Sistemas interfaces cerebro-computador (BCI): amenazas y ataques cibernéticos

Brain-Computer Interfaces (BCIs): Threats and Cyber Attacks

Juan Camilo Ospina-Cuervo[1]
Héctor Fernando Vargas Montoya[2]

DOI: https://doi.org/10.18041/1909-2458/ingeniare.33.9733

RESUMEN

La interface cerebro computador (BCI, por su sigla en inglés) es una tecnología con la cual se pueden adquirir y procesar los valores obtenidos de señales cerebrales, con el objeto de pasarlos a dispositivos finales para que interactúen de acuerdo con lo dispuesto por el cerebro. En el proceso tecnológico se pueden tener ataques y vulnerabilidades de ciberseguridad, como la negación del servicio, robo o alteración de información, que hacen del sistema un elemento vulnerable, permitiendo eventos que están fuera del control de los usuarios finales o de los administradores. El objetivo de este artículo es presentar los riesgos de seguridad que pueden afectar la información sobre las interfaces cerebro computador (BCI) locales y ofrecer una propuesta para controlar las vulnerabilidades encontradas en un ambiente de investigación. Como resultado se obtuvieron una serie de riesgos que pueden impactar la disponibilidad, integridad o confidencialidad de los datos procesados en el sistema, así como un grupo de controles.

Palabras claves: Ciberataques, gestión de riesgo, interfaces cerebro computador, sistema BCI, vulnerabilidad.

ABSTRACT

The Brain-Computer Interfaces-BCI, is a technology with which the different values obtained from brain signals can be acquired and processed in order to later pass them to final devices so that they interact according to what is arranged by the brain. Within the technological process, can have vulnerabilities and cybersecurity attacks such as denial of service, theft or alteration of information, making the system a vulnerable element, which can allow events that are beyond the control of end users or administrators. This article's objective is to present the security risks that may affect information on local Brain Computer Interfaces (BCI) and to offer a proposal on how the vulnerabilities found in a research environment could be controlled. As a result, a series of risks were obtained that can impact the availability, integrity or confidentiality of the data processed in the system, as well as a group of controls.

Keywords: Brain Computer Interfaces, Cyberattacks, Risk Management, BCI System, Vulnerability

Cómo citar este artículo: J. Ospina Cuervo and H. Vargas Montoya. "Sistemas interfaces cerebro-computador (BCI): amenazas y ataques cibernéticos". Ingeniare, vol. 19, no. 33, pp. 41-52, Diciembre 2022.

1 Candidato a Magíster en seguridad informática, Ingeniero de telecomunicaciones del Instituto Tecnológico Metropolitano, ITM, Medellín. jotaccuervo@gmail.com; juanospina87600@correo.itm.edu.co. ORCID: 0000-0002-4629-023X7
2 Msc. en seguridad TIC, Ingeniero de sistemas del Instituto Tecnológico Metropolitano, ITM, Medellín. hvargasm@gmail.com; hectorvargas@itm.edu.co. ORCID: 0000-0002-0861-2883

Fecha de recepción: 13 de diciembre del 2021 • Fecha de aceptación: 1 de junio del 2022

1. INTRODUCCIÓN

La identificación de un riesgo está ligada a determinar la probabilidad de ocurrencia de un evento de ciberseguridad sobre una vulnerabilidad y el impacto que pueda generar. Para ello, se cuenta con modelos conceptuales de análisis que proveen una guía para establecer las características con las cuales se pueden determinar los eventos adversos a los que se pueden exponer los sistemas. Para reducir los posibles riesgos es importante contar con directrices donde la privacidad y el cuidado de la información sea indispensable, así como la definición de mecanismos para la toma de decisiones frente a un ataque de seguridad.

Considerando que la interface cerebro computador BCI (*Brain Computer Interfaces*) es una tecnología a través de la cual pasa y se procesa información personal o de sumo cuidado para la toma de decisiones en el sector de la medicina, la investigación, los videojuegos y la productividad, se requieren elementos que permitan reducir los posibles riesgos que pongan en peligro el sistema y los datos de los pacientes y usuarios finales [1], [3].

Esta tecnología monitorea las señales electroencefálicas (ondas electromagnéticas producidas por el cerebro) que se implementa en el sistema BCI, una vez se capturan los datos se deben llevar a un dispositivo de salida que está ligado a un conjunto de herramientas tecnológicas, equipos o programas que recopilan la información procedente del sistema cerebro computador. Estos dispositivos pueden ser celulares, tabletas, computadores, prótesis motoras o robotizadas, brazos robóticos y algunas interfaces ligadas al manejo de equipos, permitiendo a los usuarios controlarlos a través de las señales cerebrales. Dicha información puede estar almacenada de manera local en un equipo de cómputo o celulares, o de manera remota utilizando bases de datos que se encuentran en la nube para el uso de los usuarios de los sistemas BCI. Por esta razón, el manejo de la información local o en tránsito en la red de comunicación puede ser vulnerable a ataques informáticos que atentan contra su confidencialidad (develación de datos personales), disponibilidad (no acceso al sistema) o integridad (modificación no autorizada). En ese sentido es necesario disponer de información fiable y relevante sobre las condiciones de los dispositivos finales y facilitar la conexión a los usuarios de la tecnología BCI. Por esto es fundamental contar con mecanismos o procesos que permitan establecer un nivel de seguridad para proteger la información y los datos procesados [1], [12], [13].

1.1 Componentes de un sistemas BCI

Para la adquisición de los datos se pueden utilizar programas como el Sistema Electroencefalógrafo (EEG), Emotiv G y Sistema EEG Neurosky Mindset, que toman muestras de datos de manera externa en el cráneo y no requieren procedimiento quirúrgico para su instalación y uso. Estos son sistemas comerciales que se utilizan en el mercado. Por otro lado, se encuentran los sistemas BCI interno,

que son pequeños chips que instala un especialista de manera quirúrgica en el interior del cráneo del paciente. Igual que los dispositivos externos, recogen las señales producidas por el cerebro y las envía a dispositivos finales y aplicaciones, teniendo niveles más altos y fiabilidad en la recolección de los datos. Comercialmente se encuentran referencias como Neuralink [64].

Estos dispositivos recogen la señal y la envía a un instrumento cercano a través de medios de transmisión como Bluetooh, WiFi o conexiones cableadas hacia un dispositivo que recopila la información, la procesa, extrae sus características y la clasifica (datasets). En este sistema se cumplen varios procesos en el que los datos se filtran de manera que puedan identificar patrones y estímulos que produce el usuario [1], [13], [19]. Posteriormente, el sistema BCI envía la información procesada a los dispositivos de salida que están ligados a un conjunto de herramientas tecnológicas, equipo o programas. Estos dispositivos pueden ser celulares, tabletas, computadores, prótesis motoras y robotizadas como sillas de ruedas o brazos robóticos, así como interfaces ligadas al manejo de automóviles [3}, [13].

Un sistema BCI consta al menos de tres etapas que permiten el funcionamiento del sistema (Figura 1).

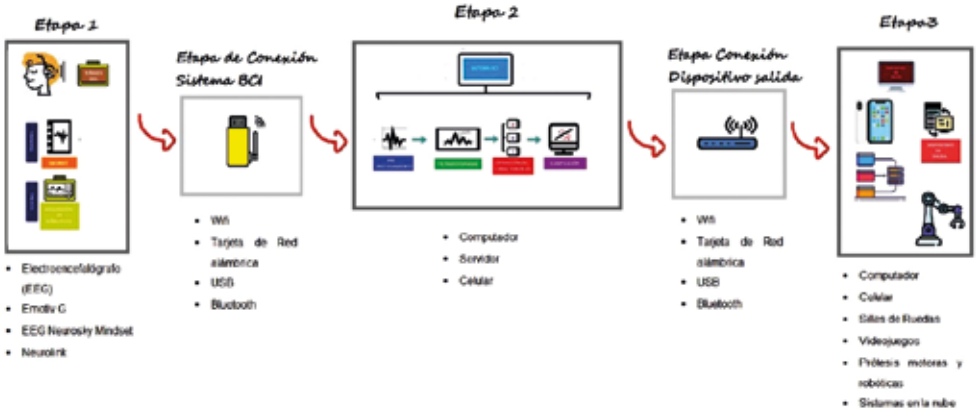

Figura 1. Componentes de un sistema BCI.

Fuente: Elaboración propia.

En la etapa 1 se capturan y digitalizan las señales. En este caso el sujeto se conecta a un electroencefalógrafo (EEG), luego se le presentan ciertas imágenes con el fin de que imagine cómo realizaría el movimiento o la actividad que se le está mostrando [1], [12], [13]. Luego, a través de algún sistema de comunicaciones se envían los datos.

En la etapa 2 se hace el preprocesamiento, cuya función principal es filtrar el ruido producido por artefactos u otras acciones no propias de la actividad, debido a que en la fase 1, por el tipo de componentes que se utilizan, se puede generar distorsión o pérdida en la señal, lo cual opaca las

señales que genera el cerebro para su interacción y se requiere obtener toda la información relevante posible [2]. Por otra parte, este tipo de dispositivos pueden ser víctimas de ataques de malware para el firmware que pueden cifrar los datos del equipo, cambiando sus configuraciones de fábrica y los códigos fuente, las firmas digitales para la conexión con los dispositivos finales y las aplicaciones, así como su cifrado, imposibilitando su funcionamiento y compilando información del equipo en segundo plano. En esta etapa también se clasifica el sistema BCI, identificando y reconociendo patrones de las actividades del EEG, recopilando las señales y asociándolas a las tareas mentales [3].

Finalmente, en la etapa 3 se recogen los datos y se llevan a un dispositivo de salida en el que se recopila la información procedente del sistema cerebro-computador para su interacción final [13].

1.2 Ataques informáticos sobre los componentes BCI

Teniendo en cuenta las diversas tecnologías e información que utilizan y generan los sistemas BCI, las amenazas informáticas se pueden presentar de diferentes formas. Algunas de estas amenazas aplican igualmente a otros sistemas tecnológicos, pero tienen relevancia para esta investigación, toda vez que pueden generar impactos negativos afectando el *hardware* y el *software*. Dichos ataques son:

- *Man in the Middle.* Este ataque consiste en capturar las comunicaciones que hay entre dos equipos o sistemas, escuchando, modificando o redireccionando los datos que cursan [10].
- ARP Spoofing. Este ataque modifica las tablas ARP (falsificación), permitiendo que un tercero pueda capturar los datos que circulan por la red [6].
- Códigos maliciosos (malware). *Software* construido para fines malintencionados. Entre sus funciones se encuentra el robo de datos, alteración de sistemas, bloqueo, cifrado y solicitud de rescate [4].
- Robo o alteración de información. En este caso, a través de alguna vulnerabilidad el atacante podría extraer información de las bases de datos o de los sistemas de almacenamiento. Así mismo, podría inyectar algún código para alterar información y dañar el sistema.
- SQL injection.: En consideración de la posibilidad de tener bases de datos para el almacenamiento final de la información, este ataque permite, a través de sentencias de tipo SQL, extraer, modificar o borrar datos e información almacenada [15].
- Denegación de servicios (DoS). La negación de servicio se puede presentar de diversas formas. La más común es el alto consumo de recursos, como el ancho de banda, CPU o memoria. También se puede presentar cuando se elimina o modifica algún archivo de configuración. El objetivo final es no entregar el servicio a los sistemas o personas que requieren el acceso [5].
- Inyección de código. Esto se puede realizar a sistemas y lenguajes de programación permitiendo la inyección de código a las aplicaciones, lo cual genera una pérdida potencial del funcionamiento u otras funcionalidades no previstas en la construcción inicial de las aplicaciones [7].

2. METODOLOGÍA

Para la obtención de los resultados se ejecutaron las siguientes fases (Figura 2):

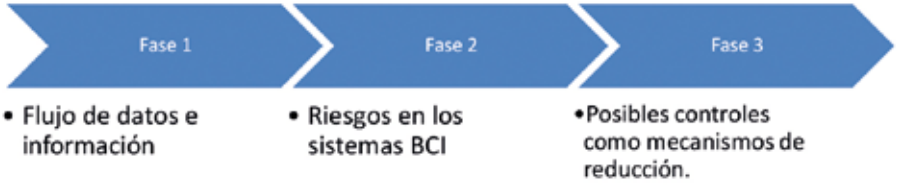

Figura 2. Metodología que se siguió para la obtención de resultados.

Fuente: Elaboración propia.

En la Fase 1 se identificaron las características de los datasets que se desprenden de la recopilación de datos, como su origen, clase y etiquetados, lo cual brinda información sobre un sistema BCI. Para esto fue necesario conocer el posible flujo de datos que se genera en las etapas del sistema y conocer un poco más la tecnología y sus componentes. Respecto a la Fase 2, partiendo de los datos e información que fluye a través del sistema, junto con las amenazas informáticas, se obtiene un mapa de riesgos que se realiza en una matriz 3x3 para efectos prácticos, iniciando con un levantamiento de activos de información asociados a un BCI; luego se hace una revisión de las posibles amenazas y vulnerabilidades, obteniendo los riesgos; seguidamente, cada riesgo se califica dependiendo de la probabilidad de ocurrencia e impacto que puede generar si se consolida.

Finalmente, se obtiene un mapa de riesgos con tres zonas de impacto (Figura 3): Alto (c), Medio (b) y Bajo (a). De esa forma es más fácil entender los niveles de impacto [11].

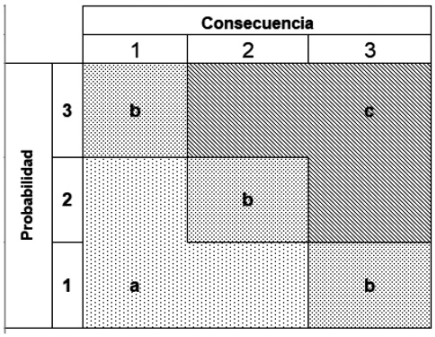

Figura 3. Mapa de riesgos de 3x3 usado para el cálculo final.

Fuente: Elaboración propia.

Para calcular los riesgos, con base en la matriz 3x3, la probabilidad de ocurrencia va de 1 a 3, siendo 1 la menor probabilidad y 3 la mayor. De manera similar se hace parar calcular la consecuencia o impacto (1 es el menor impacto y 3 el mayor).

Por último, se generan recomendaciones de protección que buscan reducir los posibles riesgos sobre los sistemas BCI. Estas recomendaciones se asocian directamente con los riesgos encontrados (amenazas que explotan vulnerabilidades sobre los activos identificados en un BCI) en las zonas media y alta, considerando lo riesgos bajos como aquellos que pueden ser asumidos, y se califican en probabilidad e impacto en el mapa de riesgos (Figura 3).

3. RESULTADOS Y DISCUSIÓN

3.1 Flujo de datos e información

La adquisición de datos se toma por señales electromagnéticas, en las que sus frecuencias y potencias se digitalizan por medio de sensores fijados en la cabeza, tomando las muestras desde la corteza cerebral del sujeto conectado al sistema BCI [1], [12], [19]. Allí, estas corrientes iónicas se convierten a impulsos eléctricos [3], [13]. Esta información la envían los dispositivos de comunicación utilizando ondas de radio para transmitir en cortas distancias.

Finalmente, los datos de entrenamiento se guardan en el servidor para realizar pruebas y procesos del BCI. Por su parte, la información de salida se envía a través de dispositivos de comunicación a los equipos cercanos, donde están los aplicativos que los controlan para que el usuario final pueda utilizar el sistema BCI. Las bases de datos que se generan en la interface se recopilan y se guardan en el servidor, ya sea local o en la nube [8].

3.2 Análisis de riesgos

Para el flujo de datos y los activos relacionados en las fases, el proceso de riesgos establece que se deben buscar las posibles amenazas y vulnerabilidades, indicando la probabilidad de ocurrencia y el impacto que pueden generar [15]. Al final, la consolidación de los riesgos en una matriz permite visualizar los posibles impactos en todo el sistema BCI a través de las fases. La norma ISO 27005:2018 indica que la matriz de riesgos debe ser de 5x5, lo cual la hace más completa a la hora de tomar una decisión respecto a los niveles de exposición de los riesgos. Para este caso de estudio se optó por una matriz 3x3 (como se indicó en la metodología).

De acuerdo con el flujo de información, para el análisis de riesgos se ejecutan los siguientes pasos: a) inventario de activos, b) amenazas y vulnerabilidades, c) construcción del escenario de riesgos, d) calificación de probabilidad e impacto y e) obtención del mapa de riesgos.

Se inicia, entonces, con los activos de información, que son claves y están relacionados con cada una de las fases y el flujo de información. Los siguientes son los activos más relevantes: Sistema EEG,

Protocolos WiFi y bluetooth, lenguaje de programación, página web, base de datos, almacenamiento local o nube y personas.

Respecto a las amenazas y vulnerabilidades, se tomaron las ya definidas: *Man in the Middle*, ARP Spoofing, códigos maliciosos (malware), robo o alteración de información, SQL injection, denegación de servicios (DoS) e inyección de códigos. Adicionalmente, está la ingeniería social, que es una amenaza asociada a las personas. Dichas amenazas tienen la posibilidad de explotar vulnerabilidades como la falta de parches, falencia en el control de acceso, falla en el flujo de datos, falencia en el monitoreo, no capacitación, no identificación de procesos o personas accediendo, entre otras (Tabla 1).

Tabla 1. Escenarios de riesgos.

ACTIVOS AMENAZAS	Electroencefalograma	Emotiv G	EEG Neurosky Mindset	Tarjeta de red Inalámbrica	Bluetooth	Neuralink	Celular	Computador	Sistema en la nube	Servidor
Ataque informático de tipo: SQL injection							x	x	x	x
Ataque informático de tipo: DoS/ DDoS	x	x	x	x	x	x	x	x	x	x
Ataque informático de tipo: Ransomware							x	x	x	x
Ataque de tipo: ingeniería social							x	x	x	x
Ataque informático de tipo: rompimiento de cifrado o llaves criptográficas.							x	x	x	x
Ataque informático de tipo: the man in the middle	x	x	x	x	x	x	x	x	x	x
Ataque informático de tipo: Spoofing: de MAC, IP, ARP o cualquier servicio		x	x	x	x	x				
Ataque informático de tipo: scanning							x	x	x	x
Ataque informático de tipo: Exploit	x	x	x	x	x	x	x	x	x	x

Fuente: Elaboración propia.

Una vez revisados los escenarios de riesgos se estableció el panorama, consolidando 17 amenazas (Tabla 2), los cuales se calificaron de acuerdo con la probabilidad e impacto:

Nota: los dispositivos finales no se consideraron, debido a que existe una gama muy amplia, como PC, juegos, robot, brazos mecánicos, IoT, etc., y los riesgos pueden ser demasiados.

Tabla 2. Cálculo de los escenarios de riesgos y su respectiva calificación.

No.	Escenario de riesgos
(1) (2)	Posibilidad que la amenaza Man in the Middle o ARP Spoofing afecte el activo: protocolos Wifi y bluetooth, página Web
(3)(4)(5)	Posibilidad que la amenaza códigos maliciosos (malware) afecte el activo: Sistema EEG, bases de datos, almacenamiento
(6)(7)	Posibilidad que la amenaza robo o alteración de información afecte el activo: almacenamiento local o nube, personas
(8)(9)(10)	Posibilidad que la amenaza SQL injection o inyección de código afecte el activo: lenguaje de programación, página web y BD
(11)(12) (13) (14) (15)(16)	Posibilidad que la amenaza denegación de servicios (DoS) afecte el activo: Sistema EEG, Wifi y bluetooth, lenguaje de programación, página web, BD, almacenamiento.
(17)	Posibilidad que la amenaza ingeniería social afecte el activo: personas

Fuente: Elaboración propia.

Luego de realizar la calificación en términos de probabilidad e impacto se obtuvo el siguiente mapa de riesgos (Figura 4):

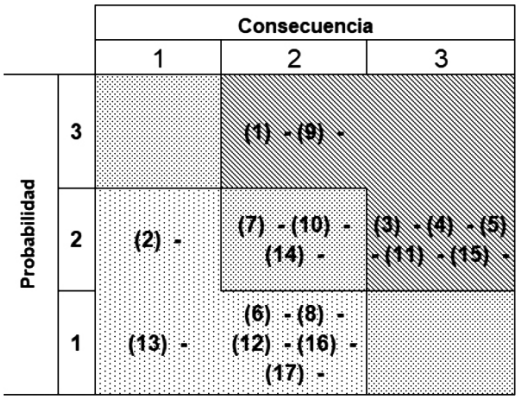

Figura 4. Mapa de riesgos final.

Fuente: Elaboración propia.

Como se puede observar, siete riesgos quedaron en la zona más baja, mientras que los diez restantes en las zonas media y alta. En ese sentido, es necesario establecer un plan de tratamiento para los riesgos altos, que permita o posibilite la reducción de sus niveles de impactos. En los riesgos altos se destacan los ataques de “Hombre en el medio”, “Malware” y “negación de servicio”, mientras que en la zona sobresalen el “robo de información” y la “inyección de código”.

3.3 Propuesta de controles

De acuerdo con las etapas del sistema BCI y con base a los riesgos encontrados se definen los siguientes controles:

i. Adquisición de las señales

Controles: 1) Verificación de seguridad por firmas y Hash para autenticación al sistema. 2) Actualización de firmware de sistema de recolección de señales EEG. 3) Cifrado de información.

ii. Conexión sistema BCI

Controles: 1) Cifrado en redes LAN. 2) Cifrado en bluetooth con LE Secare Connections, con los algoritmos ECDH. 3) Verificación de seguridad a dispositivos por medio de pines y NFC (Near Field Communication).

iii. Procesamiento de datos

Controles: 1) Verificación de seguridad a servidores por medio de pines y doble autenticación. 2) Cifrado de comunicaciones HTTPS. 3) Cifrado de datos entre las aplicaciones y los servicios. 4) Conexiones seguras en puertas de enlace por medio de cifrados de comunicación. 5) Actualizaciones de seguridad por medio de parches para los puntos vulnerables. 6) Pruebas de seguridad en proceso y actualización de firmware.

iv. Dispositivos de salida

Controles: 1) Doble autenticación biométrica por medio de huellas, NFC y pines. 2) Autenticación por medio de servidores externos a la red, con formularios de acceso HTTPS. 3) Cifrado de comunicaciones. 4) Actualización de firmware.

3.4 Discusión

A partir de los riesgos encontrados y los mecanismos propuestos para reducir los niveles de exposición es necesario establecer un plan que permita implementar soluciones tecnológicas, con lo cual los sistemas BCI quedarían más protegidos. Tomando en cuenta los avances y la tecnología que proporciona la industria 4.0 y todos sus sistemas emergentes, la ciberseguridad y la gestión de riesgos son pilares fundamentales para su correcto funcionamiento y protección.

Algunos estudios [16] establecen otro tipo de amenazas informáticas, como los ataques al firmware, obtención de credenciales de los elementos cercanos y el remplazo de la aplicación *software*, lo que exige más esfuerzo por parte del personal de tecnología para que visualice los riesgos de seguridad que existen a su alrededor.

Por otra parte, las tecnologías emergentes vienen creciendo y aumentando con la cuarta revolución industrial, haciendo que los sistemas BCI tenga un uso más frecuente y su información y datos deban ser más protegidos [6]. En ese sentido, el mapa de riesgos encontrado en este trabajo permite apoyar esa estrategia, debido a las diversas convergencias tecnológicas que se viven en la era digital.

Así mismo, son pocos los avances en materia de seguridad que pueden dar cuenta de los impactos reales que se pueden generar y los componentes que son hackeados o tienen un evento adverso de

seguridad. Al realizar una prueba de seguridad en un sistema BCI fue muy simple obtener información, lo que demuestra que los sistemas no están preparados para ataques informáticos ni para comprender la importancia de algún modelo de seguridad o ciberseguridad que pueda reducir los niveles de exposición [2]. Por esta razón, es fundamental generar un proceso de gestión de riesgos para identifica de manera temprana diversos eventos y posibles impactos.

Por último, la seguridad de los datos personales es fundamental, toda vez que es necesario cumplir leyes en Colombia, como la Ley 1581 que considera la protección de datos asociados a las personas en términos de no divulgación a terceros y la necesidad de protegerlos a través de un oficial de cumplimiento o de seguridad [21].

4. CONCLUSIONES

La 4ta. revolución industrial trae consigo retos y oportunidades, y en ese sentido los sistemas BCI desempeñan un papel importante, ya que los datos privados o personales que circulan por dichos sistemas suponen un esfuerzo importante para establecer mecanismos de protección de la información que se almacena o transmite, para lo cual son fundamentales las soluciones criptográficas y el control de acceso.

La gestión del riesgo debe estar orientada a una continua revisión por parte de los diseñadores y programadores de los sistemas BCI, para mantener un sistema actualizado, cuya premisa sea disminuir los problemas derivados de la pérdida de información y los ataques a la seguridad como la negación del servicio o el robo de datos. En ese sentido, es importante gestionar las vulnerabilidades y las amenazas de los sistemas, toda vez que se pueden evitar situaciones ligadas a ciberataques reduciendo los niveles de exposición de las interfaces cerebro-computador.

Las amenazas cibernéticas son un riesgo imperativo en el uso de dispositivos tecnológicos, pero la responsabilidad de los recursos es parte de las tareas que deben cumplir tanto los fabricantes de los sistemas como los usuarios finales. Un mecanismo podría ser el uso de estándares de seguridad como la ISO 27001 y sus anexos técnicos, para gestionar las diferentes etapas que cumplen el sistemas BCI desde el punto de vista de control y con ello minimizar las posibles filtraciones de información

REFERENCIAS

[1] F. M. Toma, “A hybrid neuro-experimental decision support system to classify overconfidence and performance in a simulated bubble using a passive BCI,” *Expert Syst. Appl.*, vol. 212, p. 118722, 2023, doi: https://doi.org/10.1016/j.eswa.2022.118722.

[2] L. Meng, J. Huang, Z. Zeng, et al., “EEG-Based Brain-Computer Interfaces Are Vulnerable to Backdoor Attacks”. PREPRINT (Version 1), 2020. doi: 10.21203/rs.3.rs-108085/v1.

[3] R. Anbarasan, D. Gómez Carmona, and R. Mahendran, “Human Taste-Perception: Brain Computer Interface (BCI) and Its Application as an Engineering Tool for Taste-Driven Sensory Studies,” *Food Eng*. Rev., vol. 14, no. 3, pp. 408-434, 2022, doi: 10.1007/s12393-022-09308-0.

[4] A. F. Osorio-Sierra, M. J. Mateus-Hernández y H. F. Vargas-Montoya, “Proceso para la identificación, clasificación y control del comportamiento de familias Ransomware”. *Revista UIS Ingenierías.* Vol. 19, n.° 3, pp. 131-142, 2020, revistas.uis.edu.co/index.php/revistauisingenierias.

[5] Amazon AWS, “¿Qué es un ataque DoS?”. Amazon Corp. https://aws.amazon.com/es/shield/ddos-attack-protection. (consultada octubre 15, 2022).

[6] C. A. Ríos Agudelo, “Arquitectura para automatizar respuesta a incidentes de seguridad de la información relacionados con ataques internos mediante la ejecución de técnicas spoofing”. Tesis de Maestría, Antioquia, Instituto tecnológico metropolitano-ITM. 2020. https://repositorio.itm.edu.co/handle/20.500.12622/4456.

[7] E. Crespo-Martínez, “Análisis de vulnerabilidades con SQLMAP aplicada a entornos APEX 5”. *Ingenius* N.° 25, pp. 103-112. enero-junio, 2021. doi: https://doi.org/10.17163/ings.n25.2021.10.

[8] E.A. Mohamed, M.Z. Yusoff, A.S. Malik, et al., “Comparison of EEG signal decomposition methods in classification of motor-imagery BCI”. *Multimed Tools Appl* 77, 21305–21327 (2018). https://doi.org/10.1007/s11042-017-5586-9.

[9] I. Choi, I. Rhiu, Y. Lee, M.H. Yun y C.S. Nam, “A systematic review of hybrid brain-computer interfaces: Taxonomy and usability perspectives”. *In PLoS ONE,* Vol. 12, Issue 4, 2017. https://doi.org/10.1371/journal.pone.0176674.

[10] Instituto Nacional de Ciberseguridad, “El ataque del ‘Man in the middle’ en la empresa, riesgos y formas de evitarlo”. *Incibe*. 2020. https://www.incibe.es/protege-tu-empresa/blog/el-ataque-del-man-middle-empresa-riesgos-y-formas-evitarlo (consultada octubre 15, 2022).

[11] M. A. Roldán Álvarez y H.F. Vargas Montoya, “Ciberseguridad en las redes móviles de telecomunicaciones y su gestión de riesgos”. *Revista Científica Ingeniería y Desarrollo*, 38(2), pp. 279-297. Julio, 2021. https://doi.org/10.14482/inde.38.2.006.31.

[12] MD, Joadder, J. Myszewski, M. Rahman y I. Wang, “A performance based feature selection technique for subject independent MI based BCI”. *Health Information Science and Systems* 7, (15). August, 2019. https://doi.org/10.1007/s13755-019-0076-2.

[13] N. Tibrewal, N. Leeuwis, and M. Alimardani, “Classification of motor imagery EEG using deep learning increases performance in inefficient BCI users,” *PLoS One*, vol. 17, no. 7 July, pp. 1-18, 2022, doi: 10.1371/journal.pone.0268880.

[14] National Institute of Standards and Technology, “Guide for Conducting Risk Assessments - NIST 800-30”. NIST. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. (consultada octubre 15, 2022).

[15] OWASP Fundation, “SQL Injection”. OWASP. https://owasp.org/www-community/attacks/SQL_Injection. (consultada octubre 15, 2022).

[16] P. Ballarin Usieto y J. Mínguez, “La importancia de la ciberseguridad en brain-computer interfaces”. https://www.bitbrain.com/es/blog/ciberseguridad-cerebro-computadora. (consultada octubre 20, 2022).

[17] P. Chaudhary y R. Agrawal, “Emerging Threats to Security and Privacy in Brain Computer Interface”. *International Journal of Advanced Studies of Scientific Research*, 3(12), pp. 340-344, 2018. https://ssrn.com/abstract=3326692.

[18] R. Martín-Clemente, J. Olias, D. Thiyam, A. Cichocki, and S. Cruces, “Information Theoretic Approaches for Motor-Imagery BCI Systems: Review and Experimental Comparison,” *Entropy*, vol. 20, no. 1, p. 7, Jan. 2018, doi: 10.3390/e20010007.

[19] S.L. Bernal, A.H. Celdrán, G.M. Pérez, M.T. Barros y S. Balasubramaniam, “Security in Brain-Computer Interfaces: State-of-the-Art, Opportunities, and Future Challenges”. *ACM Computing Surveys*, 54(1), Jan. 2021. https://doi.org/10.1145/3427376.

[20] S. Ajrawi, R. Rao, and M. Sarkar, “Cybersecurity in Brain-Computer Interfaces: RFID-based design-theoretical framework,” *Informatics Med. Unlocked*, vol. 22, p. 100489, 2021, doi: 10.1016/j.imu.2020.100489.

[21] Secretaría del Senado, República de Colombia, “Ley Estatutaria 1581 de 2012”. (2012). http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html. Octubre, 2022.