cerebro: Privacidad y seguridad en interfaces cerebro-ordenador. *IEEE Technol. Soc. Mag.* 34, 2 (junio de 2015), 32-39.

[18] Tamara Bonaci, Jeffrey Herron, Charles Matlack y Howard Jay Chizeck. 2015. Asegurar el exocórtex: Un desafío cibernético del siglo XXI. *IEEE Technol. Soc. Mag.* 34, 3 (Sep. 2015), 44-51. arxiv:hep-ph/0011146

[19] Alessio Botta, Walter de Donato, Valerio Persico y Antonio Pescapé. 2016. Integración de la computación en nube y el Internet de las cosas: Una encuesta. *Future Gen. Comput. Syst.* 56 (mar. 2016), 684-700.

[20] Proyecto Brain/MINDS. 2019. Proyecto cerebro/MINDS. Obtenido de https://brainminds.jp/en/.
[21] Proyecto de interacción cerebro-ordenador neuronal. 2015. Proyecto de interacción cerebro-ordenador neuronal. Obtenido de http://bnci-horizon-2020.eu/.
[22] Clemens Brunner, Niels Birbaumer, Benjamin Blankertz, Christoph Guger, Andrea Kübler, Donatella Mattia, José del R. Millán, Felip Miralles, Anton Nijholt, Eloy Opisso, Nick Ramsey, Patric Salomon y Gernot R. Müller-Putz. 2015. BNCI Horizonte 2020: Hacia una hoja de ruta para la comunidad BCI. *Brain-Comput. Interfaces* 2, 1 (enero de 2015), 10.
[23] Carsten Buhmann, Torge Huckhagel, Katja Engel, Alessandro Gulberti, Ute Hidding, Monika Poetter-Nerger, Ines Goerendt, Peter Ludewig, Hanna Braass, Chi-un Choe, Kara Krajewski, Christian Oehlwein, Katrin Mittmann, Andreas K. Engel, Christian Gerloff, Manfred Westphal, Johannes A. Köppen, Christian K. E. Moll y Wolfgang Hamel. 2017. Eventos adversos en la estimulación cerebral profunda: A retrospective long-term analysis of neurological, psychi- atric and other occurrences. *PLoS ONE* 12, 7 (julio de 2017), 1-21.
[24] Carmen Cámara, Pedro Peris-López y Juan E. Tapiador. 2015. Problemas de seguridad y privacidad en dispositivos médicos implantables: Un estudio exhaustivo. *J. Biomed. Info.* 55 (junio de 2015), 272-289.
[25] Debashis Das Chakladar y Sanjay Chakraborty. 2018. Extracción y clasificación de características en la interfaz cerebro-ordenador: Problemas y desafíos futuros de investigación. En *Computación natural para el aprendizaje no supervisado*. Springer, Cham, capítulo 5, 101-131.
[26] Howard Jay Chizeck y Tamara Bonaci. 2014. Anonimizador de interfaz cerebro-ordenador. Solicitud de patente estadounidense. US20140228701A1.
[27] Agencia de Ciberseguridad y Seguridad de Infraestructuras (CISA). 2020. ICS Medical Advisory (ICSMA-19-080-01). Obtenido de https://us-cert.cisa.gov/ics/advisories/ICSMA-19-080-01.
[28] Christopher G. Coogan y Bin He. 2018. Control de interfaz cerebro-ordenador en un entorno de realidad virtual y aplicaciones para el Internet de las Cosas. *IEEE Access* 6 (2018), 10840-10849.
[29] Wilson G. de Oliveira Júnior, Juliana M. de Oliveira, Roberto Munoz y Victor Hugo C. de Albuquerque. 2020. Una propuesta de Internet de las Cosas Inteligentes para el Hogar basada en el sistema BCI para ayudar a los pacientes con esclerosis lateral amiotrófica. *Neural Comput. Appl.* 32, 15 (Aug. 2020), 11007-11017.
[30] Till A. Dembek, Paul Reker, Veerle Visser-Vandewalle, Jochen Wirths, Harald Treuer, Martin Klehr, Jan Roediger, Haidar S. Dafsari, Michael T. Barbe y Lars Timmermann. 2017. La ECP direccional aumenta los umbrales de efectos secundarios: un ensayo prospectivo doble ciego. *Move. Disord.* 32, 10 (2017), 1380-1388.
[31] Tamara Denning, Yoky Matsuoka y Tadayoshi Kohno. 2009. Neuroseguridad: Security and privacy for neural de- vices. *Neurosurg. Focus* 27, 1 (2009), E7.
[32] Miguel P. Eckstein, Koel Das, Binh T. Pham, Matthew F. Peterson, Craig K. Abbey, Jocelyn L. Sy y Barry Giesbrecht. 2012. Descodificación neuronal de la sabiduría colectiva con computación multicerebro. *NeuroImage* 59, 1 (enero de 2012), 94-108.
[33] Christine A. Edwards, Abbas Kouzani, Kendall H. Lee y Erika K. Ross. 2017. Dispositivos de neuroestimulación para el tratamiento de trastornos neurológicos. *Mayo Clin. Proceed.* 92, 9 (2017), 1427-1444.
[34] Emotiv. 2019. Emotiv. Obtenido de https://www.emotiv.com/.
[35] Emotiv. 2019. Emotiv Cortex API. Obtenido de https://emotiv.github.io/cortex-docs/#introduction.
[36] Emotiv. 2019. EMOTIV EPOC+. Obtenido de https://www.emotiv.com/epoc/.
[37] Lorenzo Fernández Maimó, Alberto Huertas Celdrán, Ángel Perales Gómez, Félix García Clemente, James Weimer e Insup Lee. 2019. Detección y mitigación inteligente y dinámica de la propagación de ransomware en entornos clínicos integrados. *Sensors* 19, 5 (mar. 2019), 1114.
[38] Samuel G. Finlayson, John D. Bowers, Joichi Ito, Jonathan L. Zittrain, Andrew L. Beam e Isaac S. Kohane. 2019. Ataques adversariales en el aprendizaje automático médico. *Science* 363, 6433 (mar. 2019), 1287-1289.
[39] Heylighen Francis. 2007. El superorganismo global: Un modelo evolutivo-cibernético de la emergente sociedad red. *Soc. Evol. Hist.* 6, 1 (2007), 58-119.
[40] Mario Frank, Tiffany Hwu, Sakshi Jain, Robert T. Knight, Ivan Martinovic, Prateek Mittal, Daniele Perito, Ivo Sluganovic y Dawn Song. 2017. Uso de dispositivos BCI basados en EEG para sondear subliminalmente información privada. En *Actas del Taller sobre privacidad en la sociedad electrónica (WPES'17)*. ACM Press, Nueva York, Nueva York, 133-136. Obtenido de https://arxiv:1312.6052.
[41] Jianwen Fu, Jingfeng Xue, Yong Wang, Zhenyan Liu y Chun Shan. 2018. Visualización de malware para clasificación de grano fino. *IEEE Access* 6 (2018), 14510-14523.
[42] Ariko Fukushima, Reiko Yagi, Norie Kawai, Manabu Honda, Emi Nishina y Tsutomu Oohashi. 2014. Frecuencias de sonidos inaudibles de alta frecuencia afectan diferencialmente a la actividad cerebral: Efectos hipersónicos positivos y negativos. *PLoS ONE* 9, 4 (abr. 2014), e95464.
[43] Joyce Gomes-Osman, Aprinda Indahlastari, Peter J. Fried, Danylo L. F. Cabral, Jordyn Rice, Nicole R. Nissim, Serkan Aksu, Molly E. McLaren y Adam J. Woods. 2018. Estimulación cerebral no invasiva: Sondeando circuitos intracorticales y mejorando la cognición en el cerebro envejecido. *Front. Aging Neurosci.* 10 (2018), 177.

[44] Ian Goodfellow, Patrick McDaniel y Nicolas Papernot. 2018. Making machine learning robust against adversarial inputs. *Commun. ACM* 61, 7 (julio de 2018), 56-66.

[45] Carles Grau, Romuald Ginhoux, Alejandro Riera, Thanh Lam Nguyen, Hubert Chauvat, Michel Berg, Julià L. Amengual, Álvaro Pascual-Leone y Giulio Ruffini. 2014. Comunicación consciente cerebro-cerebro en humanos usando tecnologías no invasivas. *PLoS ONE* 9, 8 (agosto de 2014), e105225.

[46] Kanika Grover, Alvin Lim y Qing Yang. 2014. Jamming and anti-jamming techniques in wireless networks: A survey. *Int. J. Ad Hoc and Ubiquitous Computing* 17, 4 (2014), 197.

[47] Surbhi Gupta, Abhishek Singhal y Akanksha Kapoor. 2017. Estudio bibliográfico sobre ataques de ingeniería social: Ataque de suplantación de identidad. En *Actas de la Conferencia Internacional del IEEE sobre Informática, Comunicación y Automatización (ICCCA'16)*. IEEE, 537-540.

[48] Christian J. Hartmann, Sabine Fliegen, Stefan J. Groiss, Lars Wojtecki y Alfons Schnitzler. 2019. Una actualización sobre las mejores prácticas de estimulación cerebral profunda en la enfermedad de Parkinson. *Therap. Adv. Neurol. Disord.* 12 (ene. 2019), 1756286419838096.

[49] Joseph M. Hatfield. 2018. Ingeniería social en ciberseguridad: La evolución de un concepto. *Comput. Secur.* 73 (2018), 102-113.

[50] Vincent Haupert, Dominik Maier, Nicolas Schneider, Julian Kirsch y Tilo Müller. 2018. Cariño, he encogido la seguridad de tu aplicación: The state of android app hardening. En *Detección de intrusiones y malware, y evaluación de vulnerabilidades*. Springer International Publishing, Cham, 69-91.

[51] Shenghong He, Tianyou Yu, Zhenghui Gu y Yuanqing Li. 2017. Un navegador web BCI híbrido basado en señales EEG y EOG. En *Actas de la 39ª Conferencia Internacional Anual de la Sociedad IEEE de Ingeniería en Medicina y Biología (EMBC'17)*. IEEE, 1006-1009.

[52] Franz Hell, Carla Palleis, Jan H. Mehrkens, Thomas Koeglsperger y Kai Bötzel. 2019. Estimulación cerebral profunda programming 2.0: Perspectivas futuras para la identificación de objetivos y la estimulación adaptativa en bucle cerrado. *Front. Neurol.* 10 (2019), 314.

[53] HL7 International. 2019. Nivel siete de la salud. Obtenido de https://www.hl7.org/.

[54] Keum Shik Hong y Muhammad Jawad Khan. 2017. Técnicas híbridas de interfaz cerebro-ordenador para mejorar la precisión de clasificación y aumentar el número de comandos: Una revisión. *Front. Neurorobot.* 11 (julio 2017), 35.

[55] Mohammad-Parsa Hosseini, Dario Pompili, Kost Elisevich y Hamid Soltanian-Zadeh. 2017. Optimized deep learn- ing for EEG big data and seizure prediction BCI via Internet of . *IEEE Trans. Big Data* 3, 4 (dic. 2017), 392- 404.

[56] Alberto Huertas Celdrán, Ginés Dólera Tormo, Félix Gómez Mármol, Manuel Gil Pérez y Gregorio Martínez Pérez. 2016. Resolución de relaciones que preservan la privacidad sobre almacenamientos de datos cifrados externalizados. *Int. J. Info. Secur.* 15, 2 (abr. 2016), 195-209.

[57] Luca Iandoli, Mark Klein y Giuseppe Zollo. 2009. Permitir la deliberación en línea y la toma de decisiones colectiva mediante la argumentación a gran escala. *Int. J. Decis. Supp. Syst. Technol.* 1, 1 (enero de 2009), 69-92.

[58] Marcello Ienca. 2015. Neuroprivacy, neurosecurity and brain-hacking: Cuestiones emergentes en ingeniería neuronal. *Foro de Bioética* 8, 2 (2015), 51-53.

[59] Marcello Ienca y Pim Haselager. 2016. Hackear el cerebro: La tecnología de interfaz cerebro-ordenador y la ética de la neuroseguridad. *Ética Info. Technol.* 18, 2 (junio de 2016), 117-129.

[60] Marcello Ienca, Pim Haselager y Ezekiel J. Emanuel. 2018. Fugas cerebrales y neurotecnología de consumo. *Nature Biotechnol.* 36, 9 (2018), 805-810.

[61] IETF. 2011. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. Obtenido de https://tools.ietf.org/html/rfc6071.

[62] IETF. 2018. Protocolo de seguridad de la capa de transporte (TLS) versión 1.3. Obtenido de https://tools.ietf.org/html/rfc8446.

[63] Judy Illes, Samuel Weiss, Jaideep Bains, Jennifer A. Chandler, Patricia Conrod, Yves De Koninck, Lesley K. Fellows, Deanna Groetzinger, Eric Racine, Julie M. Robillard y Marla B. Sokolowski. 2019. A neuroethics backbone for the evolving canadian brain research strategy. *Neuron* 101, 3 (feb. 2019), 370-374.

[64] La iniciativa BRAIN. 2019. La iniciativa BRAIN. Obtenido de https://braininitiative.nih.gov/.

[65] ISO. 2018. ISO/IEC 27001 Gestión de la seguridad de la información. Obtenido de https://www.iso.org/isoiec-27001-information-security.html.

[66] Matthew Jagielski, Alina Oprea, Battista Biggio, Chang Liu, Cristina Nita-Rotaru y Bo Li. 2018. Manipulating ma- chine learning: Ataques de envenenamiento y contramedidas para el aprendizaje de regresión. En *Actas del Simposio del IEEE sobre seguridad y privacidad*. IEEE, 19-35.

[67] Linxing Jiang, Andrea Stocco, Darby M. Losey, Justin A. Abernethy, Chantel S. Prat y Rajesh P. N. Rao. 2019. BrainNet: Una interfaz cerebro-cerebro multipersonal para la colaboración directa entre cerebros. *Sci. Rep.* 9, 1 (dic. 2019), 6115.

[68] Sergio José y Rodríguez Méndez. 2018. Modelado de actuaciones en BCI-O. En *Proceedings of the 8th International Conference on the Internet of Things (IOT'18)*. ACM Press, Nueva York, 6.

[69] Christoph Kapeller, Rupert Ortner, Gunther Krausz, Markus Bruckner, Brendan Z. Allison, Christoph Guger y Günter Edlinger. 2014. Hacia la comunicación multicerebro: Ortografía colaborativa con un P300 BCI. En *Actas de la Conferencia Internacional sobre Cognición Aumentada*. Springer, Cham, 47-54.

[70] Ahmed A. Karim, Thilo Hinterberger, Jürgen Richter, Jürgen Mellinger, Nicola Neumann, Herta Flor, Andrea Kübler y Niels Birbaumer. 2006. Internet neuronal: Web surfing with brain potentials for the completely paralyzed. *Neu- rorehab. Neural Repair* 20, 4 (dic. 2006), 508-515.

[71] Jozsef Katona, Tibor Ujbanyi, Gergely Sziladi y Attila Kovari. 2019. *Interfaz cerebro-ordenador basada en electroencefalograma para Internet de las Cosas Robóticas*. Springer International Publishing, Cham, capítulo 12, 253-275.

[72] Elena Khabarova, Natalia Denisova, Aleksandr Dmitriev, Konstantin Slavin y Leo Verhagen Metman. 2018. Estimulación cerebral profunda del núcleo subtalámico en pacientes con enfermedad de parkinson con palidotomía o talam- otomía previa. *Brain Sci.* 8, 4 (abr. 2018), 66.

[73] G. Kirubavathi y R. Anitha. 2018. Análisis estructural y detección de botnets android utilizando técnicas de aprendizaje automático. *Int. J. Info. Secur.* 17, 2 (abr. 2018), 153-167.

[74] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou y Jeffrey Voas. 2017. DDoS en el IoT: Mirai y otras redes de bots. *Computer* 50, 7 (2017), 80-84.

[75] Jan Kubanek. 2018. Neuromodulación con ultrasonido focalizado transcraneal.*Neurosurg. Focus* 44, 2 (feb. 2018), E14.

[76] D. Richard Kuhn, Vincent C. Hu, W. Timothy Polk y Shu-Jen Chang. 2001. *Introducción a la tecnología de clave pública y a la infraestructura federal PKI*. Informe técnico. Instituto Nacional de Estándares y Tecnología, 1-54. Obtenido de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf.

[77] James Kurose y Keith Ross. 2017. *Redes de ordenadores: A Top-Down Approach* (7ª ed.). Pearson, Londres, 852 páginas.

[78] Marios Kyriazis. 2015. La neurociencia de sistemas en el punto de mira: ¿Del cerebro humano al cerebro global? *Front. Syst. Neurosci.*
9 (feb. 2015), 7.

[79] Ofir Landau, Rami Puzis y Nir Nissim. 2020. Mind your mind. *Comput. Surveys* 53, 1 (2020), 1-38.

[80] Francisco Laport, Francisco J. Vázquez-Araujo, Paula M. Castro, Adriana Dapena, Francisco Laport, Francisco J. Vázquez-Araujo, Paula M. Castro y Adriana Dapena. 2018. Interfaces cerebro-ordenador para Internet de las Cosas. *Proceedings* 2, 18 (sep. 2018), 1179.

[81] Sylvain Le Groux, Jonatas Manzolli, Paul F. Verschure, Marti Sanchez, Andre Luvizotto, Anna Mura, Aleksander Valjamae, Christoph Guger, Robert Prueckl y Ulysses Bernardet. 2010. Interacción musical incorpórea y colaborativa en la orquesta cerebral multimodal. En *Proceedings of the International Conference on New Interfaces for Musical Expression*. MIME, 309-314.

[82] Mikhail A. Lebedev y Miguel A. L. Nicolelis. 2017. Interfaces cerebro-máquina: From basic science to neuroprosthe- ses and neurorehabilitation. *Physiol. Rev.* 97, 2 (abr. 2017), 767-837.

[83] Wonhye Lee, Suji Kim, Byeongnam Kim, Chungki Lee, Yong An Chung, Laehyun Kim y Seung-Schik Yoo. 2017. Transmisión no invasiva de información sensoriomotora en humanos utilizando una interfaz cerebro-cerebro de EEG/ ultrasonido focalizado. *PLoS ONE* 12, 6 (julio de 2017), e0178476.

[84] M. León Ruiz, M. L. Rodríguez Sarasa, L. Sanjuán Rodríguez, J. Benito-León, E. García-Albea Ristol, y S. Arce Arce. 2018. Evidencia actual sobre la estimulación magnética transcraneal y su potencial utilidad en la neuroreha- bilitación post-ictus: Abriendo nuevas puertas al tratamiento de la enfermedad cerebrovascular. *Neurología (Edición en español)* 33, 7 (2018), 459-472.

[85] Timothée Levi, Paolo Bonifazi, Paolo Massobrio y Michela Chiappalone. 2018. Editorial: Sistemas de bucle cerrado para neuroprótesis de próxima generación. *Front. Neurosci.* 12 (2018), 26.

[86] Guangye Li y Dingguo Zhang. 2016. Ciborg controlado por interfaz cerebro-ordenador: Establishing a functional information transfer pathway from human brain to cockroach brain. *PLoS ONE* 11, 3 (mar. 2016), e0150667.

[87] Qianqian Li, Ding Ding y Mauro Conti. 2015. Aplicaciones de interfaz cerebro-ordenador: Security and privacy challenges. En *Proceedings of the IEEE Conference on Communications and Network Security (CNS'15)*. IEEE, 663-666.

[88] Líneas de vida Neuro. 2020. Neurodiagnóstico sin fronteras. Obtenido de https://www.lifelinesneuro.com/.

[89] Anli Liu, Mihály Vöröslakos, Greg Kronberg, Simon Henin, Matthew R. Krause, Yu Huang, Alexander Opitz, Ashesh Mehta, Christopher C. Pack, Bart Krekelberg, Antal Berényi, Lucas C. Parra, Lucia Melloni, Orrin Devinsky y György Buzsáki. 2018. Efectos neurofisiológicos inmediatos de la estimulación eléctrica transcraneal. *Nature Commun.* 9, 1 (nov. 2018), 5092.

[90] Qiang Liu, Pan Li, Wentao Zhao, Wei Cai, Shui Yu y Victor C. M. Leung. 2018. Un estudio sobre las amenazas a la seguridad y las técnicas defensivas del aprendizaje automático: Una visión basada en datos. *IEEE Access* 6 (2018), 12103-12117.

[91] Huimin Lu, Hyoungseop Kim, Yujie Li y Yin Zhang. 2018. BrainNets: Reconocimiento de emociones humanas utilizando una plataforma de Internet de Brian Things. En *las actas de la 14ª Conferencia Internacional de Comunicaciones Inalámbricas y Computación Móvil (IWCMC'18)*. IEEE, 1313-1316.

[92] Muhammad Mahmoud, Manjinder Nir y Ashraf Matrawy. 2015. A survey on botnet architectures, detection and defences. *Int. J. Netw. Secur.* 17, 3 (mayo de 2015), 272-289.
[93] Redowan Mahmud, Ramamohanarao Kotagiri y Rajkumar Buyya. 2018. Fog computing: Una taxonomía, encuesta y direcciones futuras. En *Internet of Everything*. Springer, Singapur, 103-130.
[94] Vladimir A. Maksimenko, Alexander E. Hramov, Nikita S. Frolov, Annika Lüttjohann, Vladimir O. Nedaivozov, Vadim V. Grubov, Anastasia E. Runnova, Vladimir V. Makarov, Jürgen Kurths y Alexander N. Pisarchik. 2018. Aumento del rendimiento humano compartiendo la carga cognitiva mediante una interfaz cerebro-cerebro. *Front. Neurosci.* 12 (dic. 2018), 949.
[95] Eduard Marin, Dave Singelée, Bohan Yang, Vladimir Volski, Guy A. E. Vandenbosch, Bart Nuttin y Bart Preneel. 2018. Asegurando neuroestimuladores inalámbricos. En *Proceedings of the 8th ACM Conference on Data and Application Security and Privacy (CODASPY'18)*. Association for Computing Machinery, Nueva York, NY, 287-298.
[96] Ivan Martinovic, Doug Davies y Mario Frank. 2012. On the feasibility of side-channel attacks with brain-computer interfaces. En *Proceedings of the 21st USENIX Security Symposium*. USENIX, Bellevue, WA, 143-158.
[97] Nuno R. B. Martins, Amara Angelica, Krishnan Chakravarthy, Yuriy Svidinenko, Frank J. Boehm, Ioan Opris, Mikhail A. Lebedev, Melanie Swan, Steven A. Garan, Jeffrey V. Rosenfeld, Tad Hogg y Robert A. Freitas. 2019. Interfaz cerebro humano/nube. *Front. Neurosci.* 13 (mar. 2019), 112.
[98] M. Ebrahim M. Mashat, Guangye Li y Dingguo Zhang. 2017. Control de bucle cerrado entre humanos basado en la interfaz cerebro-cerebro y la interfaz músculo-músculo. *Sci. Rep.* 7, 1 (dic. 2017), 11001.
[99] Hideyuki Matsumoto y Yoshikazu Ugawa. 2017. Eventos adversos de tDCS y tACS: Una revisión. *Clin. Neurophysiol. Pract.* 2 (2017), 19-25.
[100] M. McMahon y M. Schukat. 2018. A low-cost, open-source, BCI- VR game control development environment prototype for game-based neurorehabilitation. En *las actas de la conferencia IEEE Games, Entertainment, Media (GEM'18)*. IEEE, 1-9.
[101] Medtronic. 2020. Guía de referencia de seguridad de la ECP. Obtenido de http://manuals.medtronic.com/content/dam/emanuals/neuro/NDHF1550-189563.pdf.
[102] Medtronic. 2020. DBS Theraphy for OCD. Obtenido del sitio Web: https://www.medtronic.com/us-en/patients/treatments-therapies/deep-brain-stimulation-ocd/about/risks-probable-benefits.html.
[103] Medtronic. 2020. Boletines de seguridad. Obtenido de https://global.medtronic.com/xg-en/product-security/security-bulletins.html.
[104] Najmeh Miramirkhani, Mahathi Priya Appini, Nick Nikiforakis y Michalis Polychronakis. 2017. Cajas de arena sin manchas: Evadiendo los sistemas de análisis de malware usando artefactos de desgaste. En *Actas del Simposio del IEEE sobre seguridad y privacidad (SP'17)*. IEEE, 1009-1024.
[105] MITRE. 2019. CWE-CWE-74: Neutralización inadecuada de elementos especiales en la salida utilizada por un componente descendente ("Inyección") (3.2). Obtenido de https://cwe.mitre.org/data/definitions/74.html.
[106] MITRE. 2019. CWE-CWE-77: Neutralización indebida de elementos especiales utilizados en un comando ("Command Injec- tion") (3.2). Obtenido de https://cwe.mitre.org/data/definitions/77.html.
[107] MITRE. 2019. CWE-CWE-78: Neutralización inadecuada de elementos especiales utilizados en un comando de sistema operativo ("OS Command Injection") (3.2). Obtenido de https://cwe.mitre.org/data/definitions/78.html.
[108] MITRE. 2019. CWE-CWE-89: Neutralización inadecuada de elementos especiales utilizados en un comando SQL ("SQL Injec- tion") (3.2). Obtenido de https://cwe.mitre.org/data/definitions/89.html.
[109] MITRE. 2019. CWE-119: Restricción inadecuada de operaciones dentro de los límites de un búfer de memoria. Obtenido de https://cwe.mitre.org/data/definitions/119.html.
[110] MITRE. 2019. CWE-120: Copia de búfer sin comprobar el tamaño de la entrada ("desbordamiento de búfer clásico") (3.2). Obtenido de https://cwe.mitre.org/data/definitions/120.html.
[111] MITRE. 2019. CWE-121: Desbordamiento de búfer basado en pila (3.2). Obtenido de https://cwe.mitre.org/data/definitions/ 121.html.
[112] MITRE. 2019. CWE-122: Desbordamiento de búfer basado en montón (3.2). Obtenido de https://cwe.mitre.org/data/definitions/ 122.html.
[113] Muhammad Baqer Mollah, Md. Abul Kalam Azad, y Athanasios Vasilakos. 2017. Retos de seguridad y privacidad en la computación en nube móvil: Encuesta y camino a seguir. *J. Netw. Comput. Appl.* 84 (abr. 2017), 38-54.
[114] Ingrid Moreno-Duarte, Nigel Gebodh, Pedro Schestatsky, Berkan Guleyupoglu, Davide Reato, Marom Bikson y Felipe Fregni. 2014. Capítulo 2-Estimulación eléctrica transcraneal: Transcranial Direct Current Stimulation (tDCS), Transcranial Alternating Current Stimulation (tACS), Transcranial Pulsed Current Stimulation (tPCS), y Tran- scranial Random Noise Stimulation (tRNS). En *The Stimulated Brain*, Roi Cohen Kadosh (Ed.). Academic Press, San Diego, 35-59.
[115] Emily M. Mugler, Carolin A. Ruf, Sebastian Halder, Michael Bensch y Andrea Kubler. 2010. Diseño e implementación de una interfaz cerebro-ordenador basada en P300 para controlar un navegador de Internet. *IEEE Trans. Neural Syst. Rehab. Eng.* 18, 6 (dic. 2010), 599-609.

[116] Elon Musk y Neuralink. 2019. Una plataforma integrada de interfaz cerebro-máquina con miles de . *bioRxiv* (2019). Obtenido de arXiv:https://www.biorxiv.org/content/early/2019/08/02/703801.full.pdf.
[117] NeuroPace. 2013. Manual del paciente de NeuroPace® RNS® System. Obtenido de https://www.accessdata.fda.gov/cdrh_ docs/pdf10/p100026c.pdf.
[118] NeuroSky. 2019. NeuroSky. Obtenido de http://neurosky.com/.
[119] Miguel A. L. Nicolelis. 2001. Acciones a partir de pensamientos. *Nature* 409, 6818 (2001), 403-407.
[120] NIST. 2018. Marco de ciberseguridad. Obtenido de https://www.nist.gov/cyberframework.
[121] Abdulmalik Obaid, Mina-Elraheb Hanna, Yu-Wei Wu, Mihaly Kollo, Romeo Racz, Matthew R. Angle, Jan Müller, Nora Brackbill, William Wray, Felix Franke, E. J. Chichilnisky, Andreas Hierlemann, Jun B. Ding, Andreas T. Schaefer y Nicholas A. Melosh. 2020. Massively parallel microwire arrays integrated with CMOS chips for neural recording. *Sci. Adv.* 6, 12 (2020). Obtenido de arXiv:https://advances.sciencemag.org/content/6/12/eaay2789.full. pdf.
[122] Joseph E. O'Doherty, Mikhail A. Lebedev, Peter J. Ifft, Katie Z. Zhuang, Solaiman Shokur, Hannes Bleuler y Miguel A. L. Nicolelis. 2011. Exploración táctil activa mediante una interfaz cerebro-máquina-cerebro. *Nature* 479, 7372 (nov. 2011), 228-231.
[123] Proyecto abierto de seguridad de las aplicaciones web. 2017. Top 10-2017 A6-Security Misconfiguration-OWASP. Obtenido de https://www.owasp.org/index.php/Top_10-2017_A6-Security_Misconfiguration.
[124] Proyecto abierto de seguridad de las aplicaciones web. 2017. Top 10-2017 Top 10-OWASP. Obtenido de https://www.owasp.org/ index.php/Top_10-2017_Top_10.
[125] Proyecto abierto de seguridad de aplicaciones web. 2018. Proyecto OWASP sobre el Internet de las cosas. Obtenido de https://www. owasp.org/index.php/OWASP_Internet_of_Things_Project.
[126] Miguel Pais-Vieira, Gabriela Chiuffa, Mikhail Lebedev, Amol Yadav y Miguel A. L. Nicolelis. 2015. Construcción de un dispositivo informático orgánico con múltiples cerebros interconectados. *Sci. Rep.* 5, 1 (dic. 2015), 11869.
[127] Miguel Pais-Vieira, Mikhail Lebedev, Carolina Kunicki, Jing Wang y Miguel A. L. Nicolelis. 2013. Una interfaz cerebro-cerebro para compartir información sensoriomotora en tiempo real. *Sci. Rep.* 3, 1 (dic. 2013), 1319.
[128] Mahboubeh Parastarfeizabadi y Abbas Z. Kouzani. 2017. Avances en dispositivos de estimulación cerebral profunda de bucle cerrado.
J. NeuroEngineer. Rehab. 14, 1 (ago. 2017), 79.
[129] Rafael Polanía, Michael A. Nitsche y Christian C. Ruff. 2018. Estudiando y modificando la función cerebral con estimulación cerebral no invasiva. *Nature Neurosci.* 21, 2 (feb. 2018), 174-187.
[130] Riccardo Poli, Caterina Cinel, Ana Matran-Fernández, Francisco Sepúlveda y Adrian Stoica. 2013. Towards coop- erative brain-computer interfaces for space navigation. En *Proceedings of the International Conference on Intelligent User Interfaces (IUI'13)*. ACM Press, Nueva York, 149.
[131] Riccardo Poli, Davide Valeriani y Caterina Cinel. 2014. Interfaz cerebro-ordenador colaborativa para ayudar a la toma de decisiones. *PLoS ONE* 9, 7 (julio de 2014), 22.
[132] Mu-ming Poo, Jiu-lin Du, Nancy Y. Ip, Zhi-Qi Xiong, Bo Xu y Tieniu Tan. 2016. China brain project: Neurociencia básica, enfermedades cerebrales y computación inspirada en el cerebro. *Neuron* 92, 3 (nov. 2016), 591-596.
[133] Proyecto cerebro humano. 2019. Proyecto cerebro humano. Obtenido de https://www.humanbrainproject.eu/en/.
[134] Proyecto abierto de seguridad de las aplicaciones web. 2017. Top 10-2017 A1-Injection-OWASP. Obtenido de https://www. owasp.org/index.php/Top_10-2017_A1-Injection.
[135] Laurie Pycroft y Tipu Z. Aziz. 2018. Seguridad de dispositivos médicos implantables con conexiones inalámbricas: Los dan- gers de los ciberataques. *Expert Rev. Med. Devices* 15, 6 (julio de 2018), 403-406.
[136] Laurie Pycroft, Sandra G. Boccard, Sarah L.F. Owen, John F. Stein, James J. Fitzgerald, Alexander L. Green y Tipu Z. Aziz. 2016. Secuestro cerebral: Problemas de seguridad de los implantes en la neuromodulación invasiva. *World Neurosurg.* 92 (ago. 2016), 454-462.
[137] Rabie A. Ramadan y Athanasios V. Vasilakos. 2017. Interfaz cerebro ordenador: Revisión de señales de control. *Neurocom- put.* 223 (Feb. 2017), 26-44.
[138] Arjun Ramakrishnan, Peter J. Ifft, Miguel Pais-Vieira, Yoon Woo Byun, Katie Z. Zhuang, Mikhail A. Lebedev y Miguel A.L. Nicolelis. 2015. Computación de los movimientos del brazo con un mono Brainet. *Sci. Rep.* 5, 1 (Sep. 2015), 10767.
[139] Rajesh P. N. Rao. 2019. Hacia coprocesadores neuronales para el cerebro: Combinando decodificación y codificación en interfaces cerebro-ordenador. *Curr. Opin. Neurobiol.* 55 (abr. 2019), 142-151.
[140] Rajesh P. N. Rao, Andrea Stocco, Matthew Bryan, Devapratim Sarma, Tiffany M. Youngquist, Joseph Wu y Chantel S. Prat. 2014. Una interfaz directa cerebro-cerebro en humanos. *PLoS ONE* 9, 11 (nov. 2014), e111332.
[141] Heena Rathore, Chenglong Fu, Amr Mohamed, Abdulla Al-Ali, Xiaojiang Du, Mohsen Guizani y Zheng- tao Yu. 2020. Esquema de seguridad multicapa para dispositivos médicos implantables. *Neural Comput. Appl.* 32, 9 (2020), 4347-4360.
[142] Rodrigo Román, Javier López y Masahiro Mambo. 2018. Mobile edge computing, Fog et al: Un estudio y análisis de las amenazas y desafíos de seguridad. *Future Gen. Comput. Syst.* 78 (enero de 2018), 680-698.

[143] Ron Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau y Rosalie McQuaid. 2019. *Desarrollo de sistemas ciberresilientes: Un enfoque de ingeniería de seguridad de sistemas*. Technical Report. National Institute of Standards and Technology. Obtenido de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf.

[144] W. Saad, M. Bennis y M. Chen. 2019. Una visión de los sistemas inalámbricos 6G: Aplicaciones, tendencias, tecnologías y problemas de investigación abiertos. *IEEE Netw.* (2019), 1-9.

[145] Abdul Saboor, Felix Gembler, Mihaly Benda, Piotr Stawicki, Aya Rezeika, Roland Grichnik e Ivan Volosyak. 2018. Un deletreador web BCI basado en SSVEP impulsado por navegador. En *las actas de la Conferencia Internacional del IEEE sobre Sistemas, Hombre y Cibernética (SMC'18)*. IEEE, Miyazaki, Japón, 625-630.

[146] Abdul Saboor, Aya Rezeika, Piotr Stawicki, Felix Gembler, Mihaly Benda, Thomas Grunenberg e Ivan Volosyak. 2017. BCI basado en SSVEP en un escenario doméstico inteligente. En *Actas de la conferencia internacional de trabajo sobre redes neuronales artificiales*. Springer, Cham, 474-485.

[147] Takamichi Saito, Ryohei Watanabe, Shuta Kondo, Shota Sugawara y Masahiro Yokoyama. 2016. A survey of prevention/mitigation against memory corruption attacks. En *Actas de la 19ª Conferencia Internacional sobre Sistemas de Información basados en Redes (NBiS'16)*. IEEE, 500-505.

[148] Parthana Sarma, Prakash Tripathi, Manash Pratim Sarma y Kandarpa Kumar Sarma. 2016. Técnicas de preprocesamiento y extracción de características para aplicaciones EEG-BCI-Una revisión de la investigación reciente. *ADBU-J. Eng. Technol.* 5 (2016), 2348-7305.

[149] M. A. Scholl, K. M. Stine, J. Hash, P. Bowen, L. A. Johnson, C. D. Smith y D. I. Steinberg. 2008. *An Intro- ductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Secu- rity* Rule. Technical Report. National Institute of Standards and Technology, Gaithersburg, MD. Obtenido de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf.

[150] Suzanne B. Schwartz. 2018. Ciberseguridad de dispositivos médicos a través de la lente de la FDA. En *Actas del 27º Simposio de Seguridad de USENIX*. Asociación USENIX, Baltimore, MD.

[151] Boston Scientific. 2020. Información sobre la seguridad de los productos. Obtenido de https://www.bostonscientific.com/en-US/ customer-service/product-security/product-security-information.html.

[152] Diego Sempreboni y Luca Viganò. 2018. Privacidad, seguridad y confianza en el Internet de las neuronas. Obtenido de https://arxiv:cs.CY/1807.06077.

[153] Reza Shokri, Marco Stronati, Congzheng Song y Vitaly Shmatikov. 2017. Ataques de inferencia de membresía contra modelos de aprendizaje automático. En *Actas del Simposio del IEEE sobre seguridad y privacidad*. IEEE, 3-18.

[154] S. Sibi Chakkaravarthy, D. Sangeetha y V. Vaidehi. 2019. A Survey on malware analysis and mitigation techniques. *Comput. Sci. Rev.* 32 (mayo de 2019), 23.

[155] Saurabh Singh, Young-Sik Jeong y Jong Hyuk Park. 2016. Estudio sobre la seguridad de la computación en nube: Problemas, amenazas y soluciones. *J. Netw. Comput. Appl.* 75 (nov. 2016), 200-222.

[156] José L. Sirvent, José M. Azorín, Eduardo Iáñez, Andrés Úbeda y Eduardo Fernández. 2010. Interfaz cerebro-ordenador basada en P300 para la navegación por Internet. En *Trends in Practical Applications of Agents and Multiagent* Systems. Springer, Berlín, 615-622.

[157] Sociedad Internacional de Neuromodulación. 2020. Sociedad Internacional de Neuromodulación. Obtenido de https://www. neuromodulation.com/.

[158] Kandhasamy Sowndhararajan, Minju Kim, Ponnuvel Deepa, Se Park y Songmun Kim. 2018. Aplicación del potencial relacionado con eventos P300 en el diagnóstico del trastorno epiléptico: Una revisión. *Scientia Pharmaceutica* 86, 2 (mar. 2018), 10.

[159] William Stallings. 2017. *Criptografía y seguridad de redes: Principles and Practice* (7ª ed.). Pearson, Londres, 766 páginas.

[160] Ioannis Stellios, Panayiotis Kotzanikolaou, Mihalis Psarakis, Cristina Alcaraz y Javier López. 2018. Un estudio de los ciberataques habilitados para IoT: Evaluando las rutas de ataque a infraestructuras y servicios críticos. *IEEE Commun. Surveys Tutor.* 20, 4 (2018), 3453-3495.

[161] Andrea Stocco, Chantel S. Prat, Darby M. Losey, Jeneva A. Cronin, Joseph Wu, Justin A. Abernethy y Rajesh P. N. Rao. 2015. Jugando a 20 preguntas con la mente: Resolución colaborativa de problemas por humanos usando una interfaz cerebro-cerebro. *PLoS ONE* 10, 9 (septiembre de 2015), e0137303.

[162] Estrategia canadiense de investigación sobre el cerebro. 2019. Estrategia canadiense de investigación del cerebro. Obtenido de https://canadianbrain. ca/.

[163] Kaushik Sundararajan. 2017. *Cuestiones de privacidad y seguridad en la interfaz cerebro-ordenador*. Tesis de máster. Tecnológica de Auckland.

[164] Hassan Takabi. 2016. Cortafuegos para el cerebro: Hacia un ecosistema de preservación de la privacidad para aplicaciones BCI. En *Proceedings of the IEEE Conference on Communications and Network Security (CNS'16)*. IEEE, 370-371.

[165] Hassan Takabi, Anuj Bhalotiya y Manar Alohaly. 2016. Aplicaciones de interfaz cerebro-ordenador (BCI): Amenazas a la privacidad y contramedidas. En *Proceedings of the IEEE 2nd International Conference on Collaboration and Internet Computing*. IEEE, 102-111.

[166] Andrew S. Tanenbaum y David J. Wetherall. 2011. *Computer Networks* (5ª ed.). Pearson, Londres.
[167] William J. Tyler, Joseph L. Sanguinetti, Maria Fini y Nicholas Hool. 2017. Estimulación neural no invasiva. In *Micro- and Nanotechnology Sensors, Systems, and Applications IX*, Thomas George, Achyut K. Dutta, and M. Saif Islam (Eds.), Vol. 10194. International Society for Optics and Photonics, Anaheim, CA, 280-290.
[168] Administración de Alimentos y Medicamentos de los Estados Unidos. 2016. *Gestión posterior a la comercialización de la ciberseguridad en dispositivos médicos*. Technical Report. U.S. Food and Drug Administration, Rockville, MD.
[169] Administración de Alimentos y Medicamentos de los Estados Unidos. 2018. *Contenido de las Presentaciones Previas a la Comercialización para la Gestión de la Ciberseguridad en Dispositivos Médicos*. Technical Report. U.S. Food and Drug Administration, Rockville, MD.
[170] Satish Vadlamani, Burak Eksioglu, Hugh Medal y Apurba Nandi. 2016. Ataques de interferencia en redes inalámbricas: Un estudio taxonómico. *Int. J. Prod. Econ.* 172 (feb. 2016), 76-94.
[171] Swati Vaid, Preeti Singh y Chamandeep Kaur. 2015. Análisis de la señal EEG para la interfaz BCI: A review. En *Actas de la Conferencia Internacional sobre Informática Avanzada y Tecnologías de la Comunicación (ACCT'15)*. IEEE, 143-147.
[172] Marcel van Gerven, Jason Farquhar, Rebecca Schaefer, Rutger Vlek, Jeroen Geuze, Anton Nijholt, Nick Ramsey, Pim Haselager, Louis Vuurpijl, Stan Gielen y Peter Desain. 2009. El ciclo de la interfaz cerebro-ordenador. *J. Neural Eng.* 6, 4 (ago. 2009), 041001.
[173] Sebastian Vasile, David Oswald y Tom Chothia. 2019. Rompiendo todas las cosas-Una encuesta sistemática de técnicas de extracción de firmware para dispositivos IoT. En *Investigación de tarjetas inteligentes y aplicaciones avanzadas*. Springer, Cham, 171-185.
[174] T. M. Vaughan, D. J. Mcfarland, G. Schalk, W. A. Sarnacki, D. J. Krusienski, E. W. Sellers y J. R. Wolpaw. 2006. Programa de investigación y desarrollo de la BCI de Wadsworth: At home with BCI. *IEEE Trans. Neural Syst. Rehab. Eng.* 14, 2 (junio de 2006), 229-233.
[175] Ainuddin Wahid Abdul Wahab, Mustapha Aminu Bagiwa, Mohd Yamani Idna Idris, Suleman Khan, Zaidi Razak y Muhammad Rezal Kamel Ariffin. 2014. Técnicas pasivas de detección de falsificaciones de vídeo: A survey. En *Proceedings of the 10th International Conference on Information Assurance and* Security. IEEE, 29-34.
[176] Yijun Wang y Tzyy-Ping Jung. 2011. Una interfaz cerebro-ordenador colaborativa para mejorar el rendimiento humano. *PLoS ONE* 6, 5 (mayo de 2011), e20422.
[177] Ping Yan y Zheng Yan. 2018. Un estudio sobre la detección dinámica de malware móvil. *Softw. Qual. J.* 26, 3 (sep. 2018), 891-919.
[178] T. Yaqoob, H. Abbas y M. Atiquzzaman. 2019. Vulnerabilidades de seguridad, ataques, contramedidas y regulaciones de dispositivos médicos en red-Una revisión. *IEEE Commun. Surveys Tutor.* 21, 4 (2019), 3723-3768.
[179] Seung-Schik Yoo, Hyungmin Kim, Emmanuel Filandrianos, Seyed Javid Taghados y Shinsuk Park. 2013. Interfaz cerebro-cerebro (BBI) no invasiva: Estableciendo vínculos funcionales entre dos cerebros. *PLoS ONE* 8, 4 (abr. 2013), e60410.
[180] Tianyou Yu, Yuanqing Li, Jinyi Long y Zhenghui Gu. 2012. Navegando por Internet con un ratón BCI. *J. Neural Eng.* 9, 3 (junio de 2012), 036012.
[181] Peng Yuan, Yijun Wang, Xiaorong Gao, Tzyy-Ping Jung y Shangkai Gao. 2013. A collaborative brain-computer interface for accelerating human decision making. En *Proceedings of the International Conference on Universal Access in Human-Computer Interaction*. Springer, Berlín, 672-681.
[182] Lan Zhang, Ker Jiun Wang, Huan Chen y Zhi Hong Mao. 2016. Internet del cerebro: Decodificación de la intención humana y acoplamiento de señales EEG con servicios de Internet. En *Actas de la Conferencia Internacional sobre Ciencia de los Servicios (ICSS'16)*. IEEE, 172-179.
[183] PeiYun Zhang, MengChu Zhou y Giancarlo Fortino. 2018. Problemas de seguridad y confianza en la computación Fog: A survey.
Futura Gen. Comput. Syst. 88 (nov. 2018), 16-27.
[184] Shaomin Zhang, Sheng Yuan, Lipeng Huang, Xiaoxiang Zheng, Zhaohui Wu, Kedi Xu y Gang Pan. 2019. Control mental humano de la locomoción continua de la rata Cyborg con interfaz inalámbrica cerebro-cerebro. *Sci. Rep.* 9, 1 (dic 2019), 1321.
[185] Xiang Zhang, Lina Yao, Shuai Zhang, Salil Kanhere, Michael Sheng y Yunhao Liu. 2019. Internet de las cosas se encuentra con la interfaz cerebro-ordenador: Un marco unificado de aprendizaje profundo para permitir la interactividad cognitiva humano-cosa. *IEEE Internet Things J.* 6, 2 (abr. 2019), 2084-2092.
[186] Yulong Zou, Jia Zhu, Xianbin Wang y Lajos Hanzo. 2016. Estudio sobre la seguridad inalámbrica: Desafíos técnicos, avances recientes y tendencias futuras. *Proc. IEEE* 104, 9 (Sep. 2016), 1727-1765.

Recibido en noviembre de 2019; revisado en agosto de 2020; aceptado en septiembre de 2020