Modelo de seguridad basado en políticas de protección, para el procesamiento y manejo de datos asociados a sistemas BCI, mediante una gestión del riesgo con base en la ISO 27005 y su plan de tratamiento con el fin de reducir los niveles de exposición

Juan Camilo Ospina Cuervo

Instituto Tecnológico Metropolitano

Facultad de Ingeniería

Medellín, Colombia

2022

Modelo de seguridad basado en políticas de protección, para el procesamiento y manejo de datos asociados a sistemas BCI, mediante una gestión del riesgo con base en la ISO 27005 y su plan de tratamiento con el fin de reducir los niveles de exposición

Juan Camilo Ospina Cuervo

Trabajo de investigación presentado como requisito parcial para optar al título de:

Magister en Seguridad Informática

Director:

MSc. Héctor Fernando Vargas Montoya

Línea de Investigación:

Análisis forense y detección de Malware

Instituto Tecnológico Metropolitano

Facultad de Ingeniería

Medellín, Colombia

2022

Agradecimientos

A la academia por enseñarme a desenvolver mis capacidades intelectuales.

A los compañeros, amigos y co-trabajadores de tesis en las áreas adyacentes del estudio, por la ayuda prestada durante el desenvolvimiento de este trabajo.

A mi familia por ser el soporte más grande.

A Dios y al universo por haber conspirado para mantenerme firme y no decaer a pesar las adversidades presentadas durante este gran esfuerzo y dedicación que comprendió mi carrera.

Por quien luché siempre, mi musa y mi inspiración.
Sara…

Resumen

La interfaz cerebro computador-BCI, es una tecnología con la cual se puede adquirir y procesar los diferentes valores obtenidos de señales cerebrales que se transmiten a dispositivos finales para que interactúen de acuerdo con lo dispuesto por el celebro. Un sistema BCI está compuesto de diferentes etapas y cada una de ellas posee tecnologías que pueden tener vulnerabilidades de seguridad, con lo cual, la existencia de diferentes ataques informáticos como la negación de servicio, robo o alteración de información hacen del sistema un elemento vulnerable, lo que permite eventos que están fuera del control de los usuarios finales o de los administradores.

Esta incertidumbre genera situaciones adversas a las caracterizadas en la normalidad en las tareas que se deben realizar, ya que estos aspectos pueden generar pérdidas económicas o de información, dando como resultado una disminución en la eficiencia o desconfianza en el uso de estas tecnologías; con base en estos hechos, se ha diseñado un modelo de seguridad basado en políticas de protección, para el procesamiento y manejo de datos asociados a sistemas BCI, mediante una gestión del riesgo con base en la ISO 27005 y su plan de tratamiento, esto, con el fin de reducir los niveles de exposición. Para lograr dicho objetivo se caracterizaron los sistemas BCI, luego se establecieron cuáles pueden ser los niveles de riesgo, así, se generó un plan de tratamiento que enfocó la construcción de una metodología de protección del procesamiento y manejos de datos en sistemas BCI.

Finalmente, el modelo fue valorado a través de una simulación ejecutando algunos ataques informáticos como factores de riesgos tecnológicos.

Palabras clave: Ciberataques, Gestión de Riesgo, Interfaces Cerebro Computador, Sistema BCI, Vulnerabilidad

Abstract

Brain-computer-BCI interfaces are a technology with which the different values obtained from brain signals can be acquired and processed to pass to final devices so that they interact in accordance with the provisions of the brain. A BCI system is composed of different stages and each of them has technologies that may have security vulnerabilities, with which, the existence of different computer attacks such as denial of service, theft or alteration of information that make the system a vulnerable element, allowing events that are beyond the control of end users or administrators.

This uncertainty generates situations that are adverse to those characterized as normal in the tasks to be carried out, since these aspects can generate economic or information losses, resulting in a decrease in efficiency or distrust in the use of these technologies; Based on these facts, it has designed a security model based on protection policies, for the processing and handling of data associated with BCI systems, through risk management based on ISO 27005 and its treatment plan, with the in order to reduce exposure levels. To achieve this objective, it is expected to characterize the BCI systems, then establish what the risk levels may be, thus, generate a treatment plan that focuses on the construction of a methodology for the protection of data processing and handling in BCI systems.

Finally, the model was evaluated through a simulation executing some computer attacks as technological risk factors

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

Lista de Tablas

Contenido

Lista de Tablas

Lista de Tablas

Lista de figuras

Pág.

Lista de Tablas

Lista de Tablas

Lista de Tablas

Lista de tablas

Pág.

Lista de abreviaturas

A continuación, se presentan las abreviaturas utilizadas:

Abreviatura Término

MIRP: Máquinas Inteligentes y Reconocimiento de Patrones

ANN: Artificial Neural Network

AR: Autorregresivos

BCI: Brain Computer Interface

CSP: Common Spatial Pattern

CWT: Continuous Wavelet Transform

DFT: Discrete Fourier transform

DWT: Discrete Wavelet Transform

EEG: Electroencephalography

ERD: Event Related Desynchronization

ERP: Event Related Potentials

ERS: Event Related Synchronization

FFT: Fast Fourier transform

FT: Fourier Transform

ICA: Independent Component Analysis

k-NN: Nearest Neighbour

LDA: Linear Discriminant Analysis

MI: Motor Imaginary

MLP: Multilayered Perceptron

MRI: Magnetic Resonance Imaging

Lista de abreviaturas

PCA: Principal Component Analysis

PSD: Power Spectral Density

SVM: Support Vector Machine

WT: Wavelet Transform

Introducción

Los sistemas BCI son sistemas emergentes donde su tecnología está impactando el mercado como herramientas nuevas y cautivadoras, que cubren diferentes necesidades de las personas. Desde la perspectiva de los sistemas BCI, una vez capturan los datos, estos deben ser llevados a un dispositivo de salida que está ligado a un conjunto de herramientas tecnológicas, equipos o softwares, 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 automóviles. De igual manera, se cuenta con dispositivos como video juegos o aplicativos que pueden estar almacenados de manera local en un celular o de manera remota utilizando bases de datos que se encuentran en la nube para el uso de los usuarios de los sistemas BCI, también, sistemas de seguridad donde se recopila las señales procedentes de BCI como, firmas para los procesos de identificación y autenticación de usuarios ante un servicio computacional, por lo cual, el manejo de la información local o en tránsito en la red puede ser vulnerable a diferentes ataques informáticos que atentan contra de confidencialidad (develación de datos personales), disponibilidad (no acceso al sistema) y/o integridad (modificación no autorizada), y en ese sentido, el problema radica en no contar con mecanismos o procesos que le permitan a las organizaciones que trabajan con sistemas BCI, establecer un nivel de seguridad para la protección de la información y los datos procesados [1, 4, 5].

Diferentes proyectos están siendo impulsados por gobiernos como el de los E.E.U.U, Canadá, China, Japón y la Unión Europea, donde han financiado proyectos para el uso médico y también en ambientes empresariales, estos sistemas son grandes iniciativas para avanzar en el conocimiento del cerebro humano y con ello incursionar en procesos de adquisición de datos, aplicaciones de entretenimiento y desarrollos médicos [5, 9], abriendo la puerta a los grandes fabricantes de nuevos mercados; según estudios de la Juniper Research, se pudo valorar que para el año 2019 el uso de esta tecnología se estimó que fuera de 350.000 usuarios en el mundo, donde se adentró en procesos militares para el manejo de drones, de igual manera en

procesos médicos donde las personas con discapacidades fueran los mayores beneficiados en este tipo de recursos y no dejando de lado áreas del entretenimiento donde sistemas 3D y videojuegos fueron los que más utilizaron los sistemas BCI de manera significativa. Se estima que para el año 2030 el mercado tenga un crecimiento de 25.6 millones de usuarios [48], ya que los proyectos de servicios de BCI basado en IoT, la computación en la nube y los procesos de Big Data mejoraran la aceptación del mercado, ya sea en campos médicos como los del entretenimiento.

Es ahí donde se ve la necesidad de la seguridad de los productos y los sistemas de BCI deberán tener sistemas robustos con niveles de ciberseguridad en altos estándares ya que su expansión creara tendencia de riesgos y vulnerabilidades, al aumentar su competitividad en los desarrollos tecnológicos serán más notorios sus tendencias a ser objetivos de ciberdelincuentes [5, 9].

Diferentes riesgos se han encontrado y los más graves están asociados a la privacidad misma de un paciente, dado que los sistemas BCI pueden reflejar diferentes condiciones del ser humano como emociones, enfermedades y posturas frente a un tema específico, con ello, los Data Broker o personas que adquieren datos y los comercializan, están siempre a la espera de lograr obtener una jugosa fortuna con los datos personales de otros. En ese sentido, se puede estar pagando entre 38 y 250 dólares por historiales clínicos y este valor no deja de crecer. Así mismo, se pueden presentar ataques informáticos en el firmware de las diademas, interceptación de las comunicaciones (sniffing) o accesos no autorizados a los datos e información, esto, si no se cuenta con mecanismos de monitoreo y control sobre las plataformas [4].

Estas eventualidades hacen necesario crear escenarios y modelos de seguridad donde se pueda identificar y reducir los niveles de exposición de un sistema BCI, diseñando un modelo de seguridad basada en políticas de protección, para el procesamiento y manejo de datos asociados a sistemas BCI, mediante una gestión del riesgo con base a la ISO 27005 y su plan de tratamiento con el fin de reducir los niveles de exposición [26], donde se puedan evaluar sus características tanto de hardware como de software con el objetivo de realizar pruebas que sirvan como referencia en los eventos de seguridad de los BCI, ya que con este se podrá simular

los diferentes riesgos y amenazas para al final, hacer un análisis que nos permita diseñar una metodología para proteger las diferentes etapas que están asociadas los sistemas BCI [16, 21]. Normalmente los proyectos de implementación de BCI cuentan con diferentes herramientas tecnológicas, con las cuales han hecho visibles las posibilidades con las que pueden ser afectados o estar vulnerables, que se pueden convertir en una constante situación de riesgo, como tal se debe perfilar los riesgos con sus niveles de afectación, es por ello que iniciar con monitores y políticas para la gestión de los riesgos en seguridad se convierten en procesos mucho más notorios, generando planificaciones en los procesos de revisión, análisis y evaluación de los mismos. Es en dichas planificaciones donde se desarrollan acciones para tener certeza en la identificación de los aspectos importantes o inherentes, derivando en reportes, políticas, procesos y aseguramientos de la información, ya que se generarán modelos evaluativos en la seguridad ante diferentes ataques de la seguridad [65]

Los sistemas BCI hacen parte de los nuevos proyectos de Inteligencia artificial y el uso de tecnología máquina-humano, donde se ha logrado determinar que sus limitantes en cuanto a la ciberseguridad están ligados a su edad temprana en sus procesos, ya que utiliza dispositivos que potencialmente están expuestos a ciberataques como lo son computadores, celulares y diferentes dispositivos tecnológicos conectados a una red, que han mostrado su nivel de vulnerabilidad de una manera persistente y evidenciando que cualquier sistema tiene un nivel de vulnerabilidad latente, basado en lo anterior, han sido detectadas amenazas de ciberseguridad que afectan la integridad de las interfaces cerebro computador, esta limitación en ciberseguridad afectan la integridad de los datos que son utilizados y procesados [5].

La información personal será cada vez necesarios para su uso, dando estos criterios el almacenamiento de datos personales que puede generar un BCI, donde diferentes ataques informáticos se pueden presentar alrededor de ello, tal es el caso de malware de tipo Ransomware cuyo objetivo es cifrar la información y pedir rescate por ello, con variantes como solicitar la divulgación de datos personales sino se accede a las peticiones [47], en ese sentido,

proteger información de las diferentes personas se hace fundamental a la hora de usar, configurar, procesar y extraer datos. Dicha tendencia se sigue sosteniendo en el 2020, en dónde los atacantes visualizan que ya no basta con secuestrar la información y pedir rescate, sino de amenazar con publicar la información que se considera sensible [8, 28].

Acorde a la asociación Colombiana de Computación – ACIS (2020) [8] en su encuesta anual, ha identificado un grupo de sistemas y nuevas amenazas emergentes (Figura 2) que pueden tener fuga de información sensible (con un 39%) y problemas en seguridad en dispositivos médicos (con un 13%) son una preocupación de diferentes organizaciones, que deben estar explorando mecanismos que permitan reducir los niveles de exposición y validar cómo desde diferentes mecanismos, los ataques informáticos se deben identificar y controlar.

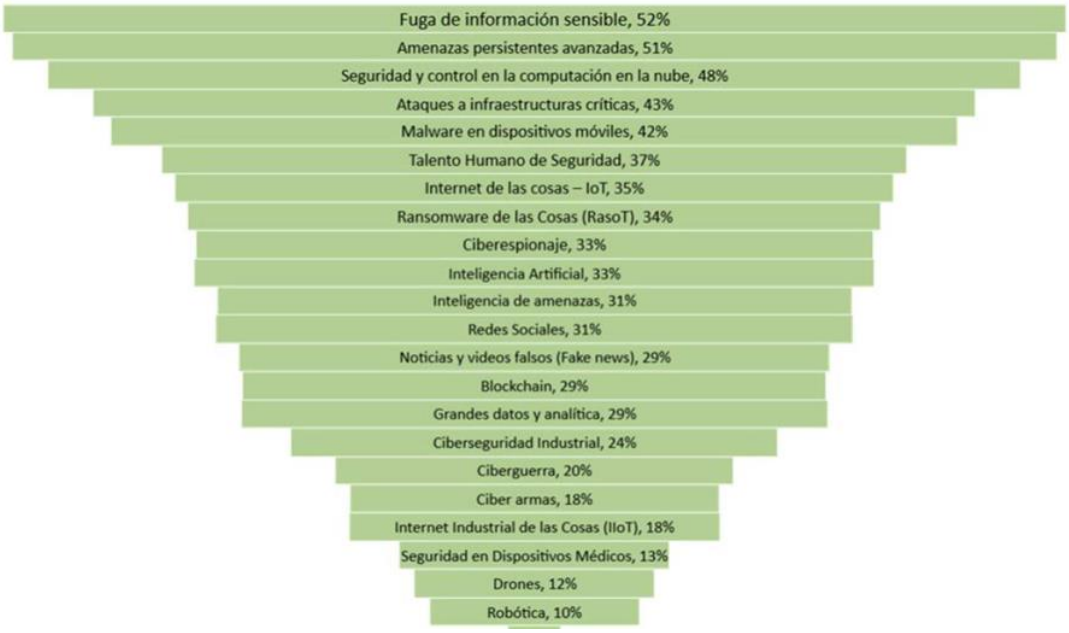


Figura 1 Temas emergentes. Fuente ACIS (2020) [8]

En esa misma línea, ACIS identificó una problemática asociada a la gestión de riesgos y la necesidad misma de fomentar este proceso, para lo cual, acorde a la Figura 2, el 44.12% de las empresas encuestadas no tienen o no llevan un proceso formal de gestión de riesgos, mientras que el 11.76% desconocen del tema (falta de formación al respecto), lo que indica que, ante eventos de seguridad, no se ha genera una propuesta de mitigación de posibles riesgos que

pudieron ser identificados de manera oportuna antes que sucedan y generen impactos negativos en las organizaciones [8]

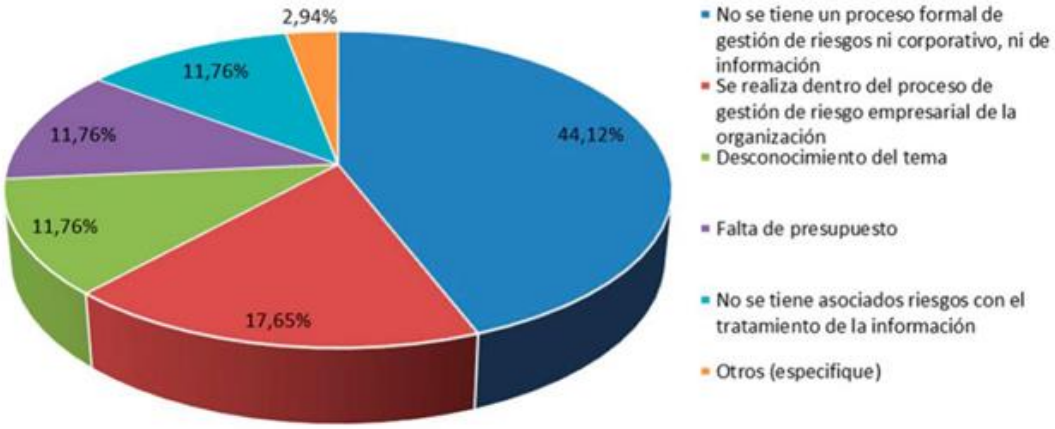


Figura 2 Cantidad de Gestión de Riesgos en Seguridad. Fuente ACIS (2020) [8]

Este proyecto de investigación aplicada aporta como objetivo general "*Diseñar un modelo de seguridad basada en políticas de protección, para el procesamiento y manejo de datos asociados a sistemas BCI, mediante una gestión del riesgo con base a la ISO 27005 y su plan de tratamiento con el fin de reducir los niveles de exposición*". Así mismo se tienen como objetivos específicos

- Realizar un mapa de riesgo, donde se identifiquen las amenazas, vulnerabilidades e impactos de la ciberseguridad asociadas a los sistemas BCI, a partir de la caracterización de sus componentes.
- Proponer un plan de tratamiento con base a los riesgos identificados el sistemas BCI, basado a los niveles de exposición e impactos.
- Validar el modelo de seguridad definido para un sistema BCI a través de una prueba técnica, una simulación o una prueba de escritorio.

1. Marco Teórico y Estado del Arte

1.1 Marco teórico

El estudio del cerebro ha sido un campo del conocimiento en el que científicos, ingenieros y especialistas de diferentes campos han enfocado todos sus esfuerzos, con el objetivo de conocer y elaborar métodos o mecanismos con los cuales se puedan adentrar más en el aprendizaje y conocimiento de cómo funciona el cerebro. Se han encontrado diferentes procesos y teorías, también se han diseñado tecnologías que ha permitido obtener conocimientos de cómo funciona el cerebro humano, aunque estos han sido mínimos, cada día se presentan nuevas investigaciones en este campo [3, 11].

Las interfaces cerebro-computador (BCI), son una tecnología con la cual se puede adquirir y procesar los diferentes valores obtenidos de señales cerebrales, con el objetivo de reconocer patrones de muestras recolectadas por un dispositivo, como puede ser el Electroencefalógrafo. Con base en estas muestras se puede monitorear las diferentes cargas electromagnéticas, e implementar un sistema BCI que se podría utilizar para generar comunicaciones entre dispositivos externos tecnológicos (computadores, manejo de máquinas o prótesis) y personas, permitiéndoles controlar estos dispositivos [17, 18]

1.1.1 Componentes de un Sistema BCI

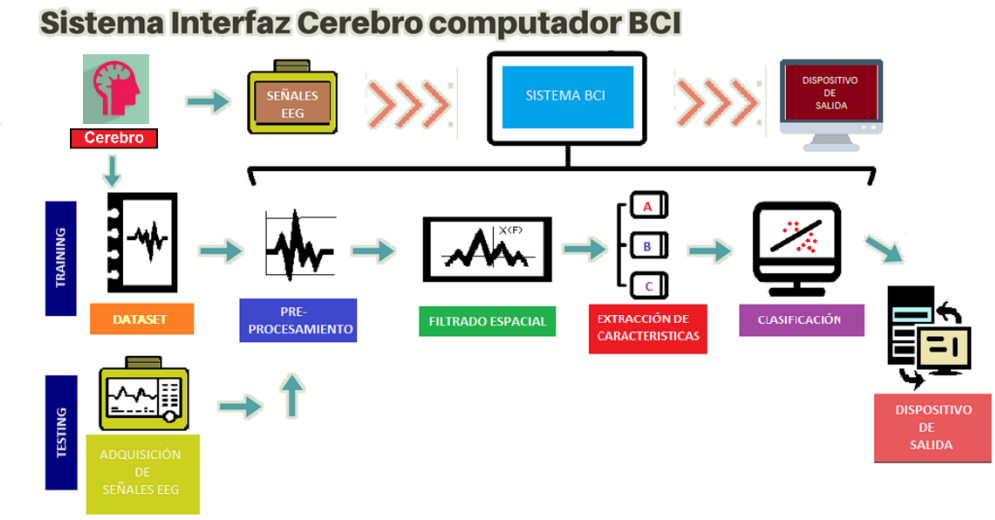


Figura 3 Componentes de un sistemas BCI. Elaboración Propia

La Figura 3 Ilustra los componentes fundamentales de un sistema BCI. En general un sistema BCI, al igual que la mayoría de sistemas de aprendizaje computacional, se desarrolla en dos etapas, una primera etapa de entrenamiento (training), en la cual el sistema aprende de muestras de las cuales se conoce la clase o categoría, en este caso el movimiento que es descrito por las señales y una segunda etapa de validación, en la cual el sistema es puesto a prueba para determinar la capacidad de generalización, al determinar el tipo de solicitud que hace el usuario a partir de señales que el sistema no había observado antes.

En los dos casos, el sistema está conformado por 6 componentes principales. Una primera etapa de adquisición de las señales, que permite la captura y digitalización de la actividad cerebral tiene dos tipos de características que son de tipo endógeno y tipo exógeno, las de tipo endógeno son asociadas totalmente a los procesos cognitivos y mentales sin ninguna estimulación, eso quiere decir que son los procesos normales que hace un ser humano cuando piensa o está en reposo, por otro lado están las de tipo exógeno que son generados por agentes externos que los motivan a moverse, pensar o realizar una actividad física [30, 50, 58].

Un Sistema BCI puede monitorear la actividad cerebral por medio de varias técnicas invasivas y no invasivas [30, 50, 58]. las técnicas invasivas son las que deben hacerse incisiones o mediante inyecciones intradérmicas o subcutáneas, donde se introduce unos electrodos con el objetivo de medir la actividad cerebral mediante estimulaciones eléctricas, esta técnica es conocida como Electrocorticografıa (ECoG), en este tipo de técnica se debe de realizar un procedimiento quirúrgico, donde un cirujano realiza un corte en el cráneo del paciente y deja expuesto una parte de la corteza cerebral para introducir los diferentes electrodos, este proceso debe ser realizado por un profesional para que el paciente no tenga secuelas en sus funciones motoras, sensoriales y de lenguaje [39,40,58], las técnicas no invasivas son las más comunes, y entre ellas se destacan algunas pruebas de imagenología como el MEG (Magneto encefalograma), la RM (Resonancia magnética) y el TAC (Tomografía axial computarizada). Este tipo de pruebas, sin embargo, tienen costos muy elevados a diferencia del EEG (Electroencefalograma). Con este último, se pueden tener diferentes conceptos y valoraciones sobre el funcionamiento de las ondas del cerebro a menor costo, por eso la realización de este examen termina siendo más

común. Este tipo de sistemas monitorean las diferentes muestras de las cargas electromagnéticas generada por el sujeto o paciente, por medio de electrodos conectados en el cuero cabelludo, en la superficie cortical o en la corteza cerebral [32, 33].

Una segunda etapa de preprocesamiento, donde las señales son tratadas haciendo uso de filtros de tipo Pasa Altas, Pasa Bajas, Rechaza Bandas o Pasa Bandas, dependiendo de las frecuencias que se necesiten para el desarrollo de la investigación, con este filtrado se trata de eliminar la mayor cantidad de ruido y distorsiones de la señal [49], así, una vez el modelo ha sido entrenado, el sistema puede usarse para la clasificación de nuevas señales.

Finalizando con la Clasificación de datos en el cual el sistema BCI se emplea para identificar y reconocer patrones de las actividades del EEG, identificando la intensión del sujeto basándose en las características que tienen los datos que se están recopilando de las señales y las asocia a tareas mentales. Existen dos técnicas de Clasificación que son populares entre las investigaciones de BCI, que son los clasificadores lineales y los clasificadores no lineales [34, 60]

los modelos de clasificación en los sistemas BCI, pueden utilizar aprendizaje profundo que tiene las facultades de determinar automáticamente, la mayor cantidad de características no relacionadas de una amplia cantidad de datos que pudieron ser omitidos en métodos previos al filtrado, gracias a su modelado de abstracciones de alto nivel con transformaciones no lineales. Una de las técnicas de aprendizaje profundo con redes neuronales son las arquitecturas convolucionales (CNN) [11, 45] que consiste en un sistema de múltiples capas de filtros convolucionales de una o varias capas, donde se realiza un mapeo causal no lineal.

1.1.2 Técnicas de Ataques en Ciberseguridad

Un ataque informático se puede presentar de diferentes maneras y puede generar diferentes impactos en las redes y sistemas de procesamiento. Los ataques buscan vulnerar los sistemas y establecer una cadena de acontecimiento negativos para los administradores y responsables de las áreas TIC. Ataques como la negación de servicios, Ransomware, modificación no autorizada de datos, entre otros, son fenómenos comunes en los sistemas y se hace necesario

su identificación y control, evitando que se generen esos impactos negativos y pérdidas potenciales [28].

En ese sentido, el requisito principal de la etapa de pruebas de las técnicas de ciberseguridad en BCI es analizar de una manera productiva que tipo de amenaza o dispositivo podría ser más vulnerables ante acciones no propias de la actividad del sistema BCI, ya que los sistemas no invasivos de EEG son altamente propensos al ruido, una señal de interés podría estar superpuesta en el tiempo y frecuencia de múltiples señales, que no son parte de las señales producidas por el cerebro o alguna parte del cuerpo, produciendo así interferencias y datos innecesarios para el trabajo que se realiza, estos datos erróneos podrían albergan algún tipo de código malicioso el cual puede estar integrado en la base de datos y con ello modificar la estructura del análisis del BCI, dando resultados diferentes al esperado, por otro lado, podría ser posible que se roben datos relevantes. Si por el contrario se hace esta etapa de una manera óptima se puede tener así una reducción de datos alterados y obtenido más información relevante para la investigación donde se puede determinar cuáles de las técnicas son más efectivas en un Sistema BCI [5].

Las diferentes técnicas para analizar la efectividad de los controles y políticas que se puede implementar en un sistema BCI para proteger la información relacionada con el transporte y clasificación son variadas, en esta etapa se utiliza diferentes tipos de diseños de pruebas que abarcan una amplia gama de técnicas que utilizan algoritmos para eliminar las posibles señales o algoritmos de entrada no deseados. Los controles permiten eliminar ataques de información que contaminan y dificultan la interpretación de las bases de datos, estas deben hacerse procurando no sustraer códigos que forman parte esencial del Sistema BCI [5].

1.1.3 Mapa de Riesgo - Gestión del Riesgo con Base a la ISO 27005

La gestión del riesgo como mecanismo para la toma de decisiones frente a ataques de seguridad, hace parte de los procesos que se deben tener en la prestación de los servicios que se brindan, dado que el uso de los sistemas de la información hacen parte de los métodos técnicos y tecnológicos de infraestructuras empresariales, de negocio o servicios tecnológicos,

de igual manera, los procesos de las diferentes áreas que conforman una entidad generan una cantidad de información que se utiliza como materia prima en sus productos o servicios, es por esto, que se debe proteger la integridad y la confidencialidad de los datos, dado que las operaciones deben minimizar los impactos que puedan tener ante ataques y amenazas capaces de afectar y disminuir la operación normal de la entidad [24, 25, 26]. Teniendo como resultado, modelos enmarcados en normativas que generan guías para la gestión de los riesgos, uno de estos es la norma ISO 27005/2013, esta normativa con su marco de referencia ha potencializado la disminución de las amenazas, garantizando mejores prácticas, y controles que han permitido iniciar con procesos donde pueden garantizar la disminución de problemáticas ligadas a los ataques de seguridad y perdida de información, evitando la perdida de la confidencialidad y disponibilidad [9, 51].

Los modelos conceptuales proveen una guía para determinar las características con las cuales se puede diferenciar riesgos, dichas interacciones deben contar con directrices donde la privacidad y el cuidado de la información sean indispensables, ya que hoy en día, uno de los grandes activos con los que se cuenta es la información, ya que los riesgos se caracterizan por ser situaciones o eventos que están fuera del control, esta incertidumbre genera situaciones adversas a las caracterizadas en la normalidad en las tareas que se deben realizar, ya que estos aspectos pueden generar pérdidas económicas, informáticas y documentales, dando como resultado una disminución en la eficiencia del producto o sistema [65]

1.1.4 Vulnerabilidad

Una vulnerabilidad se entiende como un hueco o fallo de seguridad, es la falta o falencia de un mecanismo de control que le permite a un atacante acceder a un sistema informático. Las vulnerabilidades permiten entonces, entender mejor los sistemas, en la medida que un administrador reconozca la necesidad misma de proteger ese fallo que existe, como la falta de parches, falencia de un proceso de capacitación, falta de control en las comunicaciones, deficiencia en la protección de datos locales o en tránsito, entre otras [28].

1.2 Estado del Arte

A continuación, se hará una aproximación a algunos proyectos de investigación que nos permiten conocer los diferentes alcances obtenidos acerca de los procesos pare el desarrollo de ciberseguridad en los sistema BCI, pero para iniciar con el procesos de análisis de estas prácticas se debe tener un primer análisis de los procesos de las interfaces Cerebro Computador y como en la literatura se hace la evaluación de esta, un sistema BCI, es una interfaz que permite que los humanos y las computadoras tengan interacción a través de las señales eléctricas producidas en el cerebro cuando se realiza una acción específica. Entre los diferentes esquemas BCI, se encuentran aquellos basados en el control de la modulación voluntaria de la actividad cerebral. El desarrollo de estos sistemas se basa en el reconocimiento de patrones de actividad cerebral, los cuales pueden ser identificados mediante el análisis de señales de electromagnéticas producidas por la actividad cerebral de un individuo, entre las muchas técnicas que se han desarrollado para llevar a cabo este análisis, el uso de técnicas de aprendizaje profundo se ha impuesto recientemente, por su efectividad en la discriminación de los datos producidos por los usuarios que son parte de los ensayos del uso del sistema [5].

Este tipo de nuevas tecnologías emergentes como son las interfaces cerebro computador tienen un valor agregado, que cada vez se hacen más importantes en la interacción máquina-hombre, este incremento generará nuevos paradigmas en la protección de la información, llevando a que estos sistemas deban generar procesos y políticas para la protección de los datos, ya que la información generada en los BCI puede ser susceptibles a riesgos ligados a la alteración y robo de información, y para ello se recurren a diferentes procesos en los que los métodos empíricos de verificar la disponibilidad de la información, la confiabilidad y la integridad de las bases de datos generadas, en las diferentes etapas que tiene los BCI, sean lo más seguras posibles, bajando la posibilidad de su corrupción [5].

Por otra parte, los métodos analíticos buscan evaluar la cantidad de vulnerabilidades que se pueden detectar en el sistema. Esto se realiza a través de datos subjetivos, pruebas expertas

y/o de técnicas de análisis. Las pruebas se realizan haciendo diferentes ataques en los procesos que cuenta la adquisición y clasificación de los datos, logrando evidenciar, cual es el punto más débil asociado con este tipo de nuevas tecnologías, debido a sus limitaciones por sus nuevos diseños ya sea de arquitecturas físicas o diseños de softwares, también, los sistemas BCI cuentan con características en sus datos, ya que tienen una libre disponibilidad para su uso, de la misma forma una cooperación interdisciplinaria en su desarrollo, donde investigadores, científicos en neurociencias, analistas de datos, entre otros, realizan diseños de algoritmos y esto abre las puertas a brechas de seguridad, es por eso que el analizar y documentar los ciberataques en sus diferentes fases tendrá en gran medida un impacto en la implementación de estos sistemas y como los agentes que hacen parte de los desarrollos deberán ser más cuidadosos [35, 49].

Por otro lado, se ha planteado la necesidad de establecer mecanismos de control que puedan reducir los niveles de riesgo ante estas situaciones, dentro de lo que se plantea, se dan recomendaciones como no usar software de dudosa procedencia o que este dentro de la categoría de software “pirata”, pero no es claro una solución más global que logre identificar otros riesgos asociados y como trabajarlos [6, 9]

Así mismo, se ha logrado determinar que su limitante esta ligado a la edad temprana en procesos de ciberseguridad y es por ello que han sido detectadas amenazas de ciberseguridad que afectan la integridad de las interfaces cerebro computador, esta limitación en ciberseguridad afectan la integridad de los datos que son utilizados y procesados, es por ello que se deben crear nuevos estándares para el desarrollo de estas nuevas tecnologías, junto a unas políticas de ciberseguridad que promuevan el cuidado de la información, donde se tendría que analizar qué tan expuestos están los dispositivos que pueden ser utilizados para los sistemas BCI, como son computadores, celulares y dispositivos, unido al software diseñado para interactuar entre la maquina y el usuario que utiliza la solución [5].

Se han visualizado diferentes mecanismos de ataques sobre las interfaces BCI, dado su inicio y posibilidades amplias de utilización, con lo cual, son pocos los avances en materia de seguridad

que pueden dar cuenta de los impactos reales que se pueden generar en los diferentes componentes hackeados o un evento adverso de seguridad. Dentro del planteamiento, fue muy simple obtener información a través de diferentes pruebas, lo que implica que los sistemas no estaban preparados para ataques informáticos ni tampoco para comprender la importancia de algún modelo de seguridad o ciberseguridad que pueda reducir los niveles de exposición [67,68]. La gestión de riesgos se puede considerar un medio para la mitigación de brechas ya que la disponibilidad de los datos y su protección, son ejes fundamentales para que el sistema cumpla a cabalidad sus objetivos, con parámetro ofrecidos por la ISO 27005 que tiene como objetivo contribuir en los parámetros relacionados con la infraestructura técnicas y tecnologías de proyectos para la gestión en las etapas del riesgo, este modelo complementa la normativa ISO 27001 que es un manual con el que se puede generar procesos de gestión de seguridad, esta metodología plantea un marco de seguridad ante ataques de seguridad Informática, ya que el impacto por problemas asociados en ciberseguridad está determinando las necesidades que se tienen, como requisito de seguridad se debe definir la estructura y la metodología para ser ejecutado.

Ya con el avance de la tecnología y considerando la existencia de ciberataques más sofisticados [4], la ciberseguridad viene tomando importancia en los sistemas BCI, considerando que dichos sistemas tienen la capacidad de almacenar información y datos personales de diferentes personas, en ese sentido, han surgido la necesidad de establecer mecanismos de protección sobre los datos personales, dada la alta posibilidad de que dichos sistemas y los datos que contienen o llegan a contener pueden ser hackeados. Sin embargo, no clarifican que tipos de controles podrían eventualmente servir o si a través de algún modelo de seguridad se pueden reducir los diferentes riesgos de exposición.

Los estudios mencionados anteriormente se resumen en la siguiente tabla:

Trabajos Relacionados o referencia	Propuesta / Contribución	Limitantes / Vacios	Proyecto Propuesto
H. Takabi, "Firewall for brain: Towards a privacy preserving ecosystem for BCI applications," 2016 IEEE Conf. Commun. Netw. Secur. CNS 2016, pp. 370–371, 2017, doi: 10.1109/CNS.2016.7860516.	En este trabajo se discute los problemas de privacidad únicos de los sistemas BCI y da el primer paso para abordar esos problemas al proponer un mecanismo que aplica múltiples capas de protección de la privacidad, como cifrado, control de acceso, análisis de código, abordando los desafíos de privacidad.	No aborda el tipo de tecnologias y sistemas que se pueden implementar para la proteccion de los datos en el BCI	Se contemplaran los diferentes equipos y tecnicas de protección de la información para la creación de un mapa de riegos que genere a documentación necesaria para el diseño de un plan mejoramiento.
S. L. Bernal, A. H. Celdrán, G. M. Pérez, M. T. Barros, and S. Balasubramaniam, "Security in Brain-Computer Interfaces: State-of-the-Art, Opportunities, and Future Challenges," ACM Comput. Surv., vol. 54, no. 1, 2021, doi: 10.1145/3427376.	Este trabajo presenta las versiones existentes del ciclo de vida de BCI y las homogeneiza en un nuevo enfoque que supera las limitaciones actuales. Posteriormente, ofrecemos una caracterización cualitativa de los ataques a la seguridad que afectan cada fase del ciclo BCI para analizar sus impactos y contramedidas documentadas en la literatura. Finalmente, reflexionamos sobre las lecciones aprendidas, destacando las tendencias de investigación y los desafíos futuros relacionados con la seguridad en las ICC.	No utiliza un marco de referencia para la generación de la documentación que se produce en el trabajo, dejando ligada la información a conceptos solo practicos y no brindando benas practicas en la investigación	Generar un modelo de seguridad basado en políticas de protección, para el procesamiento y manejo de datos asociados a sistemas BCI, mediante una gestión del riesgo con base a la ISO 27005 y su plan de tratamiento con el fin de reducir los niveles de exposición.
S. L. Bernal, A. H. Celdran, L. F. Maimo, M. T. Barros, S. Balasubramaniam, and G. M. Perez, "Cyberattacks on Miniature Brain Implants to Disrupt Spontaneous Neural Signaling," IEEE Access, vol. 8, pp. 152204–152222, 2020, doi: 10.1109/ACCESS.2020.3017394.	Este trabajo presenta un ejemplo de vulnerabilidades de dos tecnologías BCI, lo que demuestra la falta de principios de seguridad y privacidad en las soluciones existentes. donde cada amenaza puede afectar la actividad natural de las neuronas. Este trabajo implementa estos ataques en un simulador neuronal para determinar su impacto sobre el comportamiento neuronal espontáneo.	No caracteriza los tipos de ataques, forma en que se realizó la simulación y las posibles afectaciones	Se realizará la caracterización de los tipos de ataques posibles en un sistema BCI y validar los impactos basado en la documentación encontrada
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.C8	El objetivo de este documento es ayudar a la seguridad de la red para que las aplicaciones BCI identifiquen actividades cerebrales en un modo seguro en tiempo real.Para lograr esto, propuso ell diseño de un sistema basado en RFID (a Radio Frequency Identification)de identificación por radiofrecuencia, colocadas fuera del cerebro en el cuero cabelludo transmite las actividades cerebrales recopiladas de forma inalámbrica a un dispositivo controlador de escáner	No realiza la caracterización y documentación de los ataque mas comunes utilizando radiofrecuencias entre el sistema BCI y el dispositivo final	Se documentará los ataques y daños mas comunes en el framework que utiliza ondas electromagneticas para el transporte de información a sispositivos endpoint.
L. Meng et al., "EEG-Based Brain-Computer Interfaces Are Vulnerable to Backdoor Attacks," pp. 1–11, 2020, [Online]. Available: http://arxiv.org/abs/2011.00101.	Este artículo propone utilizar pulsos de ondas período estrecho para el ataque de envenenamiento de BCI basados en EEG, que se puede implementar en la práctica y nunca antes se había considerado. Se pueden crear puertas traseras peligrosas en el modelo de aprendizaje automático inyectando muestras de envenenamiento en el conjunto de entrenamiento.	Las muestras de las señales del EEG no demuestran la capacidad de envenenamiento del sistema y si es posible que el framework sufra fallas de hardware y software posteriores a este tipo de ataques	se realizará pruebas para ver el alcanze de los ataques en los sistemas BCI para documentar si el sufre daños temporales o totales
P. Chaudhary and R. Agrawal, "Emerging Threats to Security and Privacy in Brain Computer Interface," Int. J. Adv. Stud. Sci. Res., vol. 3, no. 12, pp. 340–344, 2018, [Online]. Available: https://ssrn.com/abstract=3326692.	Este documento analiza brevemente el proceso de desarrollo de BCI. También incluye la breve revisión sobre las posibles amenazas a la privacidad y la seguridad involucradas en los sistemas BCI con posibles medidas de seguridad para mitigar las amenazas a la privacidad.	Este trabajo no presenta la caracterización de un sistema BCI y las etapas de un ataque cibernetico en los diferentes componentes	Se realizará la valoración de los ataque en cada uno de los componetes del sistemas BCI y con dicha información generar politicas de buen uso de los componentes del framework

Tabla 1 Análisis Trabajos Relacionados y Contribuciones - Fuente Propia

Metodología

La revisión que se realizó tiene en cuenta artículos de los últimos 5 años debido que se encontraron artículos del año 2017 son relacionados con esta propuesta, de esta manera los sistemas BCI, deberán generar modelos de ciberseguridad donde se puedan valorar sus procesos, comprendiendo los alcances de las nuevas metodologías aprendidas, basado en esto se propone realizar esta investigación.

2. Metodología

El desarrollo de este trabajo se realizó cumpliendo tres diferentes fases que se exponen en la figura número 4, en donde cada fase corresponde a un objetivo específico.

La fase 1, se inició realizando una caracterización de los componentes tecnológicos que hacen parte de los sistemas BCI, donde se han identificado cada una de las etapas que permiten la comunicación entre un usuario y un computador, a través de una investigación de la literatura encontrada sobre este tema y donde se han identificado las etapas que hacen parte del sistema las cuales son: primero la adquisición de las señales eléctricas, segundo una etapa de pre procesamiento, tercero extracción de características y finalmente una etapa de clasificación en la cual se interpretan las señales de entrada como ordenes que son enviadas a dispositivos de salida.

Seguido se obtuvo un levantamiento de activos, amenazas y vulnerabilidades que hacen parte del sistema BCI, donde se evidenciaron los equipos y tecnologías que hacen posible cada uno de los procesos del sistema, como son herramientas tecnológicas que utilizan hardware y software, de igual manera, se identificaron las posibles amenazas y vulnerabilidades sobre activos de información y a partir de ello, se construyó un mapa de riesgos que permitió la identificación de riesgos sobre activos de información. Para esto se utilizó la ISO/IEC 27001:2013 y 27002:2014 [24,25] y a partir de los hallazgos, se obtuvieron los impactos negativos que se pueden generar sobre un sistema de referencia diseñado para hacer pruebas, este sistemas BCI de pruebas estaba alojada en un servidor y donde se probaron ataques utilizando los parámetros de la metodología de Ethical Hacking y se vieron las vulnerabilidades

del sistema, y con los resultados que se obtuvieron, se diseñó un plan de tratamiento y una gestión adecuada de los posibles impactos que se generaron.

La fase 2, consistió en definir un plan de tratamiento de acuerdo con los riesgos encontrados en el mapa de riesgos, donde se obtuvieron una cantidad verificada de escenarios con diferentes amenazas y vulnerabilidades, y con ello, indicar la probabilidad de ocurrencia y el impacto que pudieron generar en un activo determinado, consolidando los riesgos en una matriz que permitió visualizar los posibles impactos en todo el sistema BCI, estos riesgos potenciales tenían un grado de cuidado y se debieron generar unos procesos de tratamiento, ya que estaban ligados en los ámbitos administrativos, técnicos y tecnológicos, donde se desarrollaron escenarios para iniciar el tratamiento efectivo de los riesgos utilizando la norma ISO/IEC 27005:2018 [26] y las tareas que fueron necesarias diseñar e implementar para darle un control donde se priorizó la seguridad, donde ampliamente se determinó la efectividad y alineado la protección del sistema en sus diferentes etapas de la interfaz cerebro computador.

Por último, en la fase 3 se definió el modelo de seguridad que son las políticas que se van a implementar en el sistema BCI que se desarrolló utilizando la ISO 27001/2013 [25] y el ciclo de Madurez-Modelo de Seguridad y Privacidad de la Información de MinTic como marco de referencia, estas políticas fueron diseñadas para la gestión y control de las características y servicios con las que se obtuvieron resultados y que se pudo evidenciar con la validación de la estrategia de implementación, donde se probaron nuevamente ataques utilizando los parámetros de las metodologías de Ethical Hacking donde se vieron las vulnerabilidades del sistema y se evidenció como fueron mitigadas por los controles establecidos, dando con esto las herramientas necesarias para hacer un informe de los procesos y resultados del proyecto.

Como se indicó, en la figura 4 se tiene un esquema general de las fases usadas para la obtención de los resultados, en la cual, cada fase corresponde a un objetivo específico antes relacionados.

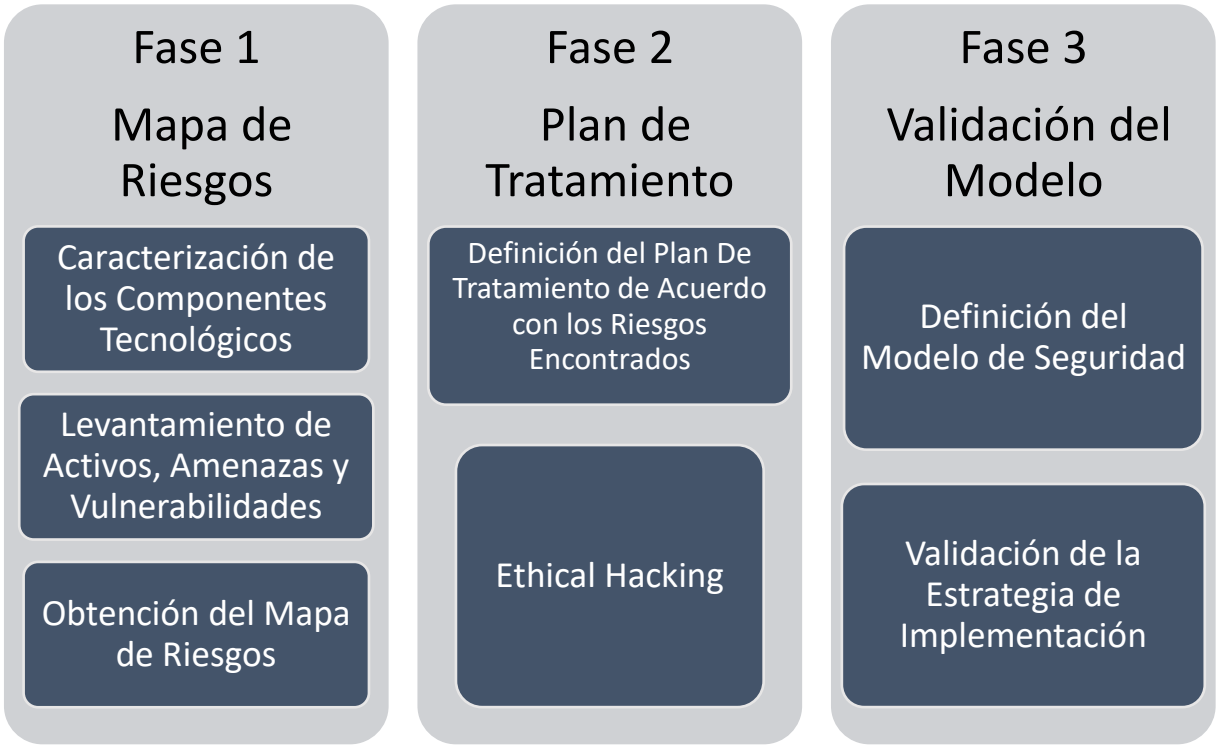


Figura 4 Metodología a seguir para el desarrollo del proyecto de grado. Fuente propia

A continuación, se da más detalles de cada una de las fases de la metodología.

2.1 Etapas de la Metodología

2.1.1 Fase 1: Mapa de Riesgos

2.1.1.1 Caracterización de los componentes tecnológicos

El trabajo realizado se incluye una revisión de la literatura y el estado del arte relacionado con los diferentes componentes de un sistema BCI, donde se han identificado las etapas para que el sistema sea funcional en todo proceso, allí se logra evidenciar que herramientas de hardware, software y programación son indispensables para que cada una de las etapas cumpla su tarea, para ello se hizo una selección de artículos, lectura de documentación, análisis de artículos, una descripción de los procesos del BCI y un informe donde se documenta cada una de las etapas, en este informe se puede leer: la etapa de adquisición de señales, la etapa de pre procesamiento, la etapa de procesamiento, la etapa de caracterización, la etapa de clasificación basado en aprendizaje profundo, dispositivos de salida y sus características,

medios de transporte de información, lenguajes de programación y para finalizar los servicios de almacenamiento locales y en la nube.

2.1.1.2 Levantamiento de Activos, Amenazas y Vulnerabilidades

Basado en la revisión sistémica que se hizo en la caracterización de los componentes donde se verifica como es la funcionalidad del sistema BCI, que es una interfaz cerebro computador que permite la traducción en tiempo real de las señales producidas por el campo electromagnético del cerebro, para tomar ese tipo de señales, se necesitó un dispositivo tipo electroencefalograma que no fuera invasivo y que permitiera tomar la muestra de datos, para el montaje y uso del sistema BCI, se colocó en la cabeza de un usuario una diadema de una de una interfaz cerebro computador que utilizó un sensor tipo el electroencefalograma este dispositivo recogió la señal y la envía un dispositivo cercano, este dispositivo cercano puede ser un computadora o un celular por medio de señales que pueden ser Bluetooth o Wifi.

Cuando el dispositivo cercano recogió esta señal la recopilo, la almacenó e inició un proceso de preprocesamiento de la actividad cerebral. La información recopilada fue enviada desde ese dispositivo cercano a una interfaz o un equipo que pudo trabajar con estas señales producidas desde el electroencefalograma de manera remota, este tipo de dispositivos finales pueden ser asociados a diferentes tipos de tecnologías, éstos pueden ser: un sistema para controlar prótesis motoras o robótica, celulares, computadores, sillas de ruedas, video Juegos y automóviles de igual manera una gran parte de esos datos también pueden ser almacenados en un sistema de la nube o aplicaciones, para ello, se necesitó que el sistema BCI estuviera conectado vía internet a un proveedor de servicios para permitir enviar esa información y recopilarla.

Ya al tener documentado el hardware y software que se utiliza para el funcionamiento del sistema BCI, se continua con la lectura del estado del arte donde se pudo determinar un listado de vulnerabilidades, ataques y amenazas que hacen parte de los procesos del sistema BCI y darle la respectiva documentación donde parte los hallazgos nos mostró, que en consideración a los riesgos, amenazas y vulnerabilidades, algunos estudios establecen una línea similar con otros tipos de ataques informáticos como son los ataques al firmware,

malware, Ransomware, obtención de credenciales de los elementos cercanos y el reemplazo de la aplicación software, lo que suma en esfuerzos para que el personal de tecnología visualice los riesgos de seguridad que pueden existir alrededor de las tecnologías emergentes que vienen en crecimiento y aumentando, lo que hace que los sistemas BCI tenga un uso más frecuente y con ello, la información y los datos deban ser protegidos, en ese sentido, esta información fue organizada y documentada para que se convirtiera en los datos utilizados en la creación del mapa de riesgos.

2.1.1.3 Obtención del Mapa de Riesgos

El mapa de riesgos encontrado en este trabajo, se realizó haciendo una evaluación utilizando como marco de referencia la normativa ISO/IEC 27001:2013 y 27002:2014 [24, 25] que fue utilizado con sus dominios y controles, seguido al seleccionar la normativa, se realizó un consolidados de activos, un inventario de amenazas y vulnerabilidades que hacen parte del sistema BCI, la información fue tomada del levantamiento de activos, amenazas y vulnerabilidades que se había realizado previamente, al tener la información organizada se inició la calificación de los riesgos utilizando un formato que se diseñó para este proceso, cada una de las calificaciones son anexadas en los resultados del mapa de riesgos que podrán observar más adelante en el proyecto, con los resultados y análisis ya referenciados del mapa de riesgos se pudo analizar y documentar cuáles son las posibles causas de eventualidades y riesgos ligados a cada actividad y proceso, de manera tal que la evaluación necesaria para verificar los procesos técnicos, tecnológicos y de seguridad fue lo más exitosa posible, ofreció un marco para el diseño, la implementación, trazabilidad y respuestas que fueron expuestas en el plan de tratamiento y que son derivadas a la realización del mapa de riesgos.

2.1.2 Fase 2: Definición del Plan De Tratamiento de Acuerdo con los Riesgos Encontrados

2.1.2.1 Definición de Plan De Tratamiento de Acuerdo con los Riesgos Encontrados

Al finalizar el proceso de elaboración del mapa de riesgos se elaboró un documento con la totalidad de eventos analizados y seleccionados que pueden afectar a un sistema BCI y que deben ser controlados, para ello, se implementó un plan de tratamientos que completa los controles y vulnerabilidades, junto a las acciones para el tratamiento de las correcciones, las acciones correctivas y las acciones preventivas, así como de la eficacia de las soluciones de los riesgos hallados. Dichas politicas fueron diseñadas y estructuradas utilizando ISO/IEC 27001:2013 y 27002:2014 [24,25] como marco de referencia, donde se seleccionaron un conjunto de dominios y controles que fueron afectados por las amenazas encontradas, de igual manera, como se indicó, se utilizó la ISO/IEC 27005:2018 [26] para el control y reducción de los riesgos, dando como resultado un documento con las politicas a implementar como controles de las amenazas en los activos del sistema. Esto como guía para los pasos a seguir para dar un nivel de seguridad de los sistemas BCI.

2.1.3 Fases 3: Validación del Modelo

2.1.3.1 Definición del Modelo de Seguridad

En esta actividad, se construyó la propuesta del diseño del modelo de seguridad basado en las 2 fases anteriores (mapa de riesgos y el plan de tratamiento), donde se generaron las politicas para el control de los riesgos que tiene como base el marco normativo la ISO/IEC 27001:2013.

Por consiguiente, se proporciona un marco legal ligado a una estructura normativa donde se ve las leyes, decretos, CONPES y normas técnicas que ayudan a la gestión de la seguridad. Junto con los parámetros entregado por el MinTic [44], para el desarrollo de modelos de seguridad con el que se contempló el uso del ciclo de operación PHVA, donde cada una de las fases del ciclo determinó una tarea a cumplir, en la **fase de planificación**, se determinó los procesos de analizar, determinar e implementar actividades que estuvieran enfocados hacia tareas administrativas y documentales, en la **fase implementación** se determinó los controles

a determinar ligados al mapa de riesgos y el plan de tratamiento, todo esto medido en el tiempo y cumplimiento, en la **fase de evaluación** se estableció los métodos de evaluación de los controles, políticas y plan de tratamiento establecidos, esto ligado a quienes son los responsables de los procesos. Finalizando con la **fase de mejora continua** donde se determinó el crecimiento y la madurez del modelo de seguridad.

Seguidamente, se determinó los niveles de madurez del modelo de seguridad [44] que están determinados por la normativa de la ISO/IEC 27001:2013 donde tenemos los dominios y controles, y deberán ser calificados y evaluados para valorar la eficacia del modelo de seguridad desarrollado para los sistemas BCI.

Ligando a lo anterior, se formularon **los mecanismos de seguridad** del modelo donde se enfocó en tres diferentes procesos, como lo son **los roles y responsabilidades** de los actores que hacen parte de los sistemas BCI, este se puede verificar en el anexo A, además de **los controles de seguridad de la información** asociados a las amenazas donde se hizo la calificación cuantitativo y cualitativo de los dominios de la ISO/IEC 27001:2013, teniendo en el anexo B cada uno de los resultados del análisis y para finalizar, se determinó **el inventario de la documentación de los dominios** de la ISO/IEC 27001:2013 para la seguridad de la información donde podrán validarse en la inserción de las labores técnicas y administrativas para la mitigación de los riesgos de los sistemas BCI y que puede verse en el anexo C.

2.1.3.2 Validación de la Estrategia de Implementación

Se realizó la validación de la estrategia de implementación con el objetivo de encontrar y/o validar posibles riesgos de seguridad, mediante la ejecución de dos diferentes procesos técnicos que nos brindaron información necesaria para la protección de los activos.

Primero, se ejecutó un análisis de vulnerabilidades con el que se identificaron fallas o defectos en los programas o servicios, donde agentes externos no identificados o sin permisos puedan realizar tareas no permitida de forma remota en el servidor donde se alojaba el sistema BCI, basado en reconocimientos, análisis y procesos de verificación de vulnerabilidades, en esta actividad se utilizó la herramienta Nessus que nos dio la información necesaria donde era

vulnerable el sistema, se documentó para que se pudiera hacer una gestión oportuna de eventualidades que podrían convertirse en problemas a futuro.

Seguido, se ejecutaron algunas pruebas considerando una metodología de Ethical Hacking, donde se tiene como tarea fundamental el explotar las vulnerabilidades encontradas, y así, validar su nivel de seguridad. Se pudo penetrar las defensas de los sistemas y capturar información restringida, para dicha tarea, se hizo pruebas de ataques maliciosos al sistema donde se seleccionó un listado de vulnerabilidades provenientes del mapa de riesgos y los hallazgos fueron documentados como evidencia de los niveles de seguridad con los que se contaba, donde se asumió una forma sistémica necesaria para lograr la finalidad de los ataques.

En consecuencia, fue necesario establecer políticas y procedimientos tratando de mantener un nivel de exposición siempre menor al nivel de riesgo, para ello, se utilizó el plan de tratamiento propuesto, donde se parcharon las vulnerabilidades y se minimizaron la superficie de ataque basado en los controles diseñados.

Acorde a lo anterior, se retomaron los diferentes pasos de los procesos técnicos descritos anteriormente, con los mismos niveles de riesgos y vulnerabilidades ya identificados en los primeros pasos, donde se ejecutó el proceso de análisis de vulnerabilidades nuevamente utilizando la herramienta Nessus, quien entrego un nuevo informe que demostró que bajaron las vulnerabilidades del sistema. Nuevamente se utilizaron las herramientas ligadas a la metodología de Ethical Hacking, donde los test de prueba mostraron que no era posible hacer ninguna infiltración de información, ingreso indebido al sistema o dejarlo sin funcionamiento.

3. Resultados

Acorde a lo indicado en la metodología, a continuación, se entregan los diferentes resultados obtenidos.

3.1 Fase 1: Mapa de Riesgos

3.1.1 Caracterización de los componentes tecnológicos de un sistema BCI

En los últimos años el estudio del cerebro ha sido un campo del conocimiento en el que científicos, ingenieros y especialistas de diferentes campos han enfocado todos sus esfuerzos, con el objetivo de conocer y elaborar métodos o mecanismos con los cuales se puedan adentrar más en el aprendizaje y conocimiento de cómo funciona el cerebro. Se han encontrado en los últimos años diferentes procesos y teorías, también se han diseñado tecnologías que ha permitido obtener conocimientos de cómo funciona el cerebro humano, aunque estos han sido mínimos, cada día se presentan nuevas investigaciones en este campo [32, 36].

La interfaz cerebro-computador (BCI), es una tecnología con la cual se puede adquirir y procesar los diferentes valores obtenidos de señales cerebrales, con el objetivo de reconocer patrones de muestras recolectadas por un dispositivo, como puede ser el Electroencefalógrafo. Con base en estas muestras se puede monitorear las diferentes cargas electromagnéticas, e implementar un sistema BCI que se podría utilizar para generar comunicaciones entre dispositivos externos tecnológicos (computadores, manejo de máquinas o prótesis) y personas, permitiéndoles controlar estos dispositivos a través de las señales cerebrales [30, 50, 58].

Para el desarrollo de un sistema BCI, se debe tener una primera etapa donde se seleccione una estrategia con la que se pueda realizar una extracción de información, el método más común para tomar estas muestras, donde un paciente o un voluntario es conectado a un Electroencefalograma (EEG), luego se le empiezan a presentar ciertas imágenes al paciente con el objetivo que imagine cómo realizaría el movimiento o la actividad que se le está mostrando, al realizar este tipo de experimentos se van generando ciertos impulsos eléctricos por parte de

Resultados

la persona que hace la actividad, similares a como si estuviera realizando realmente el movimiento, [30, 50, 58].

Sistema Interfaz Cerebro Computador (BCI)

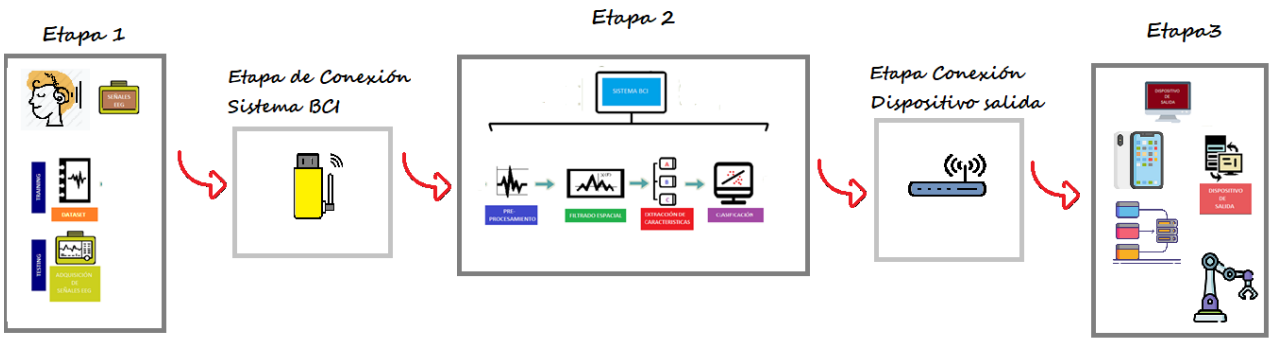


Figura 5 Etapas de un Sistema BCI. Fuente Propia

En los sistemas BCI está conformado por diferentes componentes. Una primera etapa de adquisición de las señales, que permite la captura y digitalización de las misma, en este caso el sujeto es conectado a un EEG, luego se le presentan ciertas imágenes al paciente con el objetivo que imagine cómo realizaría el movimiento o la actividad que se le está mostrando [40, 66], generando una cantidad de señales que serán ingresadas al sistema BCI. Una segunda etapa de preprocesamiento, donde las señales son tratadas haciendo uso de filtros de tipo Pasa Altas, Pasa Bajas, Rechaza Bandas o Pasa Bandas, dependiendo de las frecuencias que se necesiten para el desarrollo de la investigación, con este filtrado se trata de eliminar la mayor cantidad de ruido y distorsiones de la señal. Este tipo de filtrados son importantes ya que es normal que las señales contengan frecuencias innecesarias para el sistema. Luego se realiza un Filtrado Espacial, con el objetivo de buscar patrones de comportamiento, estos servirán para una mejor interpretación de los datos, aquí las señales son transformadas del dominio del tiempo a el dominio de la frecuencia, con esta técnica se podrá filtrar patrones de las señales en diferentes rangos de frecuencia. En el tercer componente, la extracción de características, cada uno de los valores que definen intrínsecamente las distintas frecuencias tomadas del individuo son extraídas al procesar las señales de cada uno de los eventos, tales propiedades son calculadas usando diferentes métodos matemáticos [34, 62]. Estas representaciones de la información son

usadas para clasificar la señal del EEG en una de las categorías de movimiento que se están buscando. En la etapa de entrenamiento, el sistema es entrenado para identificar y reconocer patrones de las actividades del EEG, que permitan asociar las características que describen las señales a clases que representan el movimiento imaginado. Entre mejor sea la calidad de la clasificación del conjunto de datos en la etapa de entrenamiento, mejores serán los resultados para el desarrollo de herramientas en BCI y para ser usadas en los dispositivos de salida [6, 9]. Una vez el modelo ha sido entrenado, el sistema puede usarse para la clasificación de nuevas señales.

Es importante verificar y hacer comparaciones entre señales reales tomadas de bases de datos donde ya se han realizado los análisis de estas demostrando su calidad y veracidad, para después comparar las señales imaginadas por la persona que ha realizado el experimento para verificar la eficiencia [6, 9]. Es importante resaltar que entre mejores sean los resultados comparativos entre los datos de las dos etapas del Sistema BCI, mejores serán los resultados para la etapa final del proceso que serán vistos en el dispositivo de salida.

3.1.1.1 Etapa 1: Adquisición de las Señales de EEG

El Electroencefalograma (EEG) es una herramienta para el estudio y el registro de las ondas cerebrales, por medio de unos electrodos, puestos sobre la cabeza de los sujetos. Normalmente, se conectan entre 18 y 40 electrodos en total; que a su vez están conectados a un equipo que tiene la capacidad de registrar corrientes eléctricas. El EEG se basa en las corrientes de naturaleza iónica presentes en la corteza cerebral, que son el producto de la actividad cerebral y pueden ser capturadas con unos electrodos colocados en el exterior del cráneo en diferentes combinaciones, aunque el montaje transversal y el montaje longitudinal a la cabeza del paciente), son los estandarizados por parte de la Federación Internacional de EEG y Neurofisiología. Previamente, estas corrientes iónicas deben ser convertidas a eléctricas, condición necesaria para que los electrodos metálicos puedan transportar la corriente hasta el amplificador de instrumentación. Según la frecuencia producida por estos impulsos se puede identificar varios tipos de ondas, que pueden ser medidas en cuatro bandas: las bandas delta

Resultados

0.5 Hz – 4 Hz, theta 4 Hz – 8 Hz, alfa 8 Hz – 13 Hz y beta 13 Hz – 30 Hz, donde cada una de estas frecuencias tiene la información de una tarea específica en los procesos neuropsicológicos de una persona [6, 9].

El EEG se encarga de leer el sistema nervioso y a partir de él, realiza el análisis pertinente. El sistema nervioso está compuesto por un conjunto de tejidos que están encargados de captar y procesar de manera rápida las señales internas y externas, tomando control y coordinación sobre los órganos, para así, lograr una interacción oportuna con el medio ambiente. Cuando se produce un estímulo externo, dicho estímulo es recibido en alguna región sensorial ubicados en el cerebro (capturando la información el EEG), la cual es transportada por el sistema nervioso (a través de las neuronas) hasta una componente integradora en donde se analiza. Esta componente elabora una respuesta, que es conducida a través de las neuronas hacia las fibras musculares actividad llamada respuesta motora [6, 22].

Existen diferentes tipos de sensores para la captación de las señales: Los electrodos en casco de malla, repartidos a lo largo de un casco elástico. Electrodos de contacto, los cuales son pequeños tubos de plata unidos a soportes de plástico poniendo en el extremo una almohadilla que se humedece con una solución conductora. Electrodos subdurales: los cuales se utilizan para registrar la actividad eléctrica directamente desde el cerebro. Los electrodos subdurales se implantan en el quirófano bajo anestesia general. Los dos últimos resultan un tanto más incómodo para el paciente. La Figura 6, Ilustra un sistema EEG.

Resultados

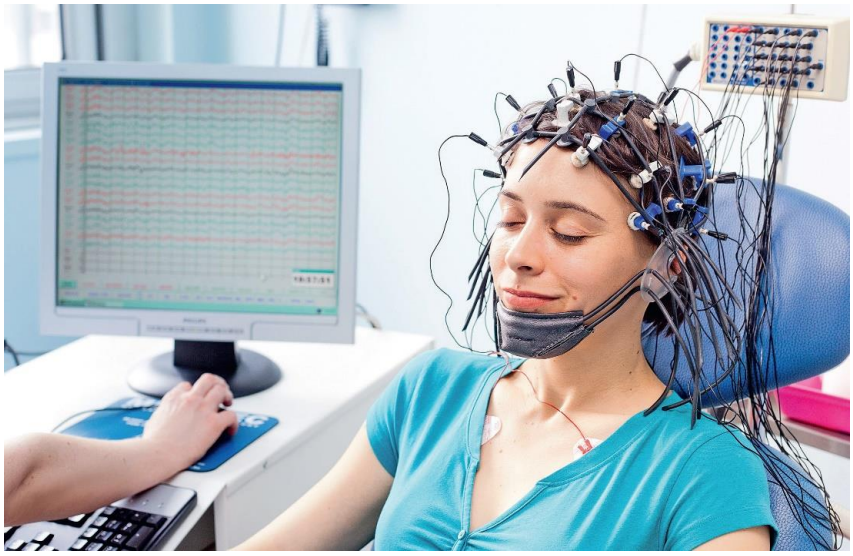


Figura 6 Sistema de EEG. Fuente: R. Ventures. "Mujer experimentando un electroencefalograma (EEG). Hospital de Limoges, Francia Fotografía de stock - Alamy".2018. https://www.alamy.es/foto-mujer-experimentando-un-electroencefalograma-eeg-hospital-de-limoges-francia-56058019.html

La captación de dichas señales se puede realizar tomando las muestras en el cuero cabelludo o en la base craneal, ya sea con el cerebro expuesto o en localizaciones cerebrales profundas. Sin olvidar la baja relación señal a ruido (SNR), ya que los sensores deben ser alimentados por frecuencias. Esto supondría una señal al menos 1000 veces mayor en amplitud que las medidas del orden de microvoltios [6]. Este tipo de adquisición de señales con EEG, está enfocado para la elaboración de bases de datos para sistemas BCI, donde las señales describen la generación de impulsos electromagnéticos, simulando movimientos reales de las extremidades del cuerpo, para generar este tipo de señales los sujetos deben imaginar que están realizando la actividad o el movimiento del cuerpo, sí se desea lograr mejores resultados, se debe tener práctica con la generación de este tipo de impulsos, una de las técnicas que ayudan al método MI, es la visualización de las tareas a imaginar(viendo videos o imágenes) para hacer que las señales sean más robustas, durante la actividad y la recolección de datos para MI, también es útil tener bases de datos que sirvan de referencia para comparar los resultados y así poder llegar a tener una señal útil para [30, 50, 58].

El método más común para tomar muestras de EEG para BCI con MI, es conectar los electrodos al cráneo del sujeto, luego se le presentan ciertas imágenes, con el objetivo que imagine cómo

realizaría el movimiento o la actividad que se le está mostrando, similares a cuando realiza realmente el movimiento, mientras más practica tenga la persona mejor serán los valores de las muestras [32, 46]. Es importante verificar y hacer comparaciones entre señales reales tomadas de bases de datos donde ya se han realizado los análisis de estas, demostrando la calidad y veracidad, y compararlas con señales imaginadas por la persona que ha realizado el experimento para verificar la robustez de la captura [30, 50, 58]. Con el auge de diseño de aplicaciones de BCI por parte de grandes laboratorios, se ha promovido diferente hardware de bajo costo para la adquisición de muestras con EEG, como son NeuroScan SynAmp, Neurosky MindSet y el Emotiv EPOC. Estas tres herramientas cuentan con especificaciones similares, entre las que se resaltan el hecho de ser portables y de fácil uso, tienen entre 8 y 64 canales para toma de muestras, cuentan con tiempo de autonomía de hasta 12 horas, y recientemente son herramientas muy utilizadas para la experimentación y desarrollo de interfaces cerebro – computador BCI. [30, 50, 58].

Las Figura 7 y 8 Ilustran sistemas de EEG para la adquisición de muestras de señales electromagnéticas del cerebro, estos sistemas son hardware bajo costos.

Figura 7 Sistema de EEG Neurosky MindSet. [70]

Figura 8 Sistema de EEG Emotiv G. Fuente: N. Webster. "Cutting edge brain control headset could cut UAE's road deaths". The National. 2018 https://www.thenational.ae/uae/cutting-edge-brain-control-headset-could-cut-uae-s-road-deaths-1.704624

3.1.1.2 Etapa 2: Procesamiento de Señales

3.1.1.2.1 Preprocesamiento

La función principal de la etapa de preprocesamiento en BCI es filtrar el ruido producido por artefactos u otras acciones no propias de la actividad, ya que los sistemas no invasivos de EEG son altamente propensos al ruido, una señal de interés podría estar superpuesta en el tiempo y frecuencia de múltiples señales, que no son parte de las señales producidas por el cerebro o alguna parte del cuerpo, produciendo así interferencias y datos innecesarios para el trabajo que se realiza. Si por el contrario se hace esta etapa de una manera óptima se puede tener así una reducción de datos erróneos y obtenido más información relevante para la investigación [10].

Las diferentes técnicas de filtrado frecuencial que se puede implementar en un sistema BCI para extraer información relacionada con las frecuencias del EEG son variadas, en esta etapa se utiliza diferentes tipos de diseños de filtros que abarcan una amplia gama de técnicas que utilizan algoritmos para eliminar de las señales de entrada las frecuencias no deseadas. Los filtros permiten eliminar frecuencias que contaminan y dificultan la interpretación de la señal. Estas deben hacerse procurando no sustraer aquellas frecuencias que forman parte esencial de la actividad eléctrica cerebral. Así, los filtros que más se reportan en la literatura son:

Resultados

Filtrado Pasa Bajas: permite filtrar las señales con un rango entre los 8 hasta los 12 HZ, este filtro tiene como características que permite el paso de las señales bajas de la frecuencia y bloquea las señales altas en frecuencia [30, 50, 58].

Filtrado Pasa Altas: filtra señales entre los rangos de 16 hasta los 24 HZ, permitiendo el paso de las señales altas de la frecuencia y bloquea las señales bajas de la frecuencia [30, 58].

Filtrado Pasa Bandas: se puede seleccionar una sección del espectro que se desea analizar o una frecuencia de corte donde los valores sean óptimos, este filtro es ideal ya que tiene unas bandas donde pasan los datos y el resto de las frecuencias son atenuadas, dando solo prioridad a un tramo de las frecuencias [30, 58].

Filtrado Rechaza Bandas: es un filtro que no permite el paso de señales cuyas frecuencias se encuentran comprendidas en las frecuencias de corte superior e inferior, creando así una banda de rechazo y dejando el resto del espectro libre para ser utilizado en la salida de la señal [30, 50, 58] , este filtro tiene como característica que filtra muy bien el ruido que es generado por señales externas, ya que se pueden eliminar picos en las frecuencias de las muestras tomadas por el EEG [30, 50, 58].

Es importante notar que las bandas de interés en las frecuencias pueden cambiar por el sujeto a quien se le toman las muestras, esto puede maximizar el rendimiento del BCI, ya que el preprocesamiento hecho con estos filtros puede mejorar las señales para que las extracciones de características tengan un proceso más eficaz para el desarrollo e implementación [30, 58].

Filtrado Espacial: La etapa de filtrado espacial se puede hacer utilizando diferentes métodos y combinaciones sobre una señal tomada previamente de un EEG. En esta etapa, las señales que fueron filtradas previamente en el preprocesamiento, donde se eliminaron los ruidos y las distorsiones, son transformadas del dominio del tiempo a el dominio de la frecuencia. Con esta técnica se podrán filtrar patrones de las señales en diferentes rangos de frecuencias, identificando los mejores patrones de comportamiento que puedan ser representados en cualidades de los datos de entrada [23, 40] A continuación, se explicarán métodos que son usados en la etapa de filtrado espacial:

Resultados

Filtrado ICA (Análisis de Componentes Independientes): es un método que recoge la información de respuesta a un estímulo y separa las señales ruidosas que se generaron dentro del EEG, extrayendo la información relevante, permitiendo la separación de las señales medidas en sus componentes independientes subyacentes fundamentales. Suponiendo que la señal de origen tiene una independencia estadística, los componentes del método no son ortogonales para su separación y únicamente se asume la independencia estadística de las componentes que se generan. Dado un conjunto de observaciones de variables aleatorias, se asume que son generadas por una combinación lineal de componentes independientes o en forma matricial, suponiendo que la matriz creada coincide con la fuente original, permitiendo encontrar una representación lineal de los datos; este tipo de representaciones permite obtener la estructura fundamental de los datos que son necesarios para la extracción de características y la separación de señales. Un punto a favor de ICA es que requiere un mínimo número de canales para funcionar bien, de igual manera, necesita inspección visual para seleccionar sus componentes manualmente para la corrección de datos [34, 66]

Filtrado PCA (análisis de componentes principales): intenta encontrar un conjunto de datos en términos de nuevas variables, utilizando matrices de covarianza. Explicando la variabilidad de los datos posibles correlacionados en un número menor de variables no correlacionadas conocido como el componente o eje principales, este se calcula con la mayor cantidad de datos obtenidos por las muestras del EEG, los datos restantes de las señales o la segunda varianza más grande es el segundo eje, y así sucesivamente. Por lo cual, una de las ventajas de PCA es dimensionar el grupo de datos, reteniendo las características que contribuyen con mayor varianza, manteniendo un orden de los componentes principales que producen las señales, dejando de lado los componentes de alto nivel y centrándose en los componentes de bajo de nivel, que son los que contiene los aspectos más importantes de la señal. Este método en sí sintetiza la información o reduce las dimensiones de número de variables. Es decir, ante una señal con muchas variables, el objetivo será reducirlas perdiendo la menor cantidad de información posible [67, 68].

Filtrado CSP (Patrones Espaciales Comunes): este es un método que se utiliza en el filtrado espacial con el cual se extrae características de las señales, esta técnica tiene como

particularidad que discrimina datos específicos de las señales de entrada, detectando patrones dentro de las señales del EEG, obteniendo así matrices con varianzas de clases máximas y mínimas al mismo tiempo, estas matrices proporcionan conjunto de patrones espaciales específicos de las señales, que reflejan la activación de las áreas corticales durante el movimiento, obteniendo matrices de la señal de entrada, es decir que el primer componente de los vectores que se crearon, que son las filas, tiene mayor varianza de tipo máximo y las columnas tienen varianzas de tipo mínimo, la interpretación más común es que las filas pueden ser vistas como los filtros espaciales estacionarios, mientras que las columnas pueden ser vistas como los patrones espaciales comunes. CSP no requiere una selección prioritaria de las bandas de frecuencia de las señales que se van a filtrar, pero si se aplica este tipo de filtros a cualquier banda de frecuencia en un rango no especificado, los resultados no serán óptimos, pero si por el contrario se selecciona un rango más estrecho en las bandas de frecuencias da una mejor clasificación de las señales [32, 48].

Hay que mencionar además que CSP tiene diferentes variaciones, las cuales están siendo utilizadas como técnicas de filtrados espaciales, obteniendo mejoras en su rendimiento. Algunas de estas son RCSP (Regulación de Patrones Espaciales Comunes) [49, 50], que es un método más robusto que el CSP y menos sensible al ruido, teniendo mayor capacidad para el filtrado de las señales. Aunque su algoritmo es similar al CSP, este agrega dos nuevos parámetros de regularización involucrados en la regulación de las estimaciones de covarianza, uno de estos valores agrega mayor estabilidad en la estimación de las matrices y el otro valor reduce la desviación en las estimaciones, teniendo una mayor precisión que su antecesor y haciendo que el algoritmo tenga una mejor regularización. Otra variación del CSP es el método SBCSP (Sub Bandas de Patrones Espaciales Comunes), es un método más empírico, que utiliza el mismo algoritmo del CSP clásico, la diferencia está en que la señal de entrada que se utiliza en el procesamiento de los datos es descompuesta en pequeñas sub-bandas y es filtrada usando un banco de filtros [49, 50], así cada sub-banda seleccionada en pequeñas muestras tiene un valor diferente en un rango de frecuencias, por los tanto la señal es transformada en la sub-banda K-ésima, obteniendo valores más grandes de las resultados de las matrices del

algoritmo CSP, es decir la información será más discriminada y tendrá un mayor conjunto de datos con resultados más precisos [49, 50].

Filtrado Laplaciano: se basa en tomar las señales producidas por los electrodos conectados para la toma de muestras del EEG y es normalizado con cada señal de cada electrodo que rodea el otro, y así sucesivamente se va promediando las potencias de los electrodos vecinos horizontales y verticales, o llamado de otra manera la potencia del electrodo k-ésimo, y dando el promedio de la actividad de referencia de las muestras tomadas [40].

Filtro CAR (Referencia de Media Común): es un método que elimina el ruido de las señales y tiene un costo computacional bajo, hace referencia al promedio de las señales tomadas por los electrodos conectados para la toma del EEG, restando de cada muestra el valor promedio de la señal a través de todos los electrodos. Por lo tanto, el promedio de toda la actividad representa una estimación de la actividad cerebral, donde ese potencial del electrodo k-ésimo muestra el promedio de la actividad de la señal de entrada al sistema [34, 40, 66].

3.1.1.2.2 Extracción de Características:

La extracción de características es una técnica que consiste en la realización de distintas combinaciones y transformaciones de las señales de EEG, con el fin de obtener representaciones con características invariables y discriminativas, para conformar un conjunto de datos con la mejor calidad para la etapa de clasificación. La Extracción de Características puede hacerse ya sea en el dominio del tiempo o en el dominio de la frecuencia, las características son cada uno de los valores que definen intrínsecamente los distintos estados del individuo, se explicará a continuación modelos usados frecuentemente en la Extracción de características en sistemas BCI [30, 50, 58].

Método Autorregresivo (AR): en este método se calcula la densidad espectral de potencia (PSD) de la señal tomada, este describe la potencia en rango de la frecuencia capturada en un proceso estocástico donde se toman magnitudes de los datos que varían en el tiempo, este método divide la señal en bloque de muestras conocidas como ventaneos y luego, en cada ventana se calcula la magnitud utilizando la transformada rápida de Fourier (FFT) [6, 20, 67,68], estimando la función de autocorrelación de la señal, dando como resultado un valor estimado en forma de PSD, en investigaciones se ha evidenciado que con ventanas más extensas, donde se tiene

mayor cantidad de muestras de la señal, se pueden obtener una mejor calidad de los datos, ya que existe mayor capacidad para promediar los datos que están dentro de las ventanas, y así la varianza es más grande, dando una calidad de las muestras de salida unas características más acertadas a las originales [67, 68].

Transformada de Wavelet: es una herramienta matemática que permite analizar señales no estacionarias y de cambios rápidos, A partir de transformaciones y construcciones de la función original, este método realiza una estructura de las señales en dominios del tiempo y la frecuencia por medio de ventanas con la combinación de la información frecuencia-tiempo se mejoran la clasificación de las señales dando como resultado mayor precisión , la transformada de wavelet utiliza ambas técnicas teniendo la información contenida en la frecuencia y en el tiempo [2], Una transformada wavelet utiliza una ventana variable en su tamaño lo que le permite realizar mayores mapeos de las señales en esos segmentos donde se requiere mayor precisión en las frecuencias altas o bajas, luego la señal inicia un proceso de separación de datos en porciones de frecuencias, haciendo este proceso en reiteradas ocasiones hasta que se haya descompuesto la señal en tres o más niveles o grupos de señales que están en función de la frecuencia, el tiempo y la amplitud, luego de este proceso se facilita el procesamiento y la discriminación de la información, dando como resultado la reconstrucción de la señal original. El uso de los coeficientes Wavelet, como características para la clasificación de señales en sistemas BCI ha mostrado buenos resultados, por lo cual es ampliamente usado [62, 63].

Dimensión Fractal (DF): en este método la señal será reconstruida por señales más pequeñas de la misma, hasta que se haga una reconstrucción o una reproducción de la original, hay muchas técnicas con las cuales se pueden estimar una dimensión fractal, entre las que se destacan el Método Higuchi y el Método Katz:

Método Higuchi: es una sumatoria de datos que están en función del tiempo, este algoritmo crea nuevas formas de la onda de la señal original en secuencias más pequeñas, creando un vector con muestras que tienen inicio y retardos en tiempos discretos, posterior a este paso se calcula la longitud de la curva de la señal, para obtener los promedios de los datos en factores normalizados de las secuencias, con estos valores se pueden hallar los promedios de todas las

longitudes y así convertir la señal en dimensiones fractales y calcular sus aproximaciones lineales en mínimos dato [30, 50, 58].

Método Katz: Encuentra la dimensión fractal, calculando la longitud de la curva de la señal, haciendo la suma de las distancias euclidianas (Las dimensiones euclidianas son todas ortogonales, formando ángulos rectos entre sí y se refieren al espacio físico con las componentes (X, Y y Z), entre varios datos sucesivos, y siendo estos divididos por las distancias más largas de los datos de las muestras, así con este paso se normalizan las tramas de datos y se puede hallar la dimensión fractal de señal de origen. El cálculo de la Dimensión fractal permite determinar las características de las señales del EEG, pero para obtener resultados más acertados se deben utilizar fractogramas más pequeños con los
cuales las señales sean reconstruidas mejor [20, 30, 50, 58].

3.1.1.2.3 Modelos de Clasificación

La Clasificación de un sistema BCI se emplea para identificar y reconocer patrones de las actividades del EEG, identificando la intensión del sujeto basándose en las características que tienen los datos que se están recopilando de las señales y las asocia a tareas mentales. Existen dos técnicas de Clasificación que son populares entre las investigaciones de BCI, que son los clasificadores lineales y los clasificadores no lineales [62, 63].

Los Clasificadores Lineales suelen ser más utilizados principalmente por su algoritmo robusto y los pocos parámetros de carga computacional que tienen, ya que los datos son separados linealmente en planos (Hiperplanos) en diferentes regiones (clase) de las señales de entrada, promediando los resultados de la clasificación con el fin de obtener unos datos estadísticamente más acertados. Por otro lado, los clasificadores NO Lineales crean un plano con más dimensiones o zonas arbitrarias con el objetivo hacer regiones (clase) para realizar la separación de datos, tiene como características que deben procesar mayores cantidades de flujos de datos y por lo que su carga computacional es más grande. A continuación, se introducen los modelos de clasificación más usados en sistemas BCI:

Análisis de Discriminante Lineal (LDA): es también conocido con el LDA de Fisher, es uno de los Clasificadores Lineales más usados para BCI, los datos son separados linealmente en planos

(Hiperplanos) en diferentes regiones (clase) de las señales, donde sus vectores de características depende exclusivamente de donde quede ubicado en el Hiperplano, LDA asume los datos como matrices de covarianzas (asociaciones lineales de las variables), para crear Hiperplanos de donde se clasifican los datos se deben maximizar las separación de las regiones (clase) de las otras y minimizar las varianzas (evaluar la cantidad de variaciones en los datos debido a factores aleatorios) en las regiones (clase), tiene grandes beneficios ya que es muy fácil de configurar y su carga computaciones es muy baja. El principal inconveniente que tiene el Método LDA es que es un sistema totalmente lineal limitado para proporcionar resultados con datos EEG no lineales [48, 65]

Máquina de vectores de soporte (SVM): es un clasificador que trabaja de manera similar al método de clasificación LDA. Sus datos son separados linealmente en un plano (Hiperplano) en diferentes regiones (clase) binarias (que solo genera un Hiperplano), con el objetivo de identificar vectores de características en las diferentes regiones, este clasificador define el Hiperplano que maximiza la distancia entre las separación de las regiones (clase), con márgenes más extensas, dando más espacio para evaluar mayor cantidad de variaciones de datos de características proyectándose en un plano dimensional más alto, donde se pueden realizar clasificaciones con mayor carga de entrenamiento de generalización de los datos de entrada del EEG, este método es utilizado con gran éxito ya que su carga computacional es [48, 63, 64].

K-vecinos más Cercanos (K-NN): es un método que utiliza la técnica donde se determinan las distancias entre un punto a clasificar creando un vector en una región de prueba en el espacio de características y un conjunto de datos que sirven para entrenamiento, con las distancias ya medidas se pueden calcular los K-vecinos y con ellos diferenciar las regiones (clase) a las que puede pertenecer y cuáles son las más cercanas, este tipo de distancias son usualmente utilizadas para medir patrones de datos que producirán límites de decisión no lineales, teniendo la probabilidad de que el error en la decisión se reduzca, tomando en cuenta a los K-vecinos en la clasificación. Este método tiene una mayor sensibilidad a la dimensionalidad [30, 32, 50, 58], que tiene como característica aumentar sus dimensiones del espacio o regiones en forma exponencial, haciendo que los datos se vuelvan dispersos, causando problemas para ser medido

el vector de características, pero cuando se utiliza con clasificación de característica con una tasa baja, la dimensión en sus vectores ha demostrado ser [32,55].

Red Neuronal Artificial (ANN): son diseñadas como una similitud a un sistema nervioso, donde se espera que la ANN tenga la capacidad de identificar patrones de entradas de datos y patrones de estados de salida (reales y muestras tomadas), en medio de este proceso la ANN tendrá la capacidad de procesar datos por medio de conexiones de nodos que son denominados capas ocultas, las cuales tienen la capacidad de aprendizaje a partir de un conjunto de patrones de entrenamiento matemáticos, este tipo de procesamiento le permite resolver problemas que no son linealmente [30, 50, 58]**,** la ANN consta de una capa de entrada, una o varias capas ocultas y una capa de salida, dándole la capacidad de reconocer patrones, ya que tiene la capacidad de aprender de los datos, utilizando un algoritmo de entrenamiento que permite actualizarse hasta que la tasa de errores de la clasificación alcance un estado estable, una vez que la ANN entra en un estado estable, inicia el cálculo de un vector en cada neurona artificial que procesan información por medio de funciones no lineales, como los datos de salida son conocidos por medio de vectores que son ingresados a la ANN, la red realiza comparaciones con los datos que clasificó en cada una de sus capas y si tiene errores realiza una nueva etapa de entrenamiento buscando minimizar estos, realizando actualizaciones hasta que la diferencia entre la salida esperada y la real sean los más mínimo posibles y los datos sean óptimos para un sistema BCI [48, 58, 63].

Deep Learning (Aprendizaje Profundo): el aprendizaje profundo tiene las facultades de determinar, automáticamente, la mayor cantidad de características no relacionadas de una amplia cantidad de datos que pudieron ser omitidos en métodos previos al filtrado, gracias a su modelado de abstracciones de alto nivel con transformaciones no lineales. Una de las técnicas de aprendizaje profundo con redes neuronales son las arquitecturas convolucionales (CNN) [48, 58, 63], que consiste en un sistema de múltiples capas de filtros convolucionales de una o varias capaz, donde se realiza un mapeo causal no lineal.

Recientemente, las investigaciones sobre clasificación de señales de EEG, están utilizando redes neuronales convolucionales (CNN) para clasificar múltiples clases de señales obtenidas,

acompañado de varios tipos de filtrados como lo son Patrón Espacial Común (CSP), Análisis De Componentes Principales (PCA), Extracción de características con La Transformada Wavelet, entre otros; este tipo de métodos mejora sustancialmente la calidad de los señales para la clasificación, los resultados que se están obteniendo muestran que los CNN pueden aprender características discriminantes para la clasificación de múltiples clases de datos de EEG [64, 69]. Las técnicas de aprendizaje profundo han logrado obtener capacidades notables en el mejoramiento de clasificación de datos ya que con los nuevos dispositivos (hardware) se ha logrado un rendimiento considerable en áreas del conocimiento, como la inteligencia artificial y visión por computador, en estos sistemas se utilizan métodos de análisis comparativos donde se analizan diferentes tipos de arquitecturas de redes neuronales profundas (DNN), utilizando una técnica llamada Pooling para reducir dimensiones, siendo Max-Pooling el más utilizado en el estado de la técnica, aunque otras funciones de agrupación pueden mejorar el rendimiento de entrenamiento que es característico en las redes neuronales; también la elección de la función de activación es importante, para que la red neuronal maneje el problema de la disminución del gradiente, esta es una de las claves para una buena limitación del flujo decreciente del gradiente [46, 63, 65].

3.1.1.3 Etapa 3: Dispositivos de Salida

Desde la perspectiva de los sistemas BCI, un dispositivo de salida está ligado a un conjunto de herramientas tecnológicas, equipo o softwares, que recopilan la información procedente del sistema cerebro computador, estos dispositivos pueden ser: celulares, tabletas, computadores, prótesis motoras y robotizadas como son sillas de ruedas o brazos robóticos, algunas interfaces ligadas al manejo de automóviles.

De igual manera se cuenta con dispositivos como video juegos o aplicativos que pueden estar almacenadas de manera local en un celular o de manera remota utilizando bases de datos que se encuentran en la nube para el uso de los usuarios de los sistemas BCI, también sistemas de seguridad donde se recopila las señales procedentes de BCI como firmas para los procesos de identificación y autenticación de usuarios ante un servicio [5].

3.1.1.3.1 Dispositivos de controles Cercanos

Los dispositivos de controles cercanos también pueden ser conocidos como los dispositivos finales y aplicativos, estos son los usados por los usuarios finales de los sistemas BCI:

- Celulares Computadores
- Sillas de ruedas
- Video Juegos
- Manejo de automóviles
- Dispositivos de controles Remotos
- Prótesis motoras y robóticas
- Sistemas de seguridad en la nube
- Video juegos en la nube
- Aplicaciones

3.1.1.3.2 Transporte de información

Los sistemas BCI utilizan tecnología tradicionales para conectarse entre los usuarios y los host que hospedan las interfaces, dichos sistemas se conecta a internet por medio de ondas electromagnéticas o Wifi, también pueden tener conexiones utilizando los medios transmisión como son fibras ópticas, UTP y Coaxial, de igual manera utiliza los modelos de referencia OSI y TCP/IP, donde los protocolos de red definen las reglas que se utilizan para las comunicaciones en hardware y software, ya que estos permiten que varios dispositivos se conecten por medio de redes, esperando que su implementación permita una transmisión segura de datos donde se tiene autenticación, cifrado e integridad. Para ello, un emisor y un receptor (identificado) recibe la información de manera garantizada, donde se tiene fluidez y velocidad de los datos trasmitidos en las aplicaciones.

Cuando se habla de protocolos que utiliza cada una de las capas de los modelos de referencia tienen diferentes funciones, aunque el que se utiliza para la trasmisión de datos es el modelo TCP/IP, donde se tiene un conjunto de protocolos estándar que pueden ser utilizados por diferentes puertos, servicios, equipos y tecnologías. En cada una de sus capas, ya que está

diseñado para la trasmisión desde las capas inferiores hasta las capas superiores, donde la capa inferior de Acceso a la red utiliza el protocolo Ethernet y WLAN, la capa de internet utiliza los protocolos IPv4 y IPv6, la capa de transporte utiliza los TCP y UDP y en la capa de aplicación HTTP, DNS, DHCP y FTP, así los datos van escalando y llegan sus destinos en los sistemas [4, 5].

3.1.1.3.3 Lenguajes de Programación

Los sistemas BCI utilizan un conjunto de diferentes tecnologías de hardware y con ello pueden contener diferentes firmwares que controla estos dispositivos, para ellos se trabajan con diferentes lenguajes de programación que están enfocados para el desarrollo de las aplicaciones que conforma en total las interfaces cerebro computador, gran parte de los diseños de las aplicaciones que se hacen con este tipo de sistema son diseñadas y programadas con las librerías de Python y C++, ya sea para los diseños de los firmwares de los diademas para la recolección de la información de los usuarios está construido en C++, los diseños y aplicativos de usuario son diseñados con las librerías de Python enfocadas en machine Learning y Deep Learning, con el objetivo de clasificar los datos que se producen en la interface, es importante utilizar este tipo de software libre ya que las comunidades científicas han diseñado un gran cantidad de software libre para la utilización de la exploración científica. Finalizando con las aplicaciones web que le dan una experiencia de usuario totalmente satisfactoria a las personas que utilizan estos sistemas, para este tipo de diseños se utilizan PHP, HTML, CSS y JavaScript, junto a los diseños web se pueden generar gran cantidad de información que puede ser recopilada para mejorar las experiencias de usuario y para ello las base de datos como SQL y MySQL y el lenguaje de programación R compila información necesarias que permite configuraciones, interacciones mucho más agradables enfocadas a las necesidades del usuario [1, 4, 5].

3.1.1.3.4 Servicios de Almacenamiento Local y la Nube

Los diseños de los sistemas BCI pueden tener diferentes tipos de equipos de almacenamiento de información ya es estos se pueden encontrar de manera local o remota, esto depende de las características del diseño y sus aplicaciones, la mayor parte de la información recopilada por las interfaces cerebro computador se encuentran en servidores personales de los usuarios donde

se implementa el software que recopila y clasifica la información y posterior las envía a los dispositivos finales que es donde se utiliza los datos en las apps, estos servidores tienen características de procesamiento estilo Workstation, un ejemplo de estos equipos sería una Dell Precisión con CPU T5810, equipado con procesadores Intel Xeon de 3 GHz, 8 núcleos, arquitectura de 64 bits, 16 GB de RAM también se utilizó GPU NVIDIA GFORCE 1080 TI y discos duro de una tera de almacenamiento, este tipo de equipos brinda una cantidad de procesamiento para procesos mucho más robusto, este tipo de arquitectura de hardware se puede implementar de manera remota utilizando la nube para poder tener sistemas con mayor escalabilidad ya que es normal que las interfaces BCI procesen grandes cantidades de información y con un sistema en la nube es más sencillo poder darle mejores características de procesamiento y almacenamiento si es necesario, esta es una de las características que tiene los servicios de nube ya que se pueden implementar arquitecturas con procesadores de alta gama como son los Intel Core I9, memorias RAM de 32GB y tarjetas gráficas GForce RTX [3].

3.1.2 Levantamiento de activos, amenazas y vulnerabilidades

En este proceso, se realizó una breve descripción de las etapas (figura 9) y sus componentes tecnológicos, seguidamente, las vulnerabilidades y amenazas que éstos pueden tener.

3.1.2.1 Cronología del Proceso de Montaje de un Sistemas BCI

Resultados

Amenazas y Ataques a los Componentes BCI

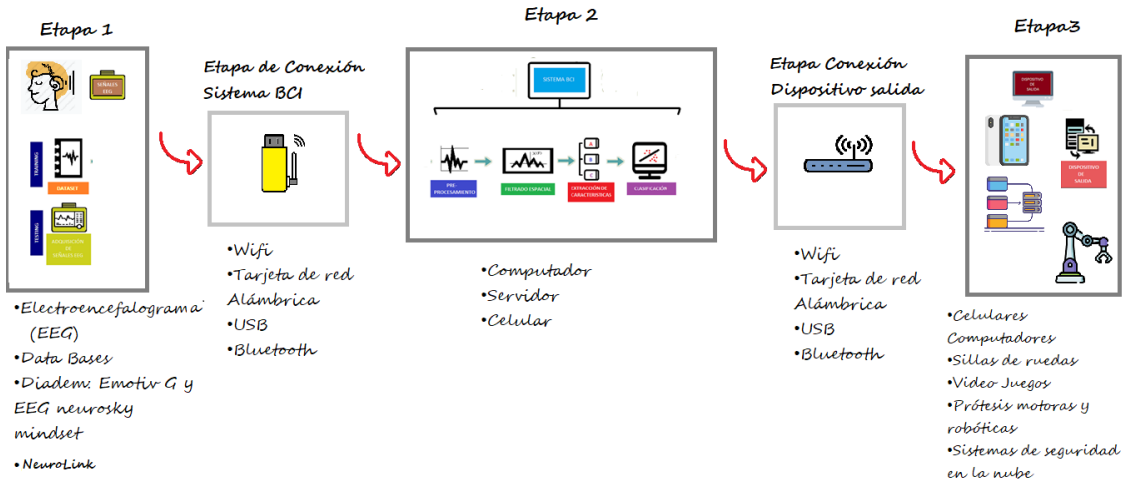


Figura 9 Componentes De Un Sistema BCI. Fuente Propia

Etapa 1

En esta etapa, se puede tener hardware para la adquisición de los datos como lo son sistema EEG Emotiv G y Sistema EEG neurosky mindset, estos son equipos que toman muestras de datos de manera externa en el cráneo y no requieren ningún procedimiento quirúrgico para su instalación y uso, estos son sistemas comerciales y que se utilizan en el mercado, este tipo de dispositivos pueden ser víctimas de ataques de malware para el firmware que pueden cifrar los datos del equipo donde se puede cambiar sus configuraciones de fábrica y códigos fuente, firmas digitales para la conexión con los dispositivos finales y aplicaciones, de igual manera el cifrado de éste, imposibilitando su funcionamiento y compilar información del equipo en segundo plano (background) [1, 4, 5].

Por otro lado se encuentran los sistemas BCI Interno, estos son pequeños chips que se instala de manera interna en el cráneo del paciente y deben implantarse de manera quirúrgica por un especialista, estos dispositivos de igual manera 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, de manera comercial se pueden encontrar referencia como Neurlink, y también pueden se víctimas de ataques cibernéticos, donde se pueden generar interferencias en el envío de datos y fallas de fuente de energía[64].

Resultados

Etapa de conexión Sistema BCI

Los sistemas sistema EEG Emotiv G y Sistema EEG neurosky mindset, se pueden comunicar a un dispositivo que recopila la información de dos formas, utilizando redes inalámbricas Wifi y bluetooth, en este tipo de comunicaciones el atacante puede interceptar la comunicación utilizando Man in the Middle, donde el atacante puede hacerse pasar por el dispositivo que recibe la información por medio de un ARP Spoofing, y con el dispositivo que recibe la información puede hacer el mismo proceso, donde toda la información va llegar un dispositivo intermediario que puede recopilar, modificar e inyectar la información a los diferentes dispositivos. Así mismo, se pueden generar ataques de negación de servicio – DoS/DDoS, lo cual imposibilita cualquier actividad en esta etapa [1, 4, 5].

Etapa 2

Dispositivo BCI, este dispositivo recopila la información y en éste se hace las etapas de procesamiento, extracción de características y clasificación, este sistema se cumplen varios procesos donde los datos serán filtrados de maneras que puedan identificar patrones y estímulos que produce el usuario y son recopilados por las diademas sistema EEG Emotiv G y Sistema EEG neurosky mindset, estos procesos deben tener niveles de seguridad ya que estos dispositivos pueden ser celulares o computadores que recopilan la información, así que están expuestos ataques de robo de credenciales por medio de ingeniería social o phishing, también puede tener brechas de seguridad ya que no tiene niveles altos de protección de datos y contraseñas como pueden ser autenticaciones doble factor, si el atacante tiene acceso al sistema BCI donde se hacen los procesos de este, podría inyectar códigos maliciosos (malware), donde los parámetros originales del sistema dejen de funcionar, haciendo que el sistema trabaje de manera defectuosa y produciendo posibles daños a equipos finales o en el peor de los casos el usuario podría sufrir daños físicos, de igual manera este tipo de estímulos podrían generar en el usuario respuestas sobre información privada y confidencial, como pueden ser claves, preferencias de compras e identificación de personas, este tipo de ataque se denomina Brainspyware [1, 4, 5].

Resultados

Etapa Conexión dispositivo de salida

Comunicación BCI con los dispositivos finales, acá se pueden tener ataques similares a los de la etapa 2 donde se puede realizar un Man in the Middle y ARP Spoofing, la diferencia está en el alcance en este punto de la información que se puede filtrar e inyectar y como el dispositivo final puede quedar expuesto a un ataque de un nivel mayor, ya que es el dispositivo final quien realiza la acción que se desea realizar en el sistema BCI y con este podría generar un nivel de daño más alto [1, 4, 5].

Etapa 3

Ataque Dispositivo Final, el atacante puede tener acceso a diferentes equipos: como son computadores, servidores, sillas de ruedas, manos robóticas, video juego y celulares, de igual manera servicios como son bases de datos y aplicaciones, utilizando técnicas y ataques como pueden ser: Ramsomware, malware, infiltración de información, SQL injection y denegación de servicios estilo: DDoS y Jamming attack.

En la figura 10 se puede observar el consolidado de los diferentes ataques a través de las etapas de procesamiento de un BCI [35, 58].

3.1.2.2 Vulnerabilidades

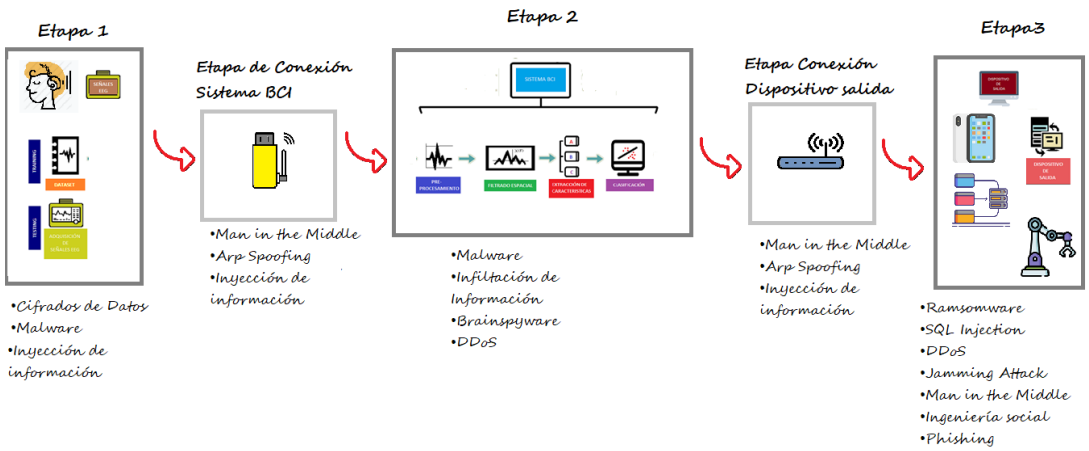


Figura 10 Tipos De Ataques De Un Sistema BCI, Fuente Propia

Resultados

Una vulnerabilidad se define como un hueco o fallo de seguridad, la falta o falencia de un control sobre un elemento o sistema determinado. Dado lo anterior, a continuación de lista una serie de vulnerabilidades posibles en un sistema BCI, las cuales pueden ser explotadas por las amenazas ya descritas:

- Falencia en el control de acceso: Identificación, autenticación, autorización
- Falta de parches en dispositivos finales
- Indebida configuración de accesos alámbricos e inalámbricos.
- Falencia o falta de capacitación de las personas con respecto a la identificación de riesgos.
- Antivirus mal configurado y/o falta de éste.
- Falla o falta de monitoreo de la red.
- No configuración del control de ejecución en las bases de datos.
- Deficiencia en la restricción de comandos privilegiados
- No implementación de un sistema tipo IPS/IDS.
- Falta de actualización de los sistemas y plataformas.

3.1.3 Obtención del mapa de riesgos

Una vez identificados los componentes tecnológicos, algunas las amenazas y vulnerabilidades, se procedió a realizar el mapa de riesgos.

3.1.3.1 Ataques informáticos sobre componentes BCI

En consideración de las diversas tecnologías e información que puede ser generada en los sistemas BCI, las amenazas informáticas se pueden presentar de diferentes formas, algunas de ellas con:

- *Man in the Middle*: Este ataque consiste en capturar las comunicaciones que hay entre 2 equipos o sistemas, con ello, poder escuchar, modificar o redireccionar los datos que cursan [28].

- *ARP Spoofing:* Este ataque hace una modificación de las tablas ARP (falsificación) permitiendo que un tercero pueda capturar los datos que circulan por la red [27].

- *Códigos maliciosos (malware):* Software construido para fines malintencionados, dentro de las funciones se encuentra el robo de datos, alteración de sistemas, bloqueo, cifrado y pedida de rescate [27, 51].

- *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 [27].

- *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 que esta almacenada [27].

- *Denegación de servicios (DoS):* la negación de servicio se puede presentar de diferentes formas, la más común es el consumo alto de recurso como el ancho de banda, CPU o Memoria, también se puede presentar cuando se elimina o modifica algún archivo de configuración, el resultado final es no entregar el servicio a los sistemas o personas que requieren el acceso [27].

- I*nyección de código:* esto se puede realizar hacia el hardware y lenguajes de programación, permitiendo la inyección de código a las aplicaciones, generando una pérdida potencial del funcionamiento o generando otras funcionalidades no previstas en la construcción inicial de las aplicación y en las funcionalidades del hardware, donde pueden tener perdidas de energía (agotamiento de energía) y su funcionamiento puede deteriorarse o tener una falla total [16, 27, 64].

Los ataques informáticos cuando explotan una vulnerabilidad en un sistema, se genera un riesgo, y para ello, es necesario realizar una gestión adecuada de los posibles impactos que se puedan generar. La gestión de riesgos es un proceso continuo e interactivo que permite la identificación de posibles amenazas sobre activos de información y a partir de ello, se obtiene los posibles impactos negativos que puedan generar sobre un sistema de referencia, así, lograr generar un posible plan de tratamiento [26].

Resultados

Para la obtención de los resultados de riesgos se ejecutaron las siguientes fases (figura 11):

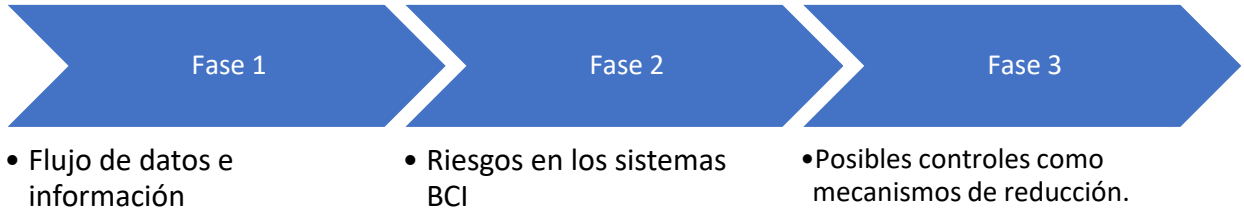


Figura 11 Metodología que se siguió para la obtención de resultados asociados al mapa de riesgos. Fuente propia

Para la fase 1, se ha estructura el tipo de datos e información que puede tener un sistema BCI, para ello fue necesario conocer el posible flujo de datos que se generan en las diferentes etapas del sistema y con ello, conocer un poco más la tecnología y sus componentes.

Con respecto a la fase 2, y partiendo de los datos e información que fluye a través del sistema, así como algunas de las amenazas informática, se obtiene un mapa de riesgos, esto se realizó con una matriz 5x5 (tabla 2), iniciando con un levantamiento de activos de información que están asociados a un BCI, luego se hace una revisión de las posibles amenazas y vulnerabilidades, seguidamente se hace una calificación con respecto a la probabilidad de ocurrencia e impacto que puede generar. Dicho mapa de riesgos considera 4 zonas de impacto a saber:

- Zona verde: Riesgos bajos
- Zona Amarilla: riesgo moderado
- Zona Naranja: riesgo alto
- Zona roja: riesgo extremo

Resultados

Probabilidad		Consecuencia				
	valor	Insignificante	Menor	Intermedio	Mayor	Superior
		1	2	3	4	5
Casi seguro	5					
Probable	4					
Posible	3					
Improbable	2					
Raro	1					

Tabla 2 Mapa de riesgos de usado para el cálculo final. Fuente propia

Para el cálculo de los riesgos, y en consideración de la matriz, la probabilidad de ocurrencia va de 1 a 5, siendo 1 la menor probabilidad y 5 la mayor, así mismo para el cálculo de la consecuencia o impacto (1 es el menor impacto y 5 el mayor).

Finalmente, se generan algunas recomendaciones de protección que buscan la reducción de posibles riesgos sobre los sistemas BCI. Estas recomendaciones se asociación directamente a los riesgos que se encontraron en las zonas alta y extrema, considerando lo riesgos bajos (amarillos y verdes) como aquellos que pueden ser asumidos [24, 25].

3.1.3.2 Análisis de riesgos

En consideración del flujo de datos y los activos relacionados en las diferentes fases, el proceso de riesgos establece que a los activos de información debe buscarse las posibles amenazas y vulnerabilidades, y con ello, indicar la probabilidad de ocurrencia y el impacto que pueden generar en un activo determinado (NIST, 2012), 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, generando más completitud a la hora de tomar una decisión con respecto a los niveles de exposición de los riesgos [26]

Por lo anterior, se ejecutan los siguientes pasos de acuerdo con el flujo de información:

Resultados

a) Inventario de activos.

b) Amenazas y vulnerabilidades

c) Construcción del escenario de riesgos

d) Calificación de probabilidad e impacto.

e) Obtención del mapa de riesgos.

Se inicia entonces con los activos de información, estos son claves y están relacionados con cada una de las fases y el flujo de información que pueda tener, para lo cual, los siguientes son los activos relacionados más relevantes:

- Sistema EEG
- Protocolos Wifi y Bluetooth
- lenguaje de programación
- Página Web
- Base de datos
- Almacenamiento local o Nube
- Personas

Con respecto a las amenazas, se tomaron las ya definidas como son el Man in the Middle, ARP Spoofing, Códigos maliciosos (Malware), Robo o alteración de información, SQL injection, Denegación de servicios (DoS) e Inyección de códigos, adicional esta la ingeniería social, la cual 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.

Resultados

Una vez establecido el panorama de riesgos, se obtuvieron 17 riesgos (tabla 3), los cuales fueron calificados en probabilidad e impacto:

No.	**Escenario de riesgos**	**PROBABILIDAD**	**IMPACTO INFORMACIÓN**
1	Posibilidad que la amenaza: Acceso físico no autorizado/indebido, afecte el activo: Servidor Base de Datos	3	4
2	Posibilidad que la amenaza: Acceso físico no autorizado/indebido, afecte el activo: Emotiv G	3	4
3	Posibilidad que la amenaza: Acceso físico no autorizado/indebido, afecte el activo: EEG Neurosky Mindset	3	4
4	Posibilidad que la amenaza: Acceso físico no autorizado/indebido, afecte el activo: Tarjeta de red inalámbrica USB	4	4
5	Posibilidad que la amenaza: Acceso físico no autorizado/indebido, afecte el activo: Bluetooth	4	4
6	Posibilidad que la amenaza: Acceso físico no autorizado/indebido, afecte el activo: Servidor Ubuntu	3	4
7	Posibilidad que la amenaza: Acceso físico no autorizado/indebido, afecte el activo: Computador	4	4

Resultados

8	Posibilidad que la amenaza: Acceso físico no autorizado/indebido, afecte el activo: Sistema en la Nube	2	4
9	Posibilidad que la amenaza: Acceso físico no autorizado/indebido, afecte el activo: Prótesis Motora	2	4
10	Posibilidad que la amenaza: Acceso físico no autorizado/indebido, afecte el activo: Robot	2	2
11	Posibilidad que la amenaza: Ataque informático de tipo: SQL injection, afecte el activo: Tarjeta de red inalámbrica USB	3	2
12	Posibilidad que la amenaza: Ataque informático de tipo: SQL injection, afecte el activo: Bluetooth	3	2
13	Posibilidad que la amenaza: Ataque informático de tipo: SQL injection, afecte el activo: Servidor Ubuntu	3	4
14	Posibilidad que la amenaza: Ataque informático de tipo: SQL injection, afecte el activo: Robot	1	2
15	Posibilidad que la amenaza: Ataque informático de tipo: DNS Reflexion/Amplification., afecte el activo: Servidor Base de Datos	3	4
16	Posibilidad que la amenaza: Ataque informático de tipo: DNS	3	2

Resultados

	Reflexion/Amplification., afecte el activo: Computador		
17	Posibilidad que la amenaza: Ataque informático de tipo: DoS/DDoS, afecte el activo: Electroencefalograma	1	4
18	Posibilidad que la amenaza: Ataque informático de tipo: DoS/DDoS, afecte el activo: Servidor Base de Datos	3	4
19	Posibilidad que la amenaza: Ataque informático de tipo: DoS/DDoS, afecte el activo: Celular	3	4
20	Posibilidad que la amenaza: Ataque informático de tipo: DoS/DDoS, afecte el activo: Computador	3	4
21	Posibilidad que la amenaza: Ataque informático de tipo: buffer overflow, afecte el activo: Electroencefalograma	1	4
22	Posibilidad que la amenaza: Ataque informático de tipo: buffer overflow, afecte el activo: Servidor Base de Datos	3	4
23	Posibilidad que la amenaza: Ataque informático de tipo: buffer overflow, afecte el activo: Tarjeta de red inalámbrica USB	1	4
24	Posibilidad que la amenaza: Ataque informático de tipo: buffer overflow, afecte el activo: Bluetooth	1	4

Resultados

25	Posibilidad que la amenaza: Ataque informático de tipo: buffer overflow, afecte el activo: Servidor Ubuntu	4	4
26	Posibilidad que la amenaza: Ataque informático de tipo: buffer overflow, afecte el activo: Celular	1	4
27	Posibilidad que la amenaza: Ataque informático de tipo: buffer overflow, afecte el activo: Computador	3	4
28	Posibilidad que la amenaza: Ataque informático de tipo: buffer overflow, afecte el activo: Robot	2	2
29	Posibilidad que la amenaza: Ataque de tipo: Ingeniería social, afecte el activo: Emotiv G	3	2
30	Posibilidad que la amenaza: Ataque de tipo: Ingeniería social, afecte el activo: EEG Neurosky Mindset	3	2
31	Posibilidad que la amenaza: Ataque de tipo: Ingeniería social, afecte el activo: Tarjeta de red Inalámbrica USB	2	4
32	Posibilidad que la amenaza: Ataque de tipo: Ingeniería social, afecte el activo: Bluetooth	2	4
33	Posibilidad que la amenaza: Ataque de tipo: Ingeniería social, afecte el activo: Servidor Ubuntu	3	4

Resultados

34	Posibilidad que la amenaza: Ataque de tipo: Ingeniería social, afecte el activo: Sistema en la Nube	3	4
35	Posibilidad que la amenaza: Ataque de tipo: Ingeniería social, afecte el activo: prótesis Motora	2	4
36	Posibilidad que la amenaza: Ataque de tipo: Ingeniería social, afecte el activo: Robot	2	4
37	Posibilidad que la amenaza: Ataque informático de tipo: tcp syn attack, afecte el activo: Servidor Ubuntu	4	2
38	Posibilidad que la amenaza: Ataque informático de tipo: tcp syn attack, afecte el activo: Celular	3	2
39	Posibilidad que la amenaza: Ataque informático de tipo: tcp syn attack, afecte el activo: Computador	4	2
40	Posibilidad que la amenaza: Ataque informático de tipo: tcp syn attack, afecte el activo: Sistema en la Nube	3	2
41	Posibilidad que la amenaza: Ataque informático de tipo: tcp syn attack, afecte el activo: prótesis Motora	2	2
42	Posibilidad que la amenaza: Ataque informático de tipo: tcp syn attack, afecte el activo: Robot	1	2

43	Posibilidad que la amenaza: Ataque informático de tipo: The man in the middle, afecte el activo: Electroencefalograma	2	4
44	Posibilidad que la amenaza: Ataque informático de tipo: The man in the middle, afecte el activo: Servidor Base de Datos	3	4
45	Posibilidad que la amenaza: Ataque informático de tipo: The man in the middle, afecte el activo: Emotiv G	3	4
46	Posibilidad que la amenaza: Ataque informático de tipo: The man in the middle, afecte el activo: EEG Neurosky Mindset	3	4
47	Posibilidad que la amenaza: Ataque informático de tipo: The man in the middle, afecte el activo: Tarjeta de red inalámbrica USB	3	4
48	Posibilidad que la amenaza: Ataque informático de tipo: The man in the middle, afecte el activo: Bluetooth	3	4
49	Posibilidad que la amenaza: Ataque informático de tipo: The man in the middle, afecte el activo: Computador	3	4
50	Posibilidad que la amenaza: Ataque informático de tipo: The man in the	3	4

Resultados

	middle, afecte el activo: Sistema en la Nube		
51	Posibilidad que la amenaza: Ataque informático de tipo: spam, afecte el activo: Electroencefalograma	1	4
52	Posibilidad que la amenaza: Ataque informático de tipo: spam, afecte el activo: Servidor Base de Datos	3	4
53	Posibilidad que la amenaza: Ataque informático de tipo: spam, afecte el activo: Servidor Ubuntu	3	4
54	Posibilidad que la amenaza: Ataque informático de tipo: spam, afecte el activo: Sistema en la Nube	3	4
55	Posibilidad que la amenaza: Ataque informático de tipo: scanning, afecte el activo: Servidor Base de Datos	3	3
56	Posibilidad que la amenaza: Ataque informático de tipo: scanning, afecte el activo: Servidor Ubuntu	4	3
57	Posibilidad que la amenaza: Ataque informático de tipo: scanning, afecte el activo: Celular	4	3
58	Posibilidad que la amenaza: Ataque informático de tipo: scanning, afecte el activo: Computador	4	3

Resultados

59	Posibilidad que la amenaza: Ataque informático de tipo: scanning, afecte el activo: Sistema en la Nube	4	3
60	Posibilidad que la amenaza: Ataque informático de tipo: PASSWORD CRAKING, afecte el activo: Electroencefalograma	2	4
61	Posibilidad que la amenaza: Ataque informático de tipo: PASSWORD CRAKING, afecte el activo: Servidor Ubuntu	3	4
62	Posibilidad que la amenaza: Ataque informático de tipo: PASSWORD CRAKING, afecte el activo: Celular	4	4
63	Posibilidad que la amenaza: Ataque informático de tipo: PASSWORD CRAKING, afecte el activo: Computador	4	4
64	Posibilidad que la amenaza: Ataque informático de tipo: PASSWORD CRAKING, afecte el activo: Sistema en la Nube	3	4
65	Posibilidad que la amenaza: Ataque informático de tipo: Exploit, afecte el activo: Electroencefalograma	1	4
66	Posibilidad que la amenaza: Ataque informático de tipo: Exploit, afecte el activo: Servidor Base de Datos	3	4

Resultados

67	Posibilidad que la amenaza: Ataque informático de tipo: Exploit, afecte el activo: Tarjeta de red inalámbrica USB	3	4
68	Posibilidad que la amenaza: Ataque informático de tipo: Exploit, afecte el activo: Servidor Ubuntu	4	4
69	Posibilidad que la amenaza: Ataque informático de tipo: Exploit, afecte el activo: Celular	4	4
70	Posibilidad que la amenaza: Ataque informático de tipo: Exploit, afecte el activo: Computador	4	4
71	Posibilidad que la amenaza: Ataque informático de tipo: Exploit, afecte el activo: Sistema en la Nube	4	4
72	Posibilidad que la amenaza: Ataque informático de tipo: Exploit, afecte el activo: prótesis Motora	2	4
73	Posibilidad que la amenaza: Ataque informático de tipo: Exploit, afecte el activo: Robot	3	4

Tabla 3 Calculo de los escenarios de riesgos y su respectiva calificación - Fuente propia

Luego de realizar la calificación en términos de probabilidad e impacto, se obtiene el respectivo mapa de riesgos y la respectiva distribución porcentual (tabla 4):

Resultados

Probabilidad		Consecuencia				
	valor	Insignificante	Menor	Intermedio	Mayor	Superior
		1	2	3	4	5
Casi seguro	5					
Probable	4		(37) - (39) -	(56) - (57) - (58) - (59) -	(4) - (5) - (7) - (25) - (62) - (63) - (68) - (69) - (70) - (71) -	
Posible	3		(11) - (12) - (16) - (29) - (30) - (38) - (40) -	(55) -	(1) - (2) - (3) - (6) - (13) - (15) - (18) - (19) - (20) - (22) - (27) - (33) - (34)	
Improbable	2		(10) - (28) - (41) -		(8) - (9) - (31) - (32) - (35) - (36) - (43) - (60) - (72) -	
Raro	1		(14) - (42) -		(17) - (21) - (23) - (24) - (26) - (51) - (65) -	

Tabla 4 Calificación Mapa de Riesgos – Fuente Propia

DISTRIBUCIÒN PORCENTUAL		
ZONA	%	Total riesgos
Aceptable	6,85	5
Tolerable	19,18	14
Inaceptable	60,27	44
Inadmisible	13,70	10

Tabla 5 Calificación en porcentaje Mapa de Riesgo - Fuente Propia

Como se puede observar, 5 de los riesgos quedaron en la zona de aceptable con un 6.85%, mientras que 14 riesgos se establecieron en la zona de tolerables con un 19.18%, por otro lado 44 riesgos con un 60.27% fueron detallados en la zona de inaceptables a estos se le debe iniciar un proceso de control, para finalizar 10 riesgos restantes quedaron en las zonas de inadmisibles con un 13.70%. En ese sentido, es necesario establecer un plan de tratamiento para los riesgos altos, que permita o posibilite la reducción de los niveles de impactos.

Se destaca en los riesgos altos, los ataque de “Hombre en el medio”, el “malware” y la negación de servicio, mientras que los que quedaron en la zona media se destaca el robo de información y la inyección de código.

3.2 Fase 2: Definición del Plan De Tratamiento de Acuerdo con los Riesgos Encontrados

La implementación de un plan de tratamiento de la información busca establecer un marco de confianza, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la organización.

Para la protección de la información se busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición reducido que permita responder por la integridad, confidencialidad y la disponibilidad, acorde con las necesidades de los diferentes grupos de interés identificados.

En consecuencia, estas acciones están orientadas a todos sus colaboradores en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las operaciones o toma de decisiones estarán determinadas por las siguientes premisas y basada basado en los lineamientos establecidos en la norma ISO 27001/2013 [24, 25, 26], estas acciones se pueden evidenciar en el anexo D:

- Minimizar el riesgo de la operación.
- Cumplir con los principios de la seguridad informática.
- Mantener la confianza en los usuarios.
- Apoyar la operación del negocio.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Proteger los activos tecnológicos.
- Proteger todos los datos de la organización.
- Fortalecer la cultura de seguridad.
- Ser garante de la continuidad del negocio.

Resultados

Alcance

Aplica a toda la organización, funcionarios, proveedores, terceros de la organización y usuarios.

Objetivo

El objetivo principal del plan de tratamiento es crear unas acciones que permita proteger los activos de información que componen la organización para asegurar credibilidad y confianza en sus clientes, proveedores, todos los que participan en la cadena de prestación de servicios.

Nivel de cumplimiento:

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento en los servicios de almacenamiento de información y bases de datos.

Responsables

- El equipo directivo es el responsable de asegurar que la seguridad de la información se gestiona adecuadamente en toda la organización.
- Cada gerente de cada área es responsable de garantizar que las personas que trabajan bajo su control protegen la información de acuerdo con las normas establecidas por la organización.
- El responsable de seguridad asesora al equipo directivo proporciona apoyo especializado al personal de la organización y garantiza que los informes sobre la situación de la seguridad de la información están disponibles.
- Cada miembro del personal tiene la responsabilidad de mantener la seguridad de información dentro de las actividades relacionadas con su trabajo.

Sanciones

Todo incumplimiento por parte de un funcionario o proveedor, así como de cualquier estándar o procedimiento es causa para iniciar acciones disciplinarias, las cuales de acuerdo con su gravedad pueden suponer la terminación de la vinculación laboral del empleado o proveedor, estos lineamientos se pueden observar en el anexo D.

3.3 Fase 3: Validación del Modelo

En el desarrollo de las actividades propuestas en el proyecto, la validación de la metodología contempla varias etapas, donde se evidenció los resultados de la implementación, donde se pudo verificar el desarrollo del modelo de seguridad y la eficacia de los controles.

3.3.1 Modelo de seguridad

El modelo de seguridad se construyó basado en un marco legal ligado a una estructura normativa donde se ve las leyes, decretos, CONPES y normas técnicas que ayudan a la gestión de la seguridad. Junto con los parámetros entregado por el Mintic [44] para el desarrollo para los modelos de seguridad con el que se contempló el uso del ciclo de operación PHVA, seguido se determinó los niveles de madurez del modelo de seguridad [44] que están determinados por la normativa de la ISO/IEC 27001:2013 y debió ser calificado y evaluado para valorar la eficacia del modelo de seguridad desarrollado para los sistemas BCI.

A continuación, se describen los diferentes componentes del modelo de seguridad:

I. Estructura Normativa
II. Normas Técnicas
III. Modelo De Seguridad De La Información (Anexo 1) De febrero 2021 Ministerio De Tecnologías De La Información Y Las Comunicaciones
    - Ciclo De Operación
    - Fase De Planificación
    - Fase De Implementación
    - Fase De Evaluación De Desempeño
    - Fase De Mejora Continua
IV. Madurez Del Modelo De Seguridad
V. Mecanismos De Seguridad

3.3.1.1 ESTRUCTURA NORMATIVA

Los modelos de seguridad de la información están ligados a un grupo de leyes que ayudan en la implantación, gestión y control de este, es importante tener referencia de ellas ya que son éstas las que darán las herramientas necesarias para hacer un buen desarrollo de en la implementación del modelo de seguridad, a continuación, se nombran las leyes revisadas.

3.3.1.1.1 LEY ESTATUTARIA 1266 DE 2008

"ARTÍCULO 1o. OBJETO. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países" [16].

3.3.1.1.2 LEY 1273 DE 2009

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.[14].

3.3.1.1.3 LEY ESTATUTARIA 1581 DE 2012

"*ARTÍCULO 1o. OBJETO. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma "*[61]

3.3.1.1.4 DECRETO 1377 DE 2013

"Artículo 1°. Objeto. El presente Decreto tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales." [57]

3.3.1.1.5 CONPES 3854 POLÍTICA NACIONAL DE SEGURIDAD DIGITAL

Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno

digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país. [54]

3.3.1.1.6 CONPES 3701 Lineamientos de política para ciberseguridad y ciberdefensa

Esta política concentró los esfuerzos del país en contrarrestar el incremento de las amenazas informáticas que lo afectaban significativamente, y en desarrollar un marco normativo e institucional para afrontar retos en aspectos de seguridad cibernética. A continuación, se presentan de manera general los avances en la implementación de dichos lineamientos de política, y las actividades de revisión de estos durante los años 2014 y 2015.[56].

3.3.1.2 NORMAS TÉCNICAS

A continuación, se tienen algunas normas, leyes, decretos, sentencias y estatutos como base jurídica y de investigación, con la intención de crear un marco jurídico que delimitara la aplicación y correcto desarrollo que se utilizaron para la redacción del modelo de seguridad.

3.3.1.2.1 NORMA TÉCNICA NTC-ISO-IEC COLOMBIANA 27001- Tecnología de la información Técnicas de seguridad. sistemas de gestión de la seguridad de la información.

Esta Norma especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. La presente Norma incluye también los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adaptados a las necesidades de la organización. [25].

3.3.1.2.2 NTC-ISO-IEC 27002 - Tecnología de la información Técnicas de seguridad. sistemas de gestión de la seguridad de la información

La presente Norma Internacional presenta directrices para las normas de seguridad de la información organizacional y las prácticas de gestión de la seguridad de la información, incluida la selección, la implementación y la gestión de controles, teniendo en cuenta el(los) entorno(s) del riesgo de seguridad de la información de la organización. [24].

3.3.1.2.3 NORMA TÉCNICA NTC-ISO-IEC COLOMBIANA 27005- Tecnología de la información Técnicas de seguridad. Gestión del riesgo en la seguridad de la información.

La norma ISO 27005 contiene diferentes recomendaciones y directrices generales para la gestión de riesgo en Sistemas de Gestión de Seguridad de la Información. [26].

3.3.1.3 MODELO DE SEGURIDAD DE LA INFORMACIÓN (ANEXO 1) DE FEBRERO 2021 MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Las nuevas tecnologías emergentes como son las interfaces cerebro computador tienen un valor agregado, que cada vez se hacen más importantes en la interacción máquina-hombre, este incremento genera nuevos paradigmas en la protección de la información, llevando a que estos sistemas deban generar procesos y políticas para la protección de los datos, pero como se encuentra en una edad temprana, el hacer la caracterización de los posibles ataques que pueden tener éxito en este tipo de sistemas es de suma importancia, ya que con ellos se puede evaluar las posibles fuentes de salidas y perdida de datos, ya que la información generada en los BCI puede ser susceptibles a riesgos ligados a la alteración y robo de información, y para ello se recurren a diferentes procesos en los que los métodos empíricos de verificar la disponibilidad de la información, la confiabilidad y la integridad de las bases de datos generadas, en las diferentes etapas que tiene los BCI, sean lo más seguras posibles, bajando la posibilidad de su corrupción, donde las amenazas cibernéticas son un riesgo imperativo dentro del uso de dispositivos tecnológicos, pero la responsabilidad de los recursos es parte de las tareas que debe cumplir tanto los fabricantes de los sistemas como los usuarios finales; una de los mecanismos es utilizar modelos de seguridad, con el cual se podrán gestionar las diferentes etapas que cumplen el sistemas BCI desde el punto de vista de control y con ello el minimizar las posibles filtraciones de información buscando mitigar las principales amenazas basado en la gestión del riesgo, donde se define los lineamientos para la implementación de la estrategia de seguridad digital.

Resultados

Objetivo del Modelo del Modelo de Seguridad

Diseñar un Modelo de seguridad basado en políticas de protección de la información, enfocado en el cuidado de los activos tecnológicos y de información asociados a los sistemas BCI, mediante una gestión del riesgo con base a las leyes reglamentadas para el cuidado de la información, a partir de los resultados del desarrollo del plan de tratamiento con el fin de reducir los niveles de exposición a los riegos asociados.

Alcance

El modelo de seguridad está enfocado en medir el nivel de madurez en la seguridad de los activos basado en actividades de valoración de los controles implementados, para una adecuada gestión de los riesgos asociados donde se cumpla los requisitos de la seguridad en la información: integridad, disponibilidad y privacidad.

CICLO DE OPERACIÓN

La figura 13 muestra el ciclo de operación del modelo de seguridad, donde se estiman las operaciones a realizar para la mitigación y control de los riesgos, ligados al sistema BCI

Figura 12 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información, tomado de https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

3.3.1.3.1 FASE DE PLANIFICACIÓN

Para el desarrollo de esta actividad se deberá contar con análisis previo de diagnóstico del sistema BCI donde se determinarán las características y su nivel de seguridad, esto dará pie para la implementación de la etapa del ciclo de planificación, donde se plantearán diferentes resultados con el objetivo analizar, determinar e implementar actividades que estén enfocados hacia tareas administrativas y documentales [44].

En la siguiente tabla 6 se establecen los parámetros que se esperan lograr en la fase de planificación, donde se tiene los controles propuestos y sus entregables que estarán determinados por resultados que se pueden evaluar y medir en el tiempo.

ID	METAS	RESULTADOS
1	Determinar las amenazas asociadas a los sistemas BCI tomados de un mapa de riegos	Documento mapa de gestión de riesgos
2	Planificar la gestión de los riesgos asociados a los sistemas BCI	Documento de plan de tratamiento con la selección de los dominios de la ISO 27001/2013
3	Detallar como va a ser el actuar ante los controles diseñados para la protección de los activos	Documento de la política y las políticas a implementar gestionado por la alta dirección Documento con inventario de documentación de los dominios para la seguridad de la información
4	Implementar directrices de acción para los roles y responsabilidades de la seguridad en la información	Documento con las tareas por roles y responsabilidades de la seguridad de información
5	Desarrollar actividades de capacitación y comunicación al personal que realizan tareas asociadas a los sistemas BCI	Documento con plan de capacitación y comunicación a implementar

Tabla 6 Parámetros FASE DE PLANIFICACIÓN - Fuente Propia

3.3.1.3.1.1 Determinar las vulnerabilidades asociadas a los sistemas BCI tomados de un mapa de riegos:

Se debe determinar las amenazas asociadas a los sistemas BCI se debe implementar un análisis de un mapa de riesgos donde se evidencien las diferentes amenazas, vulnerabilidad, activos y probabilidades de eventos de seguridad, esto tomado como referencia la norma ISO 27001/2013. Donde al final se evaluará de manera objetiva los niveles de seguridad y con los resultados se tomarán las medidas correctivas para mitigar los diferentes niveles de riegos.

3.3.1.3.1.2 Planificar la gestión de los riesgos asociados a los sistemas BCI:

Se debe realizar un proceso de plan de tratamiento donde se seleccionará actividades para una adecuada gestión de los riesgos, utilizando los dominios, objetivos de control y controles del anexo A de la norma ISO 27001/2013

3.3.1.3.1.3 Detallar como va a ser el actuar ante los controles diseñados para la protección de los activos:

Se debe implementar un documento con las políticas de seguridad donde se deberá detallar como será el actuar ante los controles de manera técnica para donde se espera que su alcance sea un nivel alto de eficacia de los controles, junto a esta tarea se espera que se realice una anexo a la política donde se comprometa a conservar altos niveles de seguridad asociados a los sistemas BCI, este objetivo deberá ser medible en el tiempo y auditado para tener altos estándares de calidad en el modelo de seguridad.

3.3.1.3.1.4 Implementar directrices de acción para los roles y responsabilidades de la seguridad en la información:

Se debe crear un documento donde se den diferentes directrices, acciones, tareas y responsabilidades a los roles que permita llevar una trazabilidad completa del tratamiento de los controles, tareas, activos, vulnerabilidad e indicadores de tiempos de respuesta, junto con el seguimiento de las acciones derivadas para el tratamiento de las correcciones, las acciones correctivas y las acciones preventivas, así como de la eficacia de las soluciones y respuestas

3.3.1.3.1.5 Desarrollar actividades de capacitación y comunicación al personal que realizan tareas asociadas a los sistemas BCI:

Se debe diseñar de cursos y talleres como un espacio exclusivo para la generación de conocimientos, donde pueden interactuar y realizar buenas prácticas asociadas a la seguridad de los activos y los controles de la gestión del riesgo, minimizando de manera sustancial las diferentes amenazas asociadas a la falta de aprendizajes y conocimientos.

3.3.1.3.2 FASE DE IMPLEMENTACIÓN

En esta fase se dará cumplimiento a las metas trazadas en la fase de planificación seguido de los controles propuestos y plan de tratamiento. En la siguiente tabla se establece los parámetros que se esperan lograr en las fases del modelo de seguridad, donde se tiene los controles que implementarán y sus entregables que estarán determinados por resultados que se pueden evaluar y medir en el tiempo

ID	METAS	RESULTADOS
1	Definir las acciones en el mapa de riesgo ligado a las amenazas asociados a los sistemas BCI	Documento de mapa de riesgo con la calificación de las amenazas
2	Implementar los controles definidos del plan de tratamiento para cada uno de los objetivos de control de la norma ISO 27001/2013 que tienen cabida en el modelo	Documento del plan de tratamiento con las actividades de cada uno de los controles a realizar anexo D
3	Ejecutar las políticas de seguridad en el entorno organizacional	Exponer las políticas de seguridad de seguridad en el entorno organizacional, junto a los roles y responsabilidades
4	Realizar las actividades de capacitación y comunicación al personal organizacional	Establecer espacios donde se ofrezcan capacitaciones al personal de la organización. Implementar espacios de comunicación.

Tabla 7 Parámetros FASE DE IMPLEMENTACIÓN - Fuente Propia

3.3.1.3.2.1 Definir las acciones en el mapa de riesgo ligado a las amenazas asociados a los sistemas BCI:

Se debe definir las amenazas asociadas a los sistemas BCI se debe calificar el mapa de riesgos donde se evidencien las diferentes amenazas, vulnerabilidad, activos y probabilidades de eventos de seguridad, esto tomado como referencia la norma ISO 27001/2013. Donde al final se definirá las tareas que se deberán realizar por cada una de las amenazas de manera objetiva, las cuales determinaran si se controlan, se transmite o se aceptan y deberán tener un responsable del control.

3.3.1.3.2.2 Implementar los controles definidos del plan de tratamiento para cada uno de los objetivos de control de la norma ISO 27001/2013 que tienen cabida en el modelo:

Se debe realizar un proceso de plan de tratamiento donde se seleccionarán las actividades para una adecuada gestión de los riesgos, utilizando los dominios, objetivos de control y controles del anexo A de la norma ISO 27001/2013

3.3.1.3.2.3 Ejecutar las políticas de seguridad en el entorno organizacional en el entorno organizacional:

Se debe implementar las políticas de seguridad donde se deberá detallar diferentes directrices, acciones, tareas y responsabilidades a las tareas y roles que permitan llevar una trazabilidad completa del tratamiento de los controles, tareas, activos, vulnerabilidad e indicadores de tiempos de respuesta, donde se espera que su alcance sea un nivel alto de eficacia de los controles, medible en el tiempo y auditado para tener altos estándares de calidad en las políticas implementadas.

3.3.1.3.2.4 Realizar las actividades de capacitación y comunicación al personal organizacional:

Se debe implementar de cursos y talleres como un espacio exclusivo para la generación de conocimientos, donde pueden interactuar y realizar buenas prácticas asociadas a la seguridad de los activos y los controles de la gestión del riesgo, minimizando de manera sustancial las diferentes amenazas asociadas a la falta de aprendizajes y conocimientos.

3.3.1.3.3 FASE DE EVALUACIÓN DE DESEMPEÑO

En el desarrollo de las actividades propuestas en la fase de implementación el paso a seguir es la evaluación de éstas, donde se evidenciará la eficacia de los controles, políticas y plan de tratamiento propuesto. Dando los responsables de cada uno de los procesos una verificación de los cumplimientos [44].

En la siguiente tabla se establece los parámetros que se esperan lograr en la fase del modelo de seguridad, donde se tiene los controles que implementarán y sus entregables que estarán determinados por resultados que se pueden evaluar y medir en el tiempo

ID	METAS	RESULTADOS
1	Verificar la eficacia de los controles definidos de plan de tratamiento para cada uno de los objetivos de control de la norma ISO 27001/2013 que tienen cabida en el modelo	Documento con la evaluación del plan de tratamiento (GAP)
2	Evaluar la eficacia de las políticas de seguridad en el entorno organizacional	Documento de estado de implementación de las políticas (valoración de los controles medibles en el tiempo)
3	Realizar las actividades de evaluación de las capacitaciones y el plan de comunicación al personal organizacional	Establecer planes de certificaciones, evaluaciones y encuestas de conocimiento
4	Realizar auditoría interna	Documento con las revisiones de la auditoria.

Tabla 8 Parámetros EVALUACIÓN DE DESEMPEÑO - Fuente Propia

3.3.1.3.3.1 Verificar la eficacia de los controles definidos del plan de tratamiento para cada uno de los objetivos de control de la norma ISO 27001/2013 que tienen cabida en el modelo:

Se debe implementar basado en el plan de tratamiento y los controles establecidos, los diferentes actores de en los procesos, deberán generar documentación que validen los controles, donde se informe actividades anómalas en los sistemas, valoración de la seguridad y responsables, esta tarea deberá contar con un proceso de pruebas y de estrés de los sistemas donde se determinara sus niveles de seguridad y efectividad propuesto.

3.3.1.3.3.2 Evaluar la eficacia de las políticas de seguridad en el entorno organizacional:

Se debe crear informes de los hallazgos en las actividades relacionadas con los controles, ya que estos darán información relevante para documentar la validez de las políticas establecidas en la organización, estos informes deben ser periódicos y realizados por sus responsables por área operacional y entregados para auditorías internas.

3.3.1.3.3.3 Realizar las actividades de evaluación de las capacitaciones y el plan de comunicación al personal organizacional:

Se debe verificar en los procesos de educación, la efectividad de los procesos formativos es dando a los asistentes certificaciones donde fomente en los entornos organizacionales un alto nivel de aprendizaje, de igual manera la retro alimentación de los procesos comunicativos por medio de encuestas y foros da mayor visibilidad a los asistentes donde sienten que sus opiniones cuentan y dan pie a los procesos de aprendizaje continuo.

3.3.1.3.3.4 Realizar auditoría interna:

Se debe evaluar procesos internos, ya que ésta brinda los conocimientos de cómo van evolucionando las políticas y controles para la gestión de la seguridad de la información, al tener este tipo de actividades es más favorable que se encuentren tareas diferenciadoras que motiven el crecimiento organizacional, dando cabida a la mejora continua y altos estándares de calidad.

3.3.1.3.4 FASE DE MEJORA CONTINUA

Valorando las fases anteriores, se cuenta con controles implementados y auditados por sus responsables y gerencia organizacional, validando su niveles de eficacia. Basado en esa información se puede determinar un plan de mejoramiento continuo, lo cual va a hacer que los procesos sigan su ciclo de crecimiento y madurez, determinando medidas y decisiones acordes a las necesidades con las que se cuenta [44].

En la siguiente tabla se establece los parámetros que se esperan lograr en la fases del modelo de seguridad, donde se tiene los controles que implementarán y sus entregables que estarán determinados por resultados que se pueden evaluar y medir en el tiempo

ID	METAS	RESULTADOS
1	Determinar el plan de mejoramiento de las políticas de seguridad en el entorno organizacional	Documento con el plan de mejoramiento de las políticas (valoración de los controles medibles en el tiempo)
2	Definir las actividades de cultura de aprendizaje continuo que implementen estrategias para la seguridad de la información organizacional	Establecer cronogramas de capacitaciones y actividades de aprendizaje continuo
3	Implementar acciones de mejora basados en la auditoría interna	Informes de compromisos de mejoras, medibles en el tiempo y avalado.

Tabla 9 Parámetros FASE DE MEJORA CONTINUA - Fuente Propia

3.3.1.3.4.1 Determinar plan de mejoramiento de Seguridad en el entorno Organizacional:

En los procesos de mejoramiento continuo se debe referenciar esta etapa como una de las más importantes ya que es esta, la que dará las tareas a implementar en el futuro basado en los controles, calificaciones y seguimiento del plan de tratamiento propuesto. Es aquí donde los

diferentes agentes que hacen parte de la organización deberán hacer retroalimentación de los objetivos que se plantearon y entregaran informes para determinar las acciones a seguir.

Definir las actividades de cultura de aprendizaje continuo que implementen estrategias para la seguridad de la información organizacional**:**

La actividades de aprendizaje continuo determinarán los niveles de conocimiento y actualización de conceptos ligados a la seguridad y protección de los activos organizacionales, este es un punto de referencia importante ya que son los usuarios, empleados y comunidad organizacional los que hacen uso de los servicios tecnológicos, y las amenazas cibernéticas tiene ciclos de evolución, basado en dicha premisa, se debe implementar y modernizar los procesos formativos con lineamientos actuales y progresistas a la seguridad de la información.

3.3.1.3.4.2 Implementar acciones de mejora basados en la auditoría interna:

La auditoría interna es una herramienta que da los mejores resultados para lograr los objetivos propuestos, determina un plan a seguir y donde se debe mejorar, todo esto deberá trabajar a un plan de mejoramiento continuo, donde la comunidad organizacional juega un rol significativo de obtener resultados hacia la seguridad de la información, donde llegar a tener los niveles de riesgos a valores aceptables e implementación de controles a niveles de madurez optimizados, se debe ser la premisa a la cual se debe apuntar.

3.3.1.4 MADUREZ DEL MODELO DE SEGURIDAD

El modelo de madurez ayudará a determinar los niveles en los que se encuentran las políticas que se han implementado para los 14 dominios, los 37 objetivos de control y sus 114 controles de la norma ISO 27001/2013, donde la valoración del control determina como será el actuar de la política y dando un informe de alto nivel con la evolución de los procesos instaurados [44].

Resultados

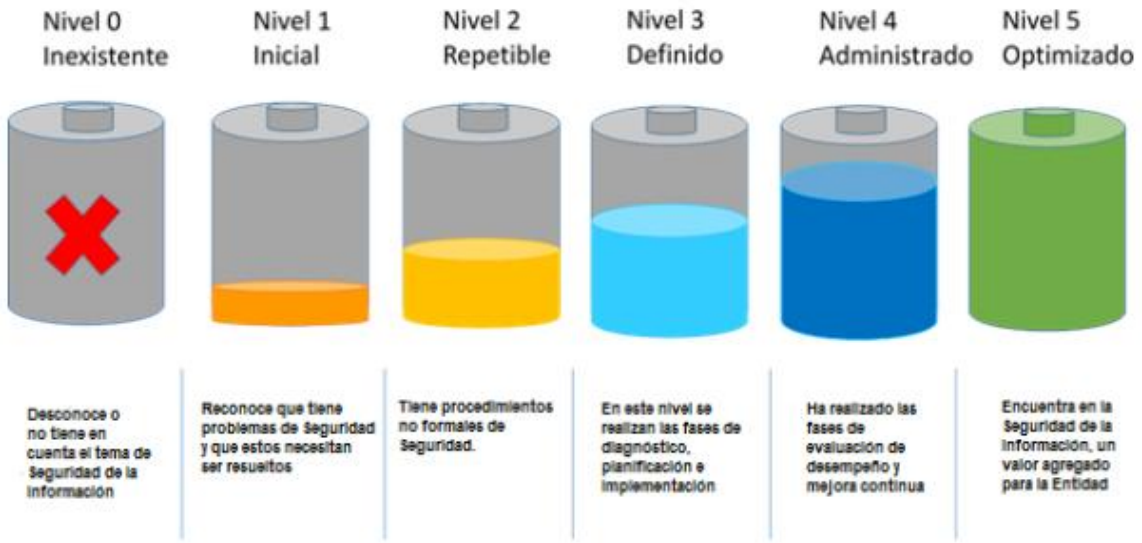


Figura 13 – Ciclo de Madurez-Modelo de Seguridad y Privacidad de la Información, tomado de https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Estas valoraciones determinadas en diferentes porcentajes y definiciones, ofrece criterios de evolución de los controles implementados en el modelo de seguridad y privacidad.

% de Cumplimiento	Nivel #	Definición	Descripción
0 %	0	Inexistente	Carencia completa de cualquier procedimiento reconocible para el control, no se ha reconocido siquiera como un problema a resolver.
10 %	1	Inicial	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen formatos o plantillas definidas por la entidad

50 %	2	Reproducible/ intuitivo	Los procesos similares se llevan a cabo en forma similar por diferentes personas con la misma tarea. Se normalizarán las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90 %	3	Procedimiento definido	La entidad entera participa en el proceso. Los procesos implantados, documentados y comunicados mediante entrenamiento.
95 %	4	Gestionado y Medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100 %	5	Optimizado	Los procesos están bajo constante mejora. Con base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Tabla 10 Valoración de Controles icm3 https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

3.3.1.5 MECANISMOS DE SEGURIDAD

Los mecanismos de seguridad están enfocados en las tareas que se deben cumplir en el desarrollo del modelo de seguridad y hacen parte de los objetivos y resultados propuestos para el desarrollo de éste [24, 25, 26].

3.3.1.5.1 Roles y responsabilidades:

En el diseño del modelo de seguridad es indispensable tener implementado la documentación de los roles y responsabilidades esto como mecanismo para auditar las tareas de las áreas de la

organización esto basado en los controles de la ISO 27001/2013, esta información se verá en el Anexo B [24, 25, 26].

3.3.1.5.2 Controles de seguridad de la información asociados a las amenazas:

Como una de las tarea en los procesos del modelo de seguridad se debe contar con un análisis de los riesgos que puede contener cada uno de los dominios del marco de referencia utilizado para dicha tarea se tomó la ISO 27001/2013, esto nos ayudará a determinar el valor cuantitativo y cualitativo del riesgo relacionado con una amenaza reconocida o situación específica en cada área de la organización, estas documentación está diseñada e integrada por el equipo de gestión en cada una de las áreas con el objetivo detener procesos comunes. Se dará detalle de los riesgos en el Anexo D [24, 25, 26].

3.3.1.5.3 Inventario de documentación de los dominios para la seguridad de la información:

El establecimiento de la documentación relacionada a cada uno de los 14 dominios de la ISO 27001/2013 dará mayores niveles de control de las políticas implementadas, donde se valorará su nivel de inserción en los procesos administrativos y técnicos, esta intervención documental deberá estará a cargo de los responsables por área y auditada por quien verificará su nivel de madurez en el modelo de seguridad, este inventario se encuentra detallado en el ANEXO C [24, 25, 26].

3.3.2 Validación de la Estrategia de Implementación

Introducción

Se ha entrado en un proceso donde se quiere realizar el análisis de vulnerabilidades del servidor Ubuntu donde se aloja el servicio de la interfaz cerebro computador (BCI), para mejorar sus capacidades tecnológicas, administrativas y de seguridad, con ello poder brindar servicios mucho más robustos, en este proceso se ha logrado identificar varios problemas con su montaje, configuración, seguridad y monitoreo. Es por ello, que es importante detectar y realizar la documentación apropiada para tener un registro y evaluación de los servicios que se

ofrecen. Se han realizado varias tareas con el objetivo de minimizar percances a futuro, también se ha evaluado las diferentes vulnerabilidades encontradas.

Objetivo

Ejecutar una revisión técnica de seguridad en el servidor Ubuntu BCI donde se aloja el servicio de la interfaz cerebro computador (BCI), utilizando el proceso de hacking ético como metodología para la gestión de riesgos, validando los niveles de exposición de los servicios en entornos productivos, para mejorar sus características de gestión de seguridad de la información con el cual se pueda garantizar un nivel de protección lo más apto posible.

3.2.1 Gestión de Riesgos

En consideración del mapa de riesgos ya obtenido, se ejecutó una prueba técnica (como se indicó en la metodología) en simulación de algunos de los ataques informáticos hacia un sistema BCI, con ello, poder validar e implementar diferentes controles técnicos asociados al modelo de seguridad ya definido.

3.2.1.1 Contexto / alcance

Servidor Ubuntu donde se aloja el servicio de la interfaz cerebro computador (BCI).

3.2.1.2 Identificación de Riesgos

Los siguientes riesgos son los ya identificados en los objetivos específicos anteriores.

Resultados

AMENAZAS \ ACTIVOS	Electroencefalograma	Servidor Base de Datos	Emotiv G	EEG Neurosky Mindset	Tarjeta de red Inalambrica USB	Bluetooth	Servidor Ubuntu	Celular	Computador	Sistema en la Nube	Protesis Motora	Robot
Acceso físico no autorizado/indebido		x	x	x	x	x	x		x	x	x	x
Ataque informático de tipo: SQL injection					x	x	x					x
Ataque informático de tipo: DNS Reflexion/Amplification.		x							x			
Ataque informático de tipo: DoS/DDoS	x	x						x	x			
Ataque informático de tipo: buffer overflow	x	x			x	x	x	x	x			x
Ataque informático de tipo: Ransomware												
Ataque de tipo: Ingeniería social			x	x	x	x	x			x	x	x
Ataque informático de tipo: Rompimiento de cifrado o llaves criptográficas.												
Ataque informático de tipo: tcp syn attack							x	x	x	x	x	x
Ataque informático de tipo: The man in the middle	x	x	x	x	x	x			x	x		
Ataque informático de tipo: spam	x	x					x			x		
Ataque informático de tipo: Spoofing: de MAC, IP, ARP o cualquier servicio												
Ataque informático de tipo: scanning		x					x	x	x	x		
Ataque informático de tipo: PASSWORD CRAKING	x						x	x	x	x		
Ataque informático de tipo: Exploit o Modificación no autorizada de datos e información	x	x			x		x	x	x	x	x	x

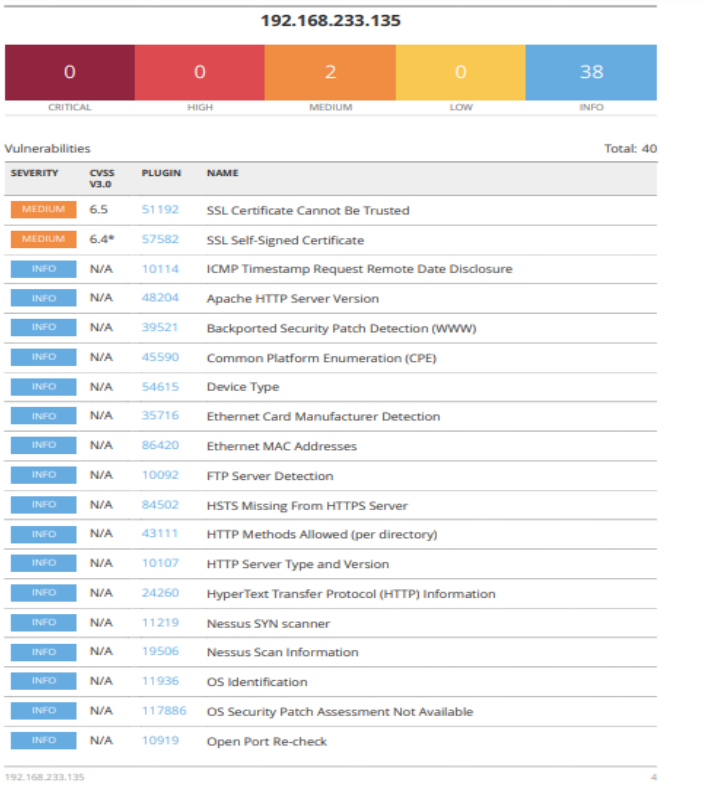
Figura 14 Listado de las vulnerabilidades analizadas y los activos afectados, Fuente Propia

3.2.2 Análisis de vulnerabilidades

El objetivo principal de este proceso de análisis de vulnerabilidades es el de evaluar la seguridad a la infraestructura y servicios con la finalidad de mitigar las vulnerabilidades y amenazas identificando riesgos e impactos que podría ocasionar, para dicha tarea el escáner utilizado es la plataforma NESSUS que tiene como características:

- Identificar vulnerabilidades en la infraestructura.
- Identificar vulnerabilidades en la página web, motores de bases de datos y servidores de correo
- Identificar fortalezas y deficiencias de la infraestructura implementada
- Entrega de informa de vulnerabilidades y formas de reparación
- Documentación de las vulnerabilidades ligadas a CVE
- Se realiza un escaneo de vulnerabilidad con la herramienta Nessus Essential y estos fueron sus resultados sobre el servidor Ubuntu BCI:
- Se puede evidenciar un total de 40 vulnerabilidades (imagen 2) en el servidor Ubuntu BCI, donde se muestran diferentes vulnerabilidades en rangos y características, de ellas, 38 son informativas y solo 2 de categoría media.

Resultados



192.168.233.135

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	2	0	38

Vulnerabilities — Total: 40

SEVERITY	CVSS V3.0	PLUGIN	NAME
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4*	57582	SSL Self-Signed Certificate
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	39521	Backported Security Patch Detection (WWW)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10092	FTP Server Detection
INFO	N/A	84502	HSTS Missing From HTTPS Server
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	117886	OS Security Patch Assessment Not Available
INFO	N/A	10919	Open Port Re-check

192.168.233.135 4

INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	149334	SSH Password Authentication Accepted
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	10287	Traceroute Information
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	10386	Web Server No 404 Error Code Check
INFO	N/A	10302	Web Server robots.txt Information Disclosure
INFO	N/A	66717	mDNS Detection (Local Network)
INFO	N/A	52703	vsftpd Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

Figura 15 Análisis de vulnerabilidades Nessus - Fuente Propia

3.2.3 Descripción de Vulnerabilidades de Medio Nivel e Informativas

3.2.3.1 The SSL certificate for this service cannot be trusted (No se puede confiar en el certificado SSL para este servicio)

Descripción

No se puede confiar en el certificado X.509 del servidor, esta situación puede ocurrir de tres maneras diferentes, en las que la cadena de confianza puede romperse, como se indica a continuación:

- Primero, la parte superior de la cadena de certificados enviada por el servidor puede no descender de una autoridad de certificación pública conocida.
- En segundo lugar, la cadena de certificados puede contener un certificado que no sea válido en el momento de la exploración.
- En tercer lugar, la cadena de certificados puede contener una firma que no coincide con la información del certificado o que no se pudo verificar.
- Si el host remoto es un host público en producción, cualquier interrupción en la cadena dificulta que los usuarios verifiquen la autenticidad y la identidad del servidor web.

Ataque

Esto podría facilitar la realización de ataques man-in-the-middle contra el host remoto.

Solución

Comprar o generar un certificado SSL adecuado para este servicio.

3.2.3.2 The SSL certificate chain for this service ends in an unrecognized self-signed certificate. (La cadena de certificados SSL para este servicio termina en un certificado auto firmado no reconocido)

Descripción

- La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida.
- Si el host remoto es un host público en producción, esto anula el uso de SSL, ya que cualquiera podría establecer un ataque de intermediario contra el host remoto.

Solución

Comprar o generar un certificado SSL adecuado para este servicio.

3.2.3.3 Apache HTTP Server Version

Se pudo identificar el servicio remoto

Descripción

El servicio remoto por su banner o mirando el mensaje de error que envía cuando recibe una solicitud HTTP.

3.2.3.4 HTTP Server Type and Version

Un servidor web se está ejecutando en el host remoto.

Descripción

Este complemento intenta determinar el tipo y la versión del servidor web remoto.

3.2.3.4 FTP Server Detection.

Un servidor FTP está escuchando en un puerto remoto

Descripción

Es posible obtener el banner del servidor FTP remoto conectándose a un puerto remoto.

3.2.3.5 Apache HTTP server.

Es posible obtener el número de versión del servidor Apache HTTP remoto

Descripción

El host remoto ejecuta Apache HTTP Server, un servidor web de código abierto. Era posible leer el número de versión del banner.

3.2.4 Ethical Hacking

Identificar necesidades

El proceso de Ethical Hacking brinda las capacidades para determinar y evaluar la seguridad de un servicio informático donde se realizan pruebas técnicas de intrusión controladas, en este caso la infraestructura implementada es el servidor Ubuntu BCI, donde se aloja el servicio de la interfaz cerebro computador (BCI) con sus librerías, con la finalidad de encontrar y auditar las vulnerabilidades y amenazas de las aplicaciones web y los motores de bases de datos, los cuales puedan poner en riesgo la operabilidad de los servicios tecnológicos.

3.2.4.1 Identificación de riesgos e impactos que podría ocasionar las pruebas

- Identificar vulnerabilidades en la infraestructura, basados en el escaneo producido por la herramienta Nessus Essential.
- Identificar vulnerabilidades en el aplicativo, sistema operativo, motores de bases de datos y servicios expuestos basados en el escaneo producido por la herramienta Nessus Essential.
- Identificar fortalezas y deficiencias de la infraestructura implementada que se evidencien en el pentesting.

3.2.4.2 Validación sobre qué plataformas internas o externas se harán las pruebas

- Sistema Operativo: Linux
- Versión: Ubuntu 20.04.2.0
- Arquitectura: Amd 64

3.2.4.3 Preparar y programar pruebas

Este informe se enfoca a realizar una evaluación por medio de un pentesting de Ethical Hacking de forma escalonada de tipo caja blanca, dado que se tiene acceso a los servicios.

Las características principales de los tipos de ataques que pueden ser ejecutados son:

Acceso físico no autorizado/indebido
Ataque informático de tipo: SQL injection
Ataque informático de tipo: DNS Reflexion/Amplification.
Ataque informático de tipo: DoS/DDoS
Ataque informático de tipo: buffer overflow
Ataque informático de tipo: Ransomware
Ataque de tipo: Ingeniería social
Ataque informático de tipo: Rompimiento de cifrado o llaves criptográficas.
Ataque informático de tipo: tcp syn attack
Ataque informático de tipo: The man in the middle
Ataque informático de tipo: spam
Ataque informático de tipo: Spoofing: de MAC, IP, ARP o cualquier servicio
Ataque informático de tipo: scanning
Ataque informático de tipo: PASSWORD CRAKING
Ataque informático de tipo: Exploit o Modificación no autorizada de datos e información

Tabla Tipos de ataques seleccionado proceso Ethical Hacking - Fuente Propia

Del anterior listado se seleccionaron un grupo de ataques los cuales serán probados y se demostrará la solución ligada a éstos. Ya que varios ataques para poder ser realizados se necesitaría una implementación empresarial tanto de la parte de hardware y software, como instalaciones físicas y grupo de empleados, para este paso se seleccionan ataques que de manera lógica tienen una afectación y pueden evidenciar los niveles de exposición con los que se cuenta, y poder mitigar las amenazas posibles en un escenario con una cantidad de vulnerabilidades identificadas, también se determinan que los ataques que se van a implementar son de los ataques más comunes en ámbitos empresariales y servicios web [8]

3.2.4.4 Las aplicaciones para utilizar en el pentesting son:

- Búsqueda de información: Nmap, OWASP ZAP
- Escaneo de Vulnerabilidad: Nessus Essentials
- Exploits: Metasploit.

Resultados

- Distribución de Linux: Kali 2020.4

3.2.5 Pruebas Realizadas

3.2.5.1 Ataque informático de tipo DoS/DDoS:

el ataque de denegación de servicios se trata de llenar de solicitudes el servidor hasta que no tenga la capacidad de respuesta, dando como resultado la ciada del servicio prestado.

Se evidencia que los procesos de la CPU se encuentran en valores menores del 10% previo a que se realice el ataque DDoS.

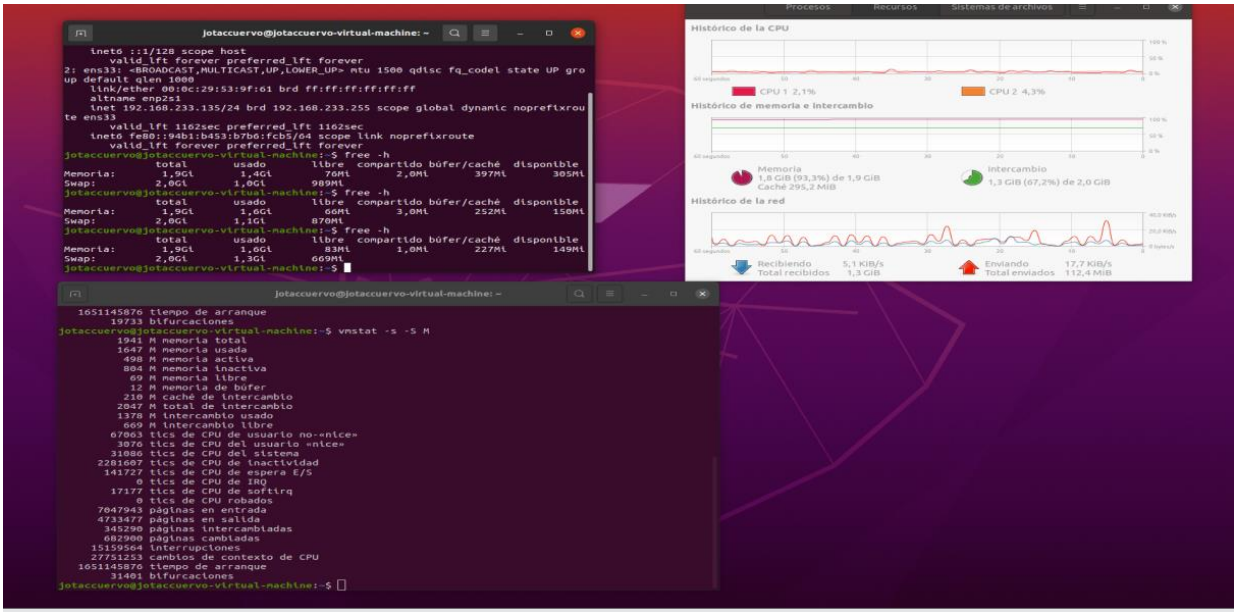


Figura 16 Ataque informático de tipo DoS/DDoS - Fuente Propia

Se muestra como los servicios web se encuentran en funcionamiento normal, donde se puede tener ingreso a la plataforma OPENBCI_WEB.

Resultados

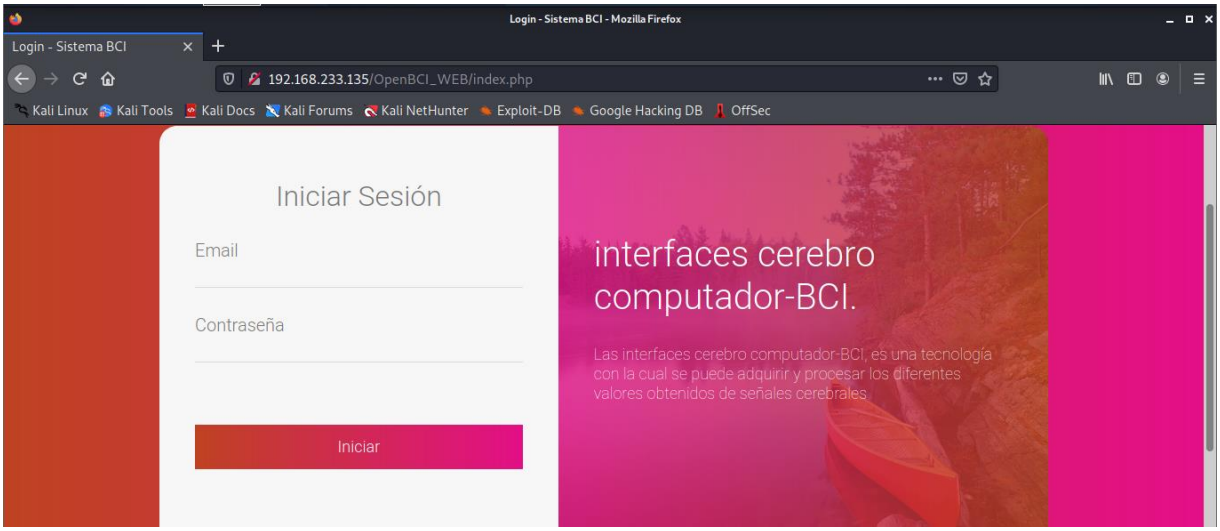


Figura 17 Plataforma OPENBCI_WEB - Fuente Propia

Se utiliza la herramienta wireshark con la que se verifica el tránsito de desde la maquina Kali Linux hacia el servidor OPENBCI_WEB. Allí podemos observar que se utiliza la aplicación Hping3 que crea paquetes que son utilizados en el protocolo TCP/IP, este tipo de aplicativos tiene la capacidad de crear un desborde de paquetes creados y diseñados por el atacante.

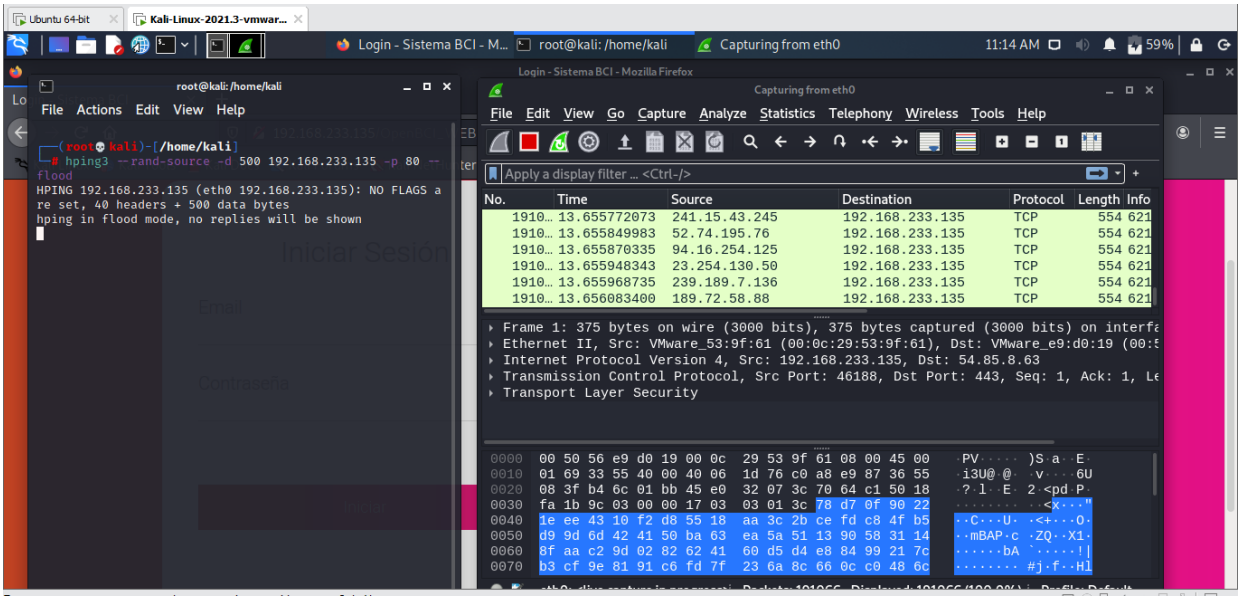


Figura 18 - Análisis herramienta wireshark - Fuente Propia

Posterior a que se realiza el ataque se puede observar como la características de hardware del servidor empiezan a evidenciar un alto consumos en la conexión de red y la capacidad de la CPU

dando picos con valores por encima del 80%, dando la saturación en los procesos del servidor y de esta forma impidiendo el uso a los usuarios del servicio WEB.

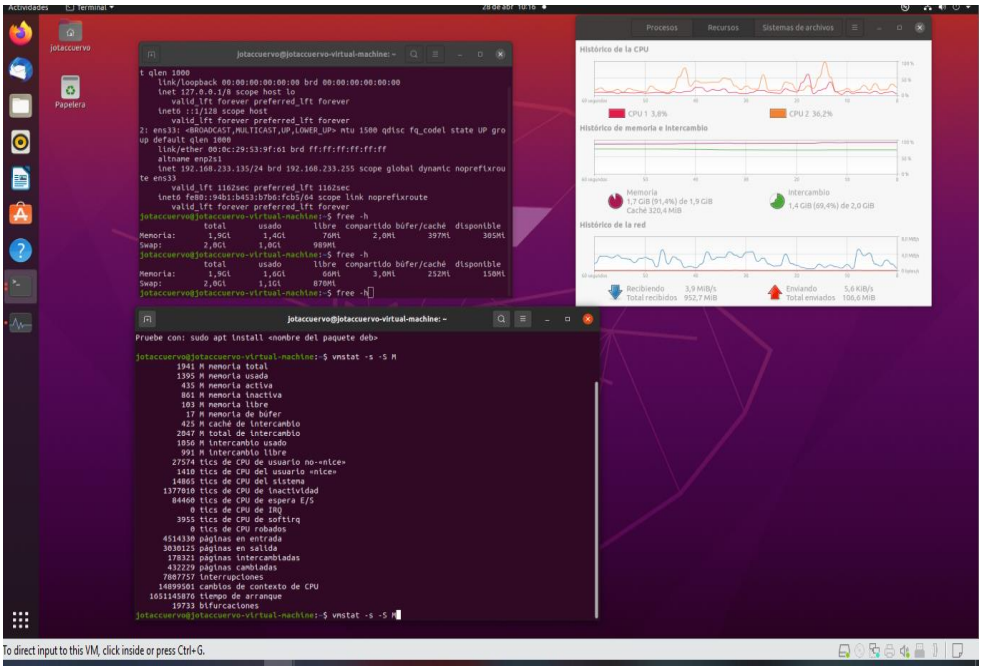


Figura 19 - Análisis Servidor - Fuente Propia

Cuando se trata de ingresar al servicio web que ofrece OPENBCI_WEB, podemos identificar que no fue posible ya que el servidor quedo inoperativo.

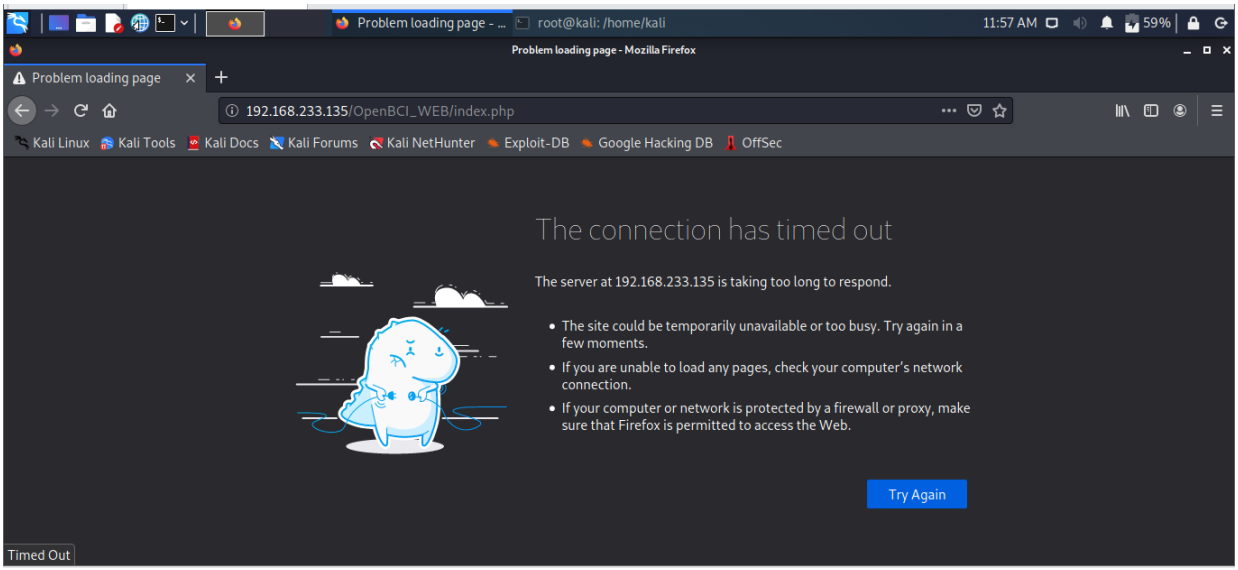


Figura 20 - Servicio Web inoperativo - Fuente Propia

3.2.5.2 Ataque informático de tipo Scanning:

Este tipo de ataque también conocido como port scan, tiene como objetivo que el atacante tenga la mayor cantidad de información procedente del servidor, todo esto basado en una investigación de puertos abiertos y servicios donde se revisan de manera automática y sistemáticamente los puertos.

Para esta primera fase de análisis de puertos se utilizó la herramienta Nikto, donde esta es un escáner de servidores web y de vulnerabilidades.

Los resultados de este escaneo fueron:

- Información del tipo de servidor web apache /2.4.41,
- El tipo de sistema operativo: UBUNTU
- Las cabeceras de las conexiones web
- Las fallas de configuración: anti-clickjacking que permite el secuestro de la página web
- Las fallas de configuración: X-XSS-Protection, lo que significa que cualquier página de este sitio web podría correr el riesgo de sufrir un ataque Cross-Site.

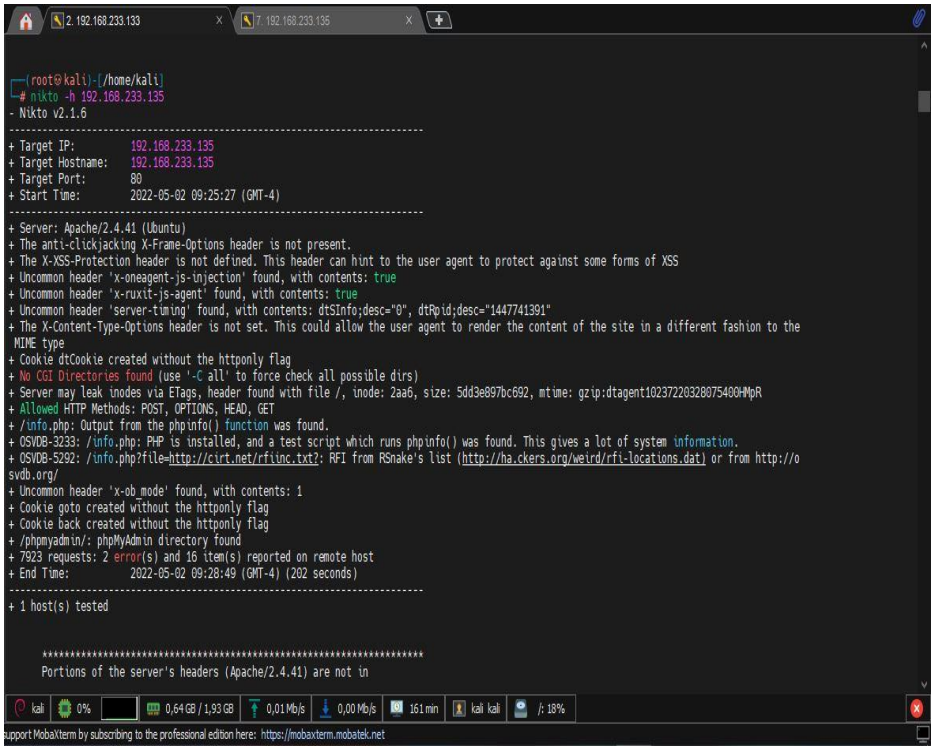


Figura 21 - Ataque informático de tipo Scanning - Fuente Propia

Resultados

En la segunda fase del ataque tipo scanning se utilizó la herramienta DIRB KALI LINUX, DIRB es un escáner de contenido web y busca objetos Web existentes y ocultos. Utilizando diccionarios contra un servidor web y analizando las respuestas.

Los resultados de este escaneo fueron:

Ingreso a dos servicios: phpmyadmin/index.php y info.php

Se encuentra que dos servicios que deben ser privados están de manera pública, basados en una mala configuración y exposición, esto significaría una falla de seguridad del servidor, dejando a éste a posibles ataques.

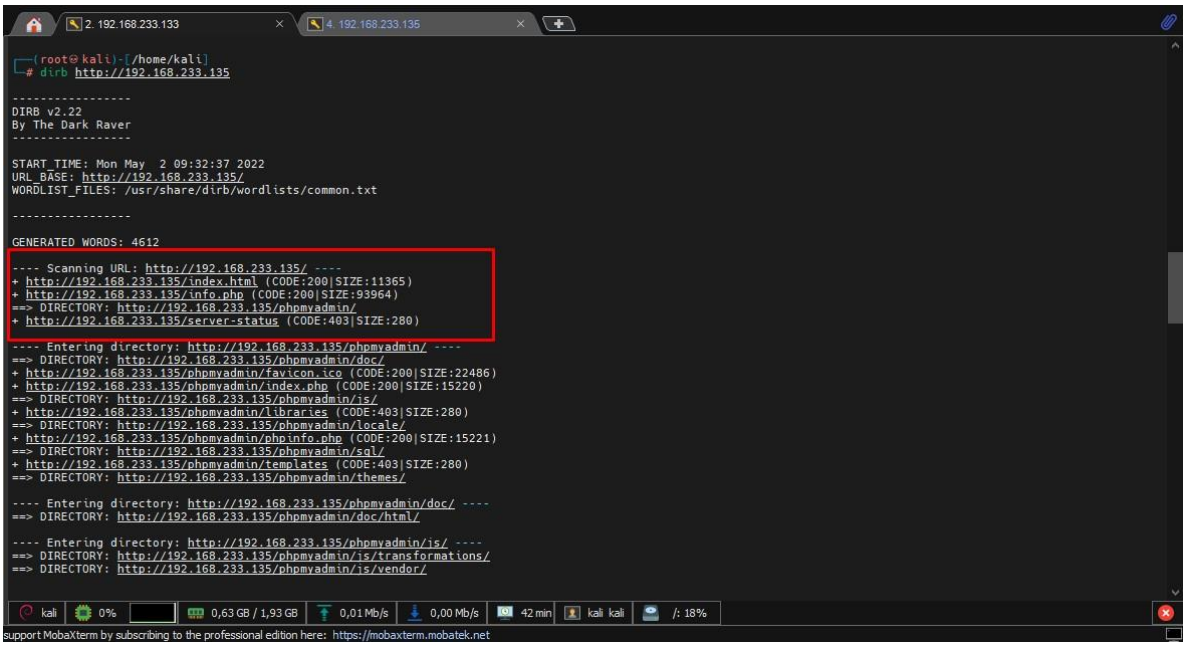


Figura 22 - Escáner de contenido web, herramienta Dirb - Fuente Propia

Resultados

Este servicio de bases de datos está expuesto ante un atacante con experiencia podría encontrar las credenciales de login y poder ingresar al motor de base de datos. phpmyadmin/index.php

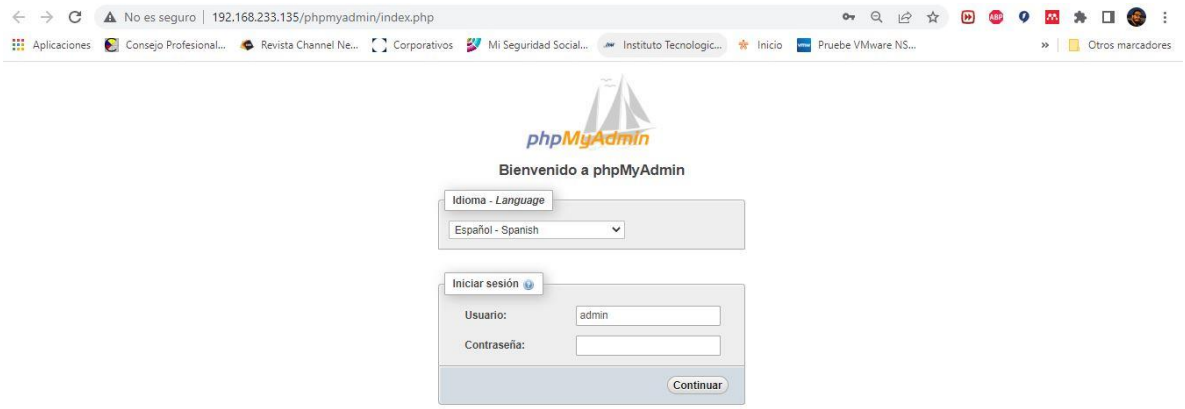


Figura 23 - Motor de base de datos - Fuente Propia

Este servicio PHP de configuración está expuesto y puede ser editado las características del servicio y librerías /info.php

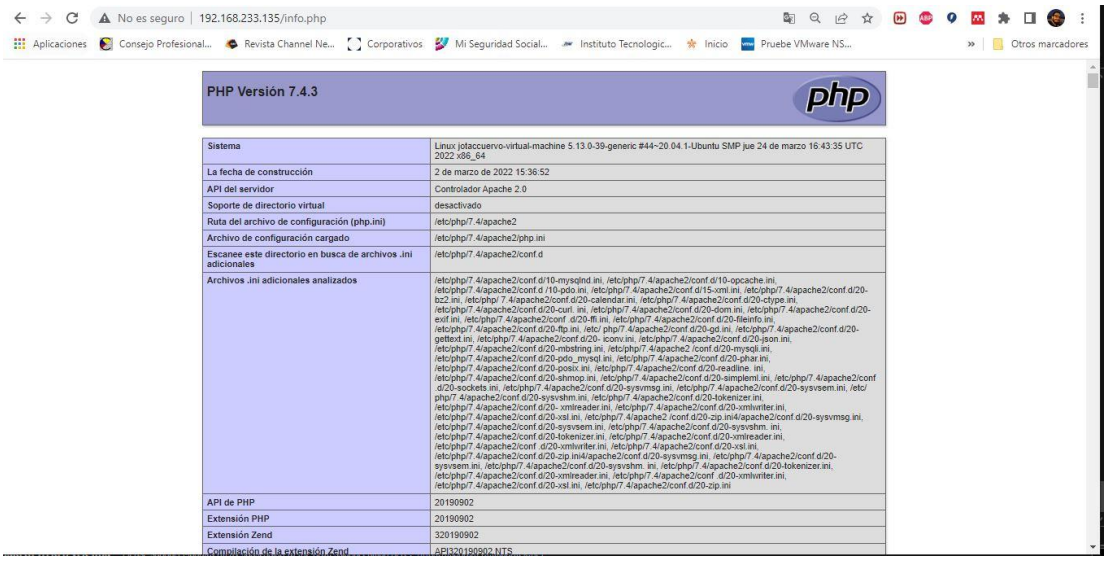


Figura 24 - Configuración servicio PHP - Fuente Propia

3.2.5.3 Ataque informático de tipo PASSWORD CRAKING

El ataque tipo PASSWORD CRAKING también conocido como ataque de fuerza bruta, donde su objetivo es conocer las credenciales de acceso a un host para esta tarea se utilizan diccionarios de usuarios y passwords que son usuales en los sistemas hasta que se encuentre una coincidencia de las credenciales y se pueda dar acceso al servicio atacado.

En este caso se hizo un análisis de puertos abiertos utilizando NMAP que entrego el listado.

Se puede evidenciar que se encuentra los servicios FTP puerto 21 y SSH puerto 22 abiertos, con una breve descripción de sus características y versiones, un atacante experimentado con esta información podría buscar exploits diseñados para este servicio activos.

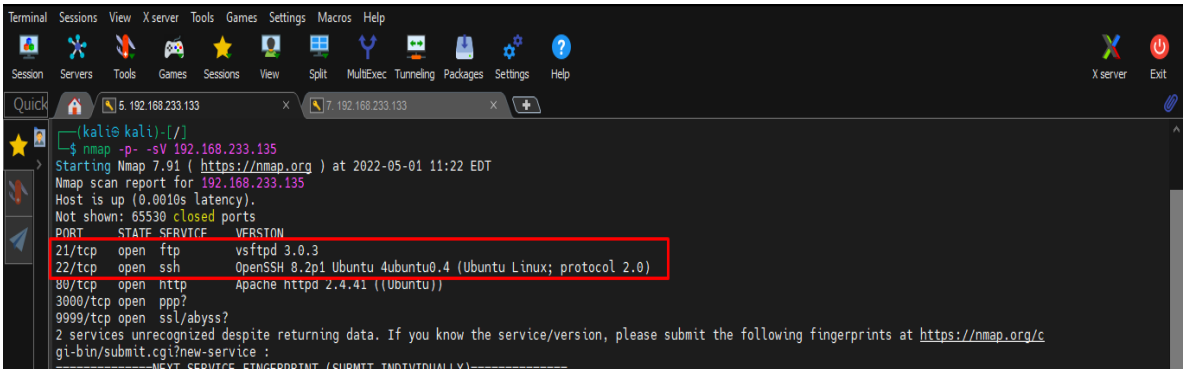


Figura 25 - Ataque informático de tipo PASSWORD CRAKING - Fuente Propia

Se realizó un análisis simple de usuarios y passwords donde se pudo determinar que se tenía las configuraciones legacy del servicio, donde el usuario del servicio FTP era ADMIN, esto da un punto de partida para el siguiente paso del ataque.

Resultados

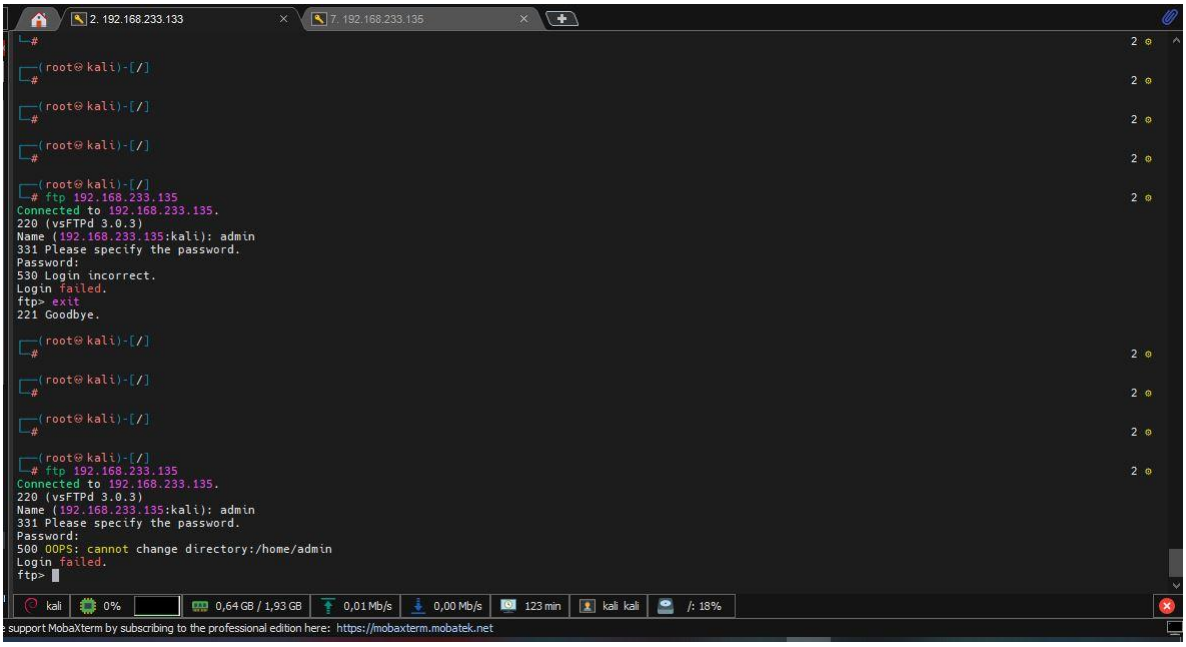


Figura 26 - Análisis simple de usuarios y passwords - Fuente Propia

Con la ayuda de la herramienta HYDRA de KALY LINUX, se pudo crear un script donde se utiliza una librería de passwords llamada fastrack.txt y utilizando el usuario encontrado anteriormente.

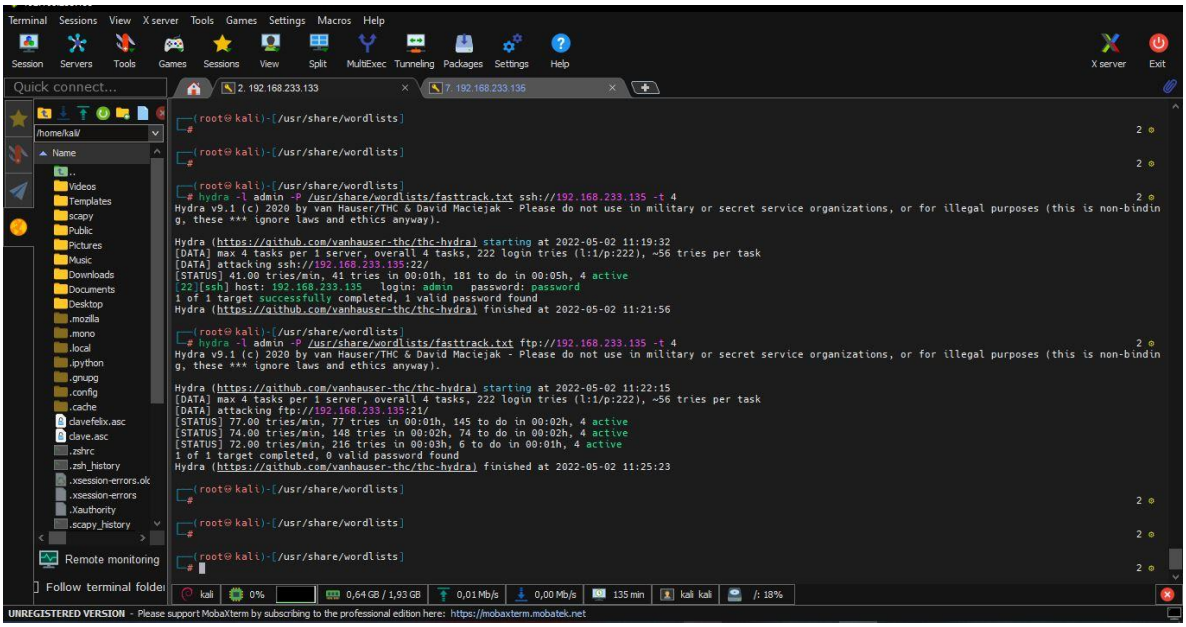


Figura 27 - Prueba herramienta HYDRA - Fuente Propia

Resultados

Posterior al ataque de fuerza bruta con la herramienta HYDRA, se pudo ganar una Shell con el servicio SSH por el puerto 22 y con ella se pudo hacer movimientos en las diferentes librerías.

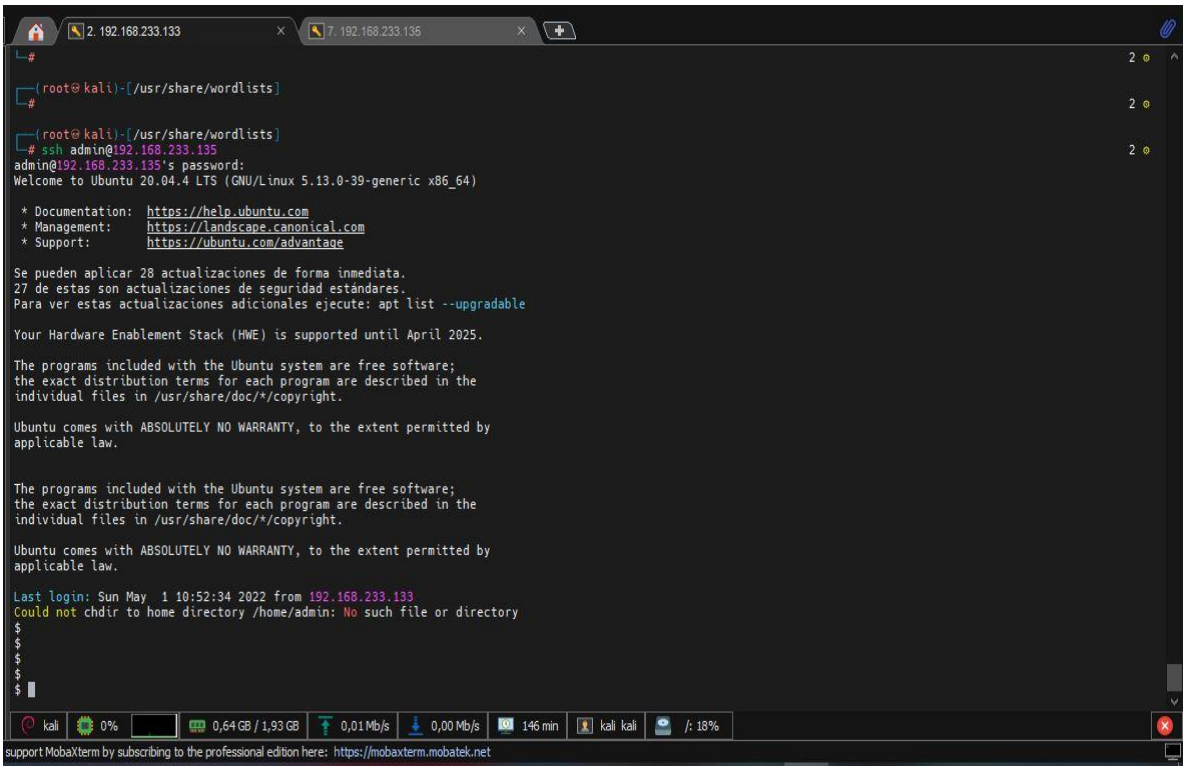


Figura 28 - Ataque de fuerza bruta con la herramienta HYDRA - Fuente Propia

3.2.5.4 Ataque informático de tipo: Exploit o Modificación no autorizada de datos e información:

El ataque tipo modificación no autorizada se deriva de procesos de aprovechamiento de vulnerabilidades que pueda tener un dispositivo que sea parte de una red de telecomunicaciones, en esta caso el servidor Ubuntu que tiene el servicio de BCI, al haber vulnerado su seguridad y poder tener acceso a su librerías el siguiente paso por parte de un atacante es poder tener acceso a información relevante del sistema, deteriorando la confidencialidad, integridad y autenticidad de los archivos y documentos que hacen parte del servidor.

Resultados

En este caso se puede evidenciar como el atacante tiene acceso a diferentes librerías críticas del servidor donde puede ver los usuarios de sistemas, dando así un escalamiento de privilegios y poder extraer información no autorizada y privada.

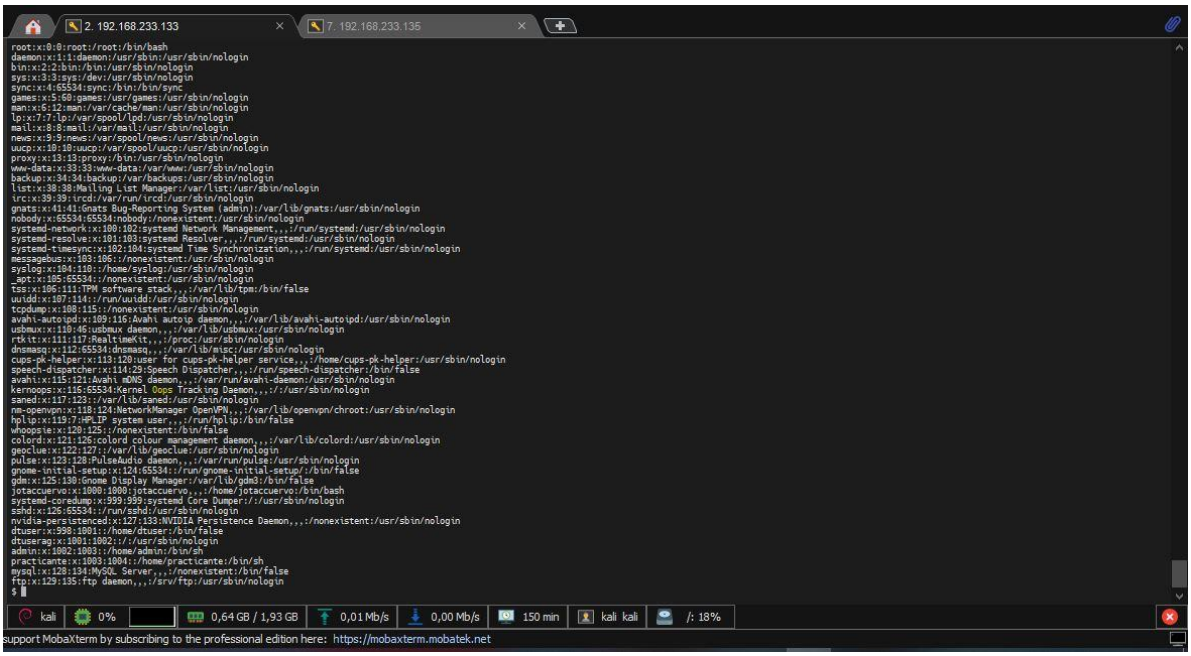


Figura 29 - Ataque informático de tipo: Exploit o Modificación no autorizada de datos e información - Fuente Propia

3.2.6 Plan de tratamiento

Después de realizar la valoración de los riegos y al ejecución de los ataques informáticos, se pudo constatar que se cuenta con una cantidad 73 escenarios con un porcentaje del 89.02%, estos riesgos potenciales tienen que tener un grado de cuidado y se deben generar unos procesos de tratamientos que tienen que generar unas prácticas donde se pueda tener una capacidad para generar ambientes empresariales de confianza, esto basado en las buenas prácticas y directrices que pueden ser exitosas en la práctica, es por eso que se decide implantar varios escenarios para iniciar el tratamiento efectivo del riesgo.

Se debe tener mucho cuidado con la situación del análisis de vulnerabilidades realizado con el software NESSUS ya que nos entregó una gama de 40 vulnerabilidades con diferentes niveles de afectación a la infraestructura del servidor, es necesario que en ese plan de tratamiento se

les dé una solución a dichas vulnerabilidades ya que son estas las que abren las puerta para que las amenazas que pueden afectar el servidor lleguen a ser explotadas.

3.2.6.1 Fases Plan de Tratamiento:

Fase Uno - Reducir los niveles de riesgos: Solución de amenazas derivadas de las vulnerabilidades encontradas en el proceso de análisis con Nessus.

Se seleccionan un grupo de cuatro diferentes vulnerabilidades para darle la solución, estas probadas anteriormente donde se identifican que son posibles para ser atacadas.

- Actualizar los servicios de conexiones seguras que se pueden tener con diferentes tipos de herramientas como son TLS, Netbios, SSH, Telnet y SMB, estos deberán tener sus últimas actualizaciones y parches de seguridad, tener un control de configuración para mitigar alguna conexión no segura, de igual manera se deberán tener parámetros para contraseñas seguras, cifrado de información y encriptado, el tener herramientas que permitan conexiones son necesarias pero si se deja una brecha abierta pueden convertirse en el camino para ser parte de un ataque cibernético. *Controlar*

  Para controlar esta vulnerabilidad se decidió que en el servidor donde se ejecuta los servicios de BCI, se implementaran varias soluciones:

  Se implementó en las reglas IPTABLES con las que se limitaron las conexiones de la red local, así no permitir escaneos e ingresos por los puertos: 21, 3000 y 9999 que anteriormente se identificaron abiertos.

Resultados

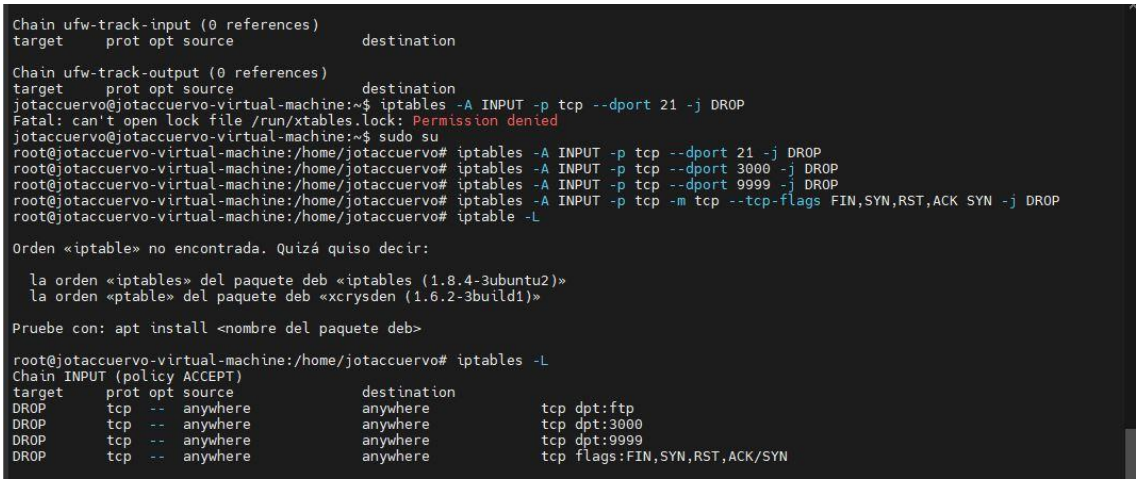


Figura 30 - Reglas IPTABLES - Fuente Propia

- Donde las amenazas asociadas a: Ataque informático de tipo DoS/DDoS, donde se deberá adquirir una solución de Firewall y/o antivirus donde se generarán políticas de control, de igual manera realizar actividades y cursos donde los empleados de la empresa inicien un proceso de aprendizaje sobre diferentes amenazas cibernéticas. *Controlar*

  Para controlar esta vulnerabilidad se decidió implementar un firewall PFSENSE de borde con el que se controla las conexiones de la red WAN hacia el servidor donde se ejecuta los servicios de BCI:

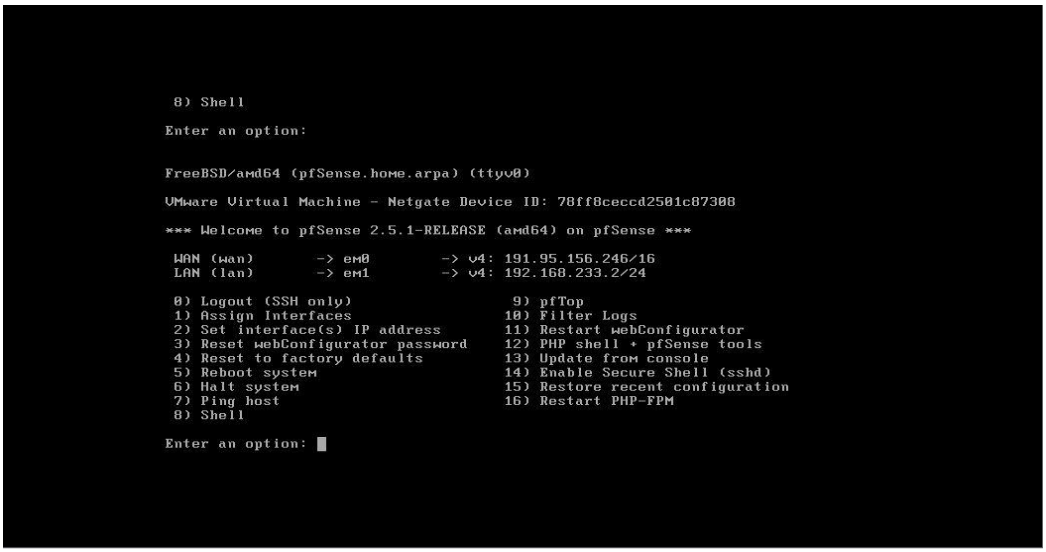


Figura 31 - Firewall PFSENSE - Fuente Propia

Resultados

Se ingresa a la interfaz gráfica del servidor donde se realizaron los cambios de la configuración de las reglas de firewall PFSENSE

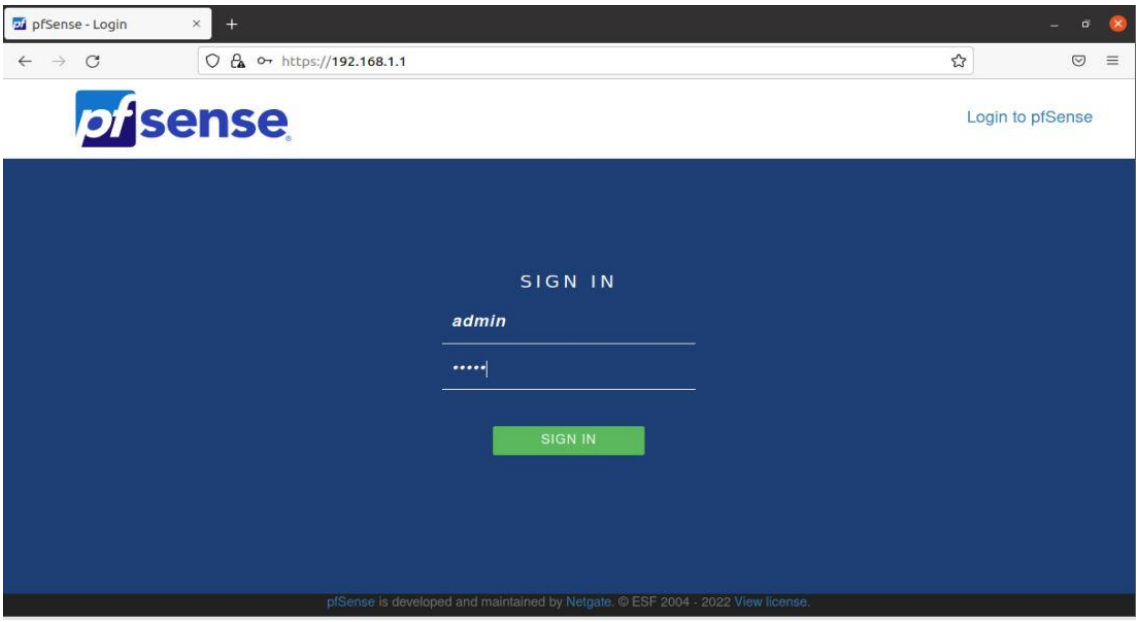


Figura 32 - Servicio Web firewall PFSENSE - Fuente Propia

Se implementó las reglas con las que se limitaron las conexiones de la red externa, así no permitir escaneos e ingresos por los puertos: 21, 3000 y 9999 que anteriormente se identificaron abiertos, para

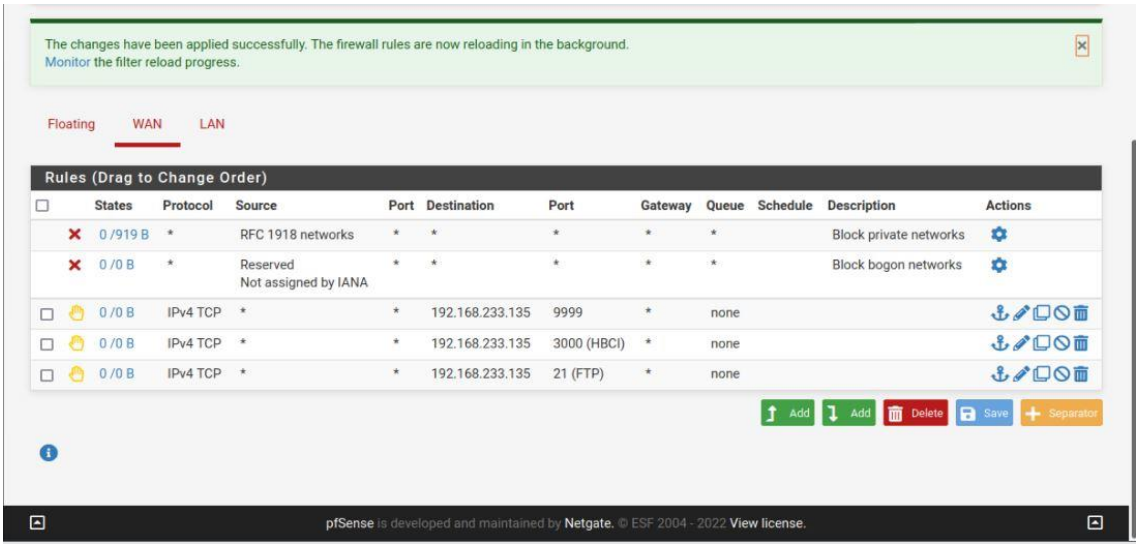


Figura 33 - Configuración de las reglas de firewall PFSENSE - Fuente Propia

Resultados

- Los servidores cuentan con la configuración inicial que viene de fábrica, es necesario cambiar las políticas de configuración para los servicios web y servicios de los gestores de bases de datos que se unifican en los servicios ofrecidos, sino se hacen estos cambios dejaran una brecha por la cual se podrán hacer ingresos al servidor ya que sus niveles de seguridad no son los óptimos, es recomendable crear políticas de login, no permitir conexiones remotas por consola, no permitir ping, generar políticas de trafico de información para evitar ataques DDoS, SQL INJECTION, ESCANNING. *Controlar*

  Para controlar esta vulnerabilidad se decidió implementar un WAF (FIREWALL DE APLICACIONES DE WEB) con el que se controla las conexiones y trafico HTTP de la red WAN y LAN hacia el servidor donde se ejecuta los servicios de BCI:

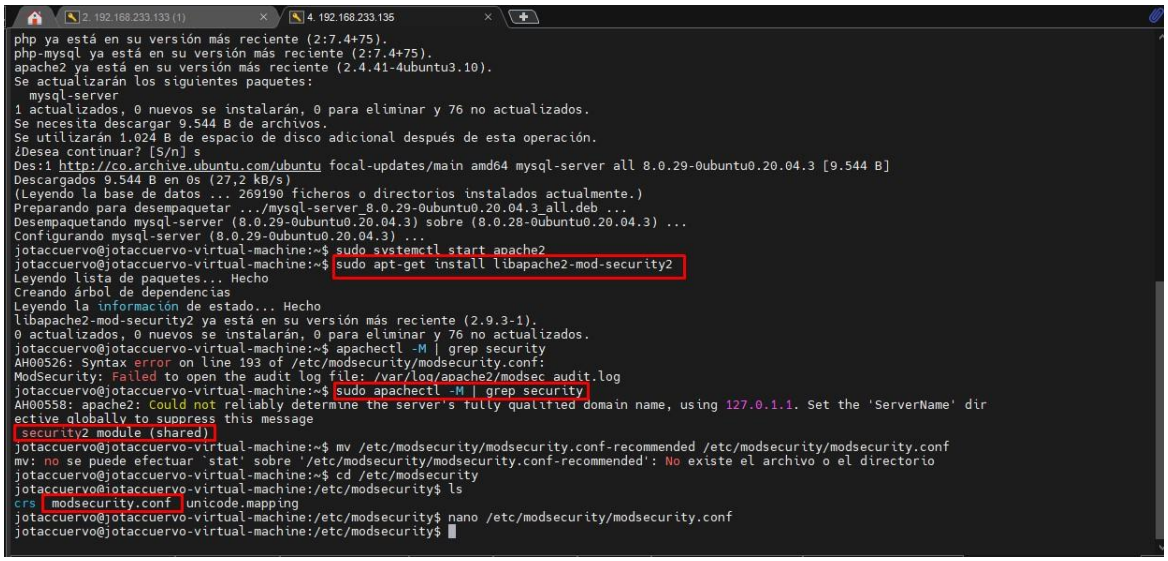


Figura 34 - Instalación WAF Modsecurity - Fuente Propia

En el archivo /etc/modsecurity/modsecurity.conf, se determinan la regla de conexiones, detención de posibles ataques, bloqueos de amenazas, subida y bajada de archivos, informes de errores en logs, archivos de listas blancas y archivo de conexiones negras

Resultados

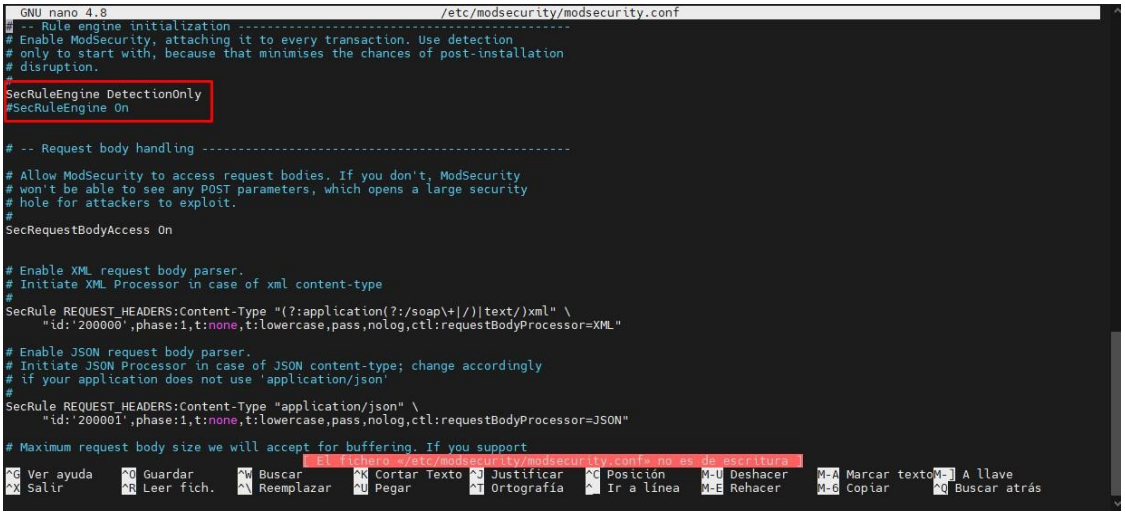


Figura 35 - Configuración WAF Modsecurity - Fuente Propia

Para controlar las conexiones por el servicio SSH se decidió configurar las diferentes reglas para que pueda tener un funcionamiento óptimo y seguro, para ello se ingresó al archivo de configuración y se agregaron políticas de no inicio con el usuario ROOT, se agregó un tiempo de para el intento de login para evitar que un atacante pueda limitar sus intentos de conexión, de igual manera no se permite más de 2 intentos de conexión, esto evita un ataque de fuerza bruta.

Este archivo también permite la configuración de ingreso por claves tipo privada y pública y claves tipo hash.

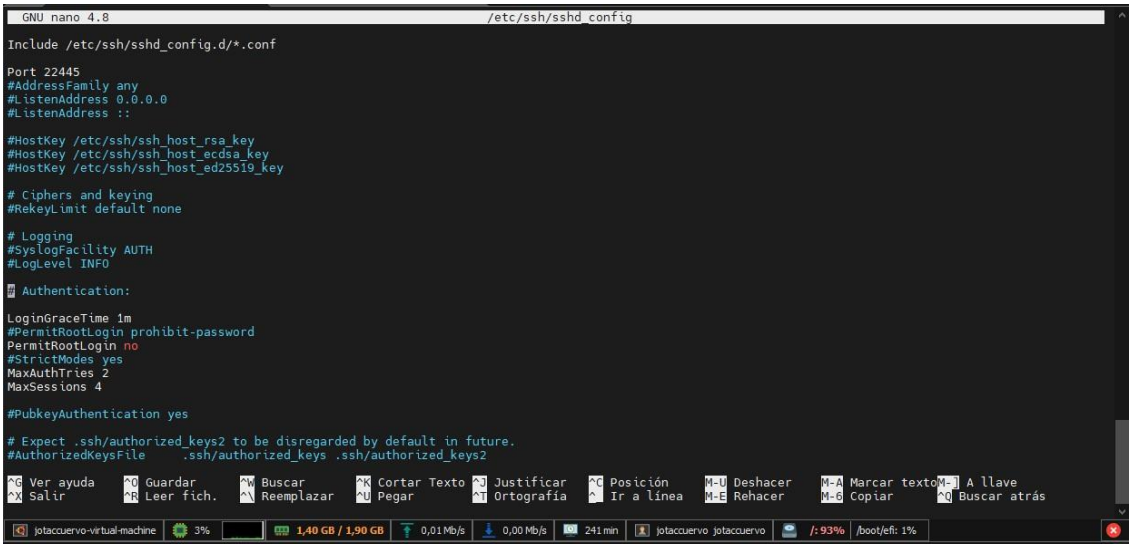


Figura 36 - Configuración Servicio SSH - Fuente Propia

Resultados

Fase Dos - los controles sobre los ataques: Posterior a la implementación de las soluciones a los diferentes riesgos se debe demostrar la efectividad de esta tarea validando su control y la calificación de éstos en el mapa de riesgos para determinar su eficiencia.

3.2.6.2 Análisis de vulnerabilidades Nessus Posterior a la implementación de las soluciones

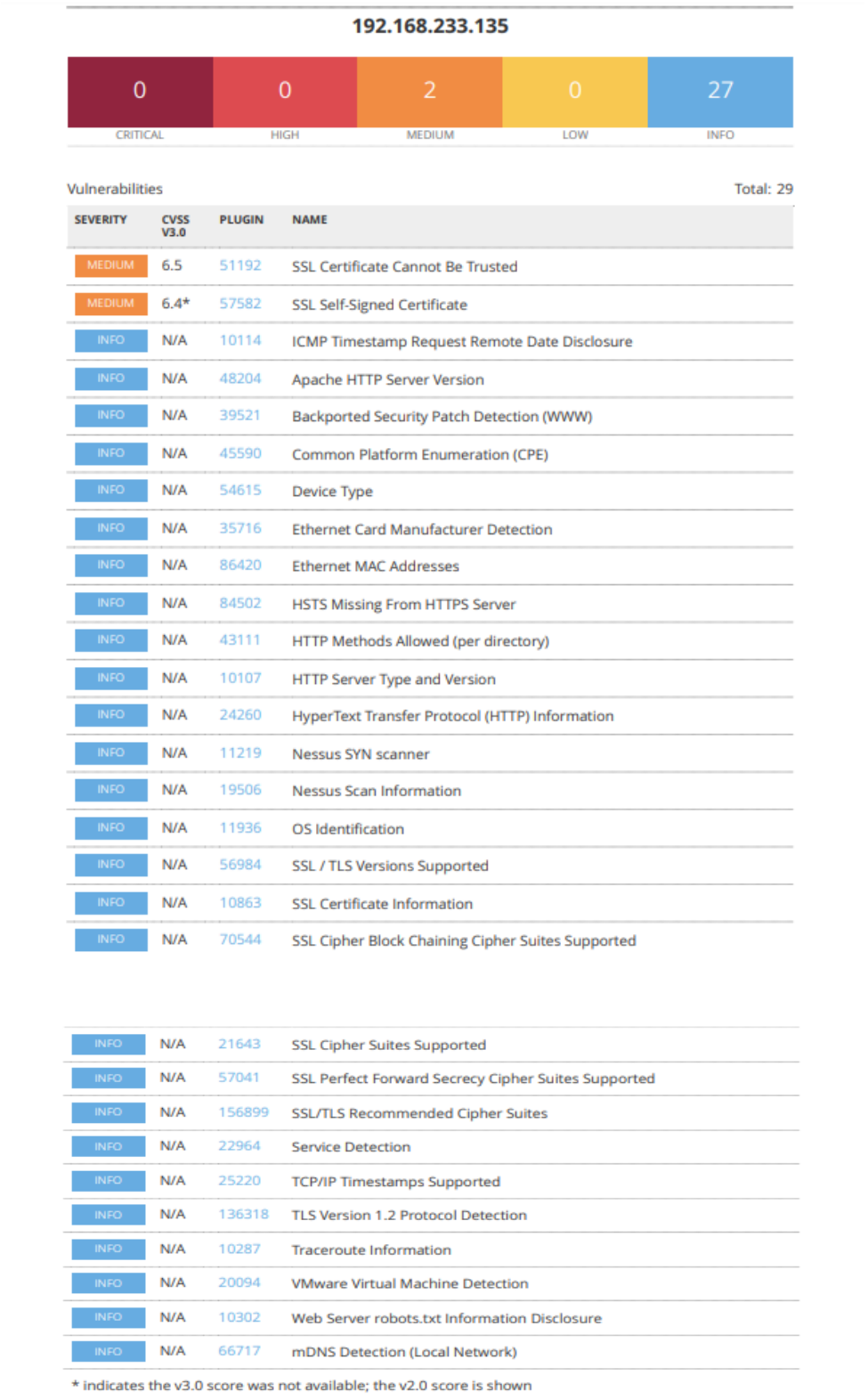
El objetivo principal de este proceso de análisis de vulnerabilidades es el evaluar la efectividad de los controles implementados para mejorar la seguridad a la infraestructura y servicios del servidor Ubuntu BCI, con la finalidad de mitigar las vulnerabilidades y amenazas identificando riesgos e impactos que podría ocasionar, para dicha tarea el escáner utilizado es la plataforma NESSUS que tiene como características:

- Identificar vulnerabilidades en la infraestructura.
- Identificar vulnerabilidades en la página web, motores de bases de datos y servidores de correo
- Identificar fortalezas y deficiencias de la infraestructura implementada
- Entrega de informa de vulnerabilidades y formas de reparación
- Documentación de las vulnerabilidades ligadas a CVE

Se realizó un nuevo proceso de escaneo de vulnerabilidades con la herramienta Nessus Essential y estos fueron sus resultados sobre el servidor Ubuntu BCI:

- Se puede evidenciar una reducción de 11 vulnerabilidades al escaneo anterior donde se muestra un total de 40 diferentes vulnerabilidades en rangos y características.
- Se logra tener un nivel de 29 vulnerabilidades en diferentes rangos y características, esto ya que se realizaron las correcciones necesarias de los hallazgos.

Resultados



192.168.233.135

0	0	2	0	27
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 29

SEVERITY	CVSS V3.0	PLUGIN	NAME
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4*	57582	SSL Self-Signed Certificate
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	39521	Backported Security Patch Detection (WWW)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	84502	HSTS Missing From HTTPS Server
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	10287	Traceroute Information
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	10302	Web Server robots.txt Information Disclosure
INFO	N/A	66717	mDNS Detection (Local Network)

* indicates the v3.0 score was not available; the v2.0 score is shown

Figura 37 - Análisis de vulnerabilidades Nessus Posterior a la Implementación de las Soluciones - Fuente Propia

3.2.6.3 Pruebas Ataques informático

En la primera fase ataque tipo scanning se utilizó la herramienta NMAP

Los resultados de este escaneo fueron: Los 65535 puertos fueron escaneados y todos se encuentran filtrados, esto demuestra que hay un firewall impidiendo saber el estado del puerto.

```
NSE: Script scanning 192.168.233.135.
Initiating NSE at 21:39
Completed NSE at 21:39, 0.00s elapsed
Initiating NSE at 21:39
Completed NSE at 21:39, 0.00s elapsed
Initiating NSE at 21:39
Completed NSE at 21:39, 0.00s elapsed
Nmap scan report for 192.168.233.135
Host is up (0.00026s latency).
All 65535 scanned ports on 192.168.233.135 are filtered
MAC Address: 00:0C:29:53:9F:61 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

Figura 38 - Solución ataque tipo scanning, herramienta NMAP - Fuente Propia

En la segunda fase ataque tipo scanning: Se hizo un análisis de puertos para ello se utilizó la herramienta Nikto, donde esta es un escáner de servidores web y de vulnerabilidades.

Los resultados de este escaneo fueron: No se encontró ningún host, esto nos demuestra que el control que se creó impidió la realización del escaneo del servicio.

En la tercera fase ataque tipo scanning: Se utilizó la herramienta DIRB KALI LINUX,

Los resultados de este escaneo fueron: No se encontró ningún host, página web o servicio en la IP, esto nos demuestra que el control que se creó impidió la realización del escaneo del servicio.

En la cuarta fase ataque tipo DDoS: Se utilizó la herramienta HPING 3

Los resultados de este ataque fueron: No fue posible hacer el desbordamiento de solicitudes, se rechazó la conexión.

Resultados

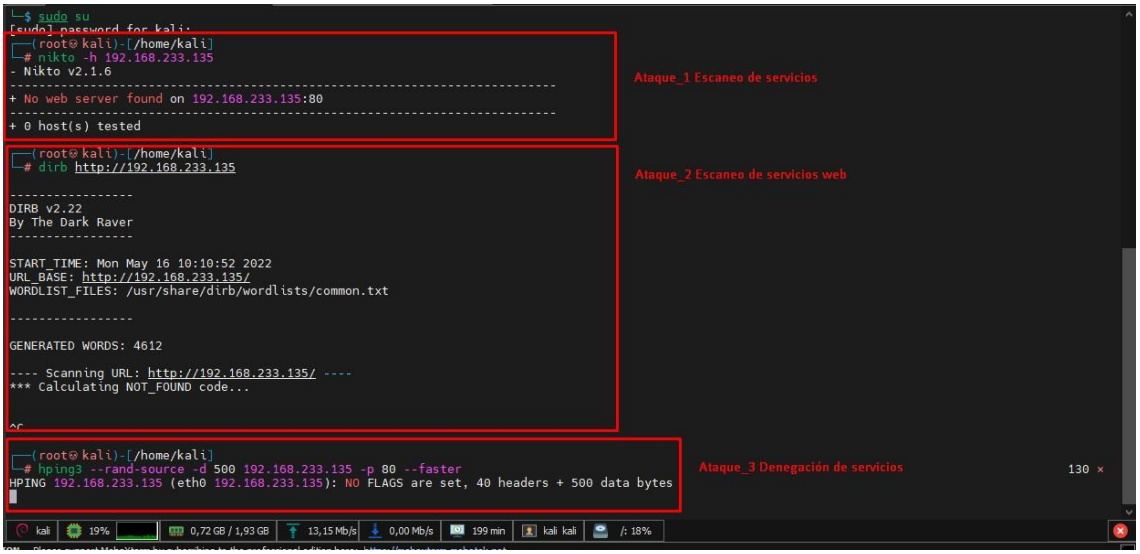


Figura 39 - Solución Ataque tipo Scanning – Fuente Propia

En la quinta fase ataque tipo scanning: Conexión a páginas de configuración de servicios del servidor Ubuntu BCI.

Los resultados de este ataque fueron:

- Este servicio PHP de configuración no está expuesto y no puede ser editado info.php, se encuentra FORBIDDEN, eso demuestra que la configuración del WAF bloqueo las conexiones a los servicios.

Figura 40 - Solución Ataque Scanning, servicio info.php - Fuente Propia

Resultados

- Este servicio de bases de datos no está expuesto donde se puede ingresar las credenciales de login y poder ingresar al motor de base de datos. phpmyadmin/index.php, se encuentra FORBIDDEN, eso demuestra que la configuración del WAF bloqueo las conexiones a los servicios que no deben ser expuestos.

Figura 41 - Solución Ataque Scanning, servicio phpmyadmin/index.php - Fuente Propia

En la quinta fase ataque tipo PASSWORD CRAKING también conocido como ataque de fuerza bruta: Se puede evidenciar que se encuentra los servicios FTP puerto 21 y SSH puerto 22 cerrados y el puerto 22445 hacia donde se migro el servicio SSH no permite más de 2 intentos fallidos de login, seguido al Timeout de 1 minuto sino se intenta la conexión al servicio.

Resultados

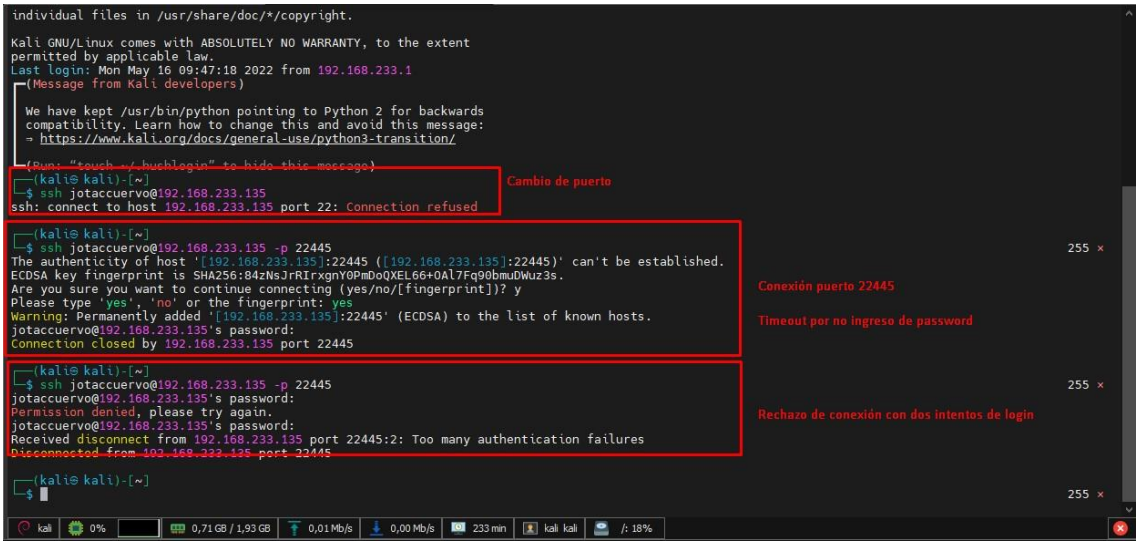


Figura 42 - Solución Ataque informático de tipo PASSWORD CRAKING - Fuente Propia

3.2.7 Análisis de Riesgos Posterior a la Implementación de las Soluciones

Posterior al análisis de las diferentes pruebas que se realizaron en el servidor Ubuntu BCI, se realizó una nueva calificación de los riesgos, ya que sus niveles de exposición y vulnerabilidades sufrieron cambios significativos dado el plan de tratamiento, para esta tarea se tomaran las tablas de probabilidad de frecuencia y la tabla de impacto de imagen para hacer las calificaciones idóneas todo esto ligado a la norma ISO 27001, como marco de referencia que fue la elegida para la implementación.

Nivel	Rangos	Ejemplo detallado de la descripción
1	**Raro**	Puede ocurrir solo bajo circunstancias excepcionales
2	**Improbable**	Podría ocurrir algunas veces
3	**Posible**	Puede ocurrir en algún momento
4	**Probable**	Probabilidad de ocurrencia en la mayoría de las circunstancias
5	**Casi seguro**	La expectativa de ocurrencia se da en la mayoría de las circunstancias

Tabla 11 Valoración de las Frecuencias/probabilidad

Nivel	Rangos	Ejemplo detallado de la descripción
1	**Insignificante**	Se identifica el problema de imagen a nivel del grupo de trabajo
2	**Menor**	Se identifica el problema de imagen a nivel empresa.
3	**Intermedio**	Se identifica el problema de imagen a nivel regional.
4	**Mayor**	Se identifica el problema de imagen a nivel nacional.
5	**Superior**	Se identifica el problema de imagen a nivel internacional.

Tabla 12 Impacto de Imagen

3.2.7.1 Resultados Calificación Riesgos [24, 25].

Después de realizar el análisis y el control de los riesgos se pudo determinar que:

Se cuenta con una cantidad verificada de escenarios con diferentes probabilidades e impactos donde se puede ver afectada la tareas diarias donde el servidor Ubuntu con los servicios de bases de datos, plataformas web y correo electrónicos, cuentan con unos riesgos reales y con una calificación de estos donde se pueden observar que varios de estos son de suma importancia tenerlos bajos control, cuando vemos la tabla 14 de distribución de los riesgos es notorio que se cuentan con 13 casos que son aceptables con un 17.81%, donde se tiene información sobre estos y sus probabilidades de ocurrencia son bajos (improbables), es necesario estar en continuo análisis para que no vayan a tener una escalabilidad y puedan convertirse en amenazas relevantes.

ZONA	%	Total, riesgos
Aceptable	**17,81**	**13**
Tolerable	**35,62**	**26**
Inaceptable	**42,47**	**31**
Inadmisible	**4,11**	**3**

Tabla Distribución Porcentual de Riesgos - Fuente propia

Por otro lado, 26 escenarios tienen un nivel de tolerables, donde sus probabilidades de suceso son posibles y un impacto sea menor, este 35.62 % es relevante iniciar con un proceso de verificación y análisis ya que aunque no tiene una aceptabilidad en los procesos de la organización se deben tener monitoreados y generar procesos de verificación ya que están a un paso de convertirse en amenazas latentes dentro de la organización, esta tasa porcentual de escenarios tolerables es muy significativa, es importante no perder de vista su evolución, en un futuro sería recomendable tratar de minimizar a una tasa porcentual a un nivel inferior del 30%.

De igual manera en el análisis de la tabla de distribución de riegos, se puede disponer y verificar una información inaceptable, donde se tiene la cantidad de 31 escenarios que están en la escala de inaceptables con un porcentaje de 42.47%, es por ello que se debe tener un grado de cuidado y generar unos procesos de control de estos, ya que están en un nivel donde puede llegar afectar el desarrollo normal de la operación empresarial, es necesario no conceder ninguna escalabilidad de estos casos se conviertan en situaciones recurrentes en el ámbito empresarial, en términos de protección se debe de regir unos procesos de control y su tratamiento.

Para finalizar se puede constatar que se cuenta con 3 escenario inadmisible, con un 4.11%, este nivel es importante tener un control y una verificación ya que este es el nivel más relevante, ya que su ocurrencia podría significar un nivel de afectación mayor al que se está dispuesto de aceptar, es necesario estar haciendo verificaciones y auditorias ya que sí no se generan controles y tratamientos cualquier riesgo puede entrar a este nivel**.**

Por otro lado, hay que se evidencio que el proceso de Ethical hacking varios ataques no fueron realizados y varias de las vulnerabilidades encontradas en las pruebas con la herramienta NESSUS demuestran altos niveles de probabilidades de ocurrencia, por lo tanto, se hacen recomendaciones hacia las diferentes amenazas para que se minimicen los niveles de exposición al riesgo y se pueda hacer una contención de las vulnerabilidades presentes.

3.2.7.2 Acciones por Tomar con Amenazas Presentes

- Donde las amenazas asociadas a: Ataque informático de tipo SSL Stripping, deberá ser controlado, Los certificados SSL deberán ser actualizados basado en los dominios de las páginas

web que se tiene montadas en el servidor, con esto se mitigara la falencia de seguridad en los procesos de autenticación de transferencias, credenciales y compras, también los procesos de navegación serán seguros donde la transmisión de datos entre cliente y servidor estarán encriptadas o cifradas.

- Donde las amenazas asociadas a: Ataque informático de tipo SQL Injection, deberá ser controlado realizando por parte de los desarrolladores buenas prácticas en los controles de la aplicación, haciendo en las aplicaciones auditorías continua en seguridad, esperando que las brechas de seguridad sean mínimas ante este tipo de ataques.
- Donde las amenazas asociadas a: Ataque informático de tipo DNS Reflexion/Amplication, deberá ser controlado, donde se deberá adquirir una solución de Firewall y antivirus donde se generarán políticas de control, de igual manera realizar actividades y cursos donde los empleados de la empresa inicien un proceso de aprendizaje sobre diferentes amenazas cibernéticas.
- Donde las amenazas asociadas a: Ataque informático de tipo Buffer overflow, deberá ser controlado, se deberá realizar por parte de los analistas de seguridad TI y de monitoreo, un control de las solicitudes que lleguen a los servidores de bases datos validando las solicitudes entrantes para que no exista un desbordamiento de solicitudes que hagan que los servidores tengan congestión en solución de solicitudes.
- Donde las amenazas asociadas a: Ataque informático de tipo Ramsomware, deberá ser controlado, donde se deberá adquirir una solución de Firewall y antivirus donde se generarán políticas de control, de igual manera realizar actividades y cursos donde los empleados de la empresa inicien un proceso de aprendizaje sobre diferentes amenazas cibernéticas.

3.2.8 Plan de Monitoreo

Diseñar un control de cambios por cada servicio vulnerable que el proceso de Ethical Hacking evidenció con el archivo generado por Nessus, ligado a un modelo de seguridad y las políticas de seguridad a implementar, donde el plan de monitoreo identifique los siguientes pasos:

- Fechas de inicio y finalización

Resultados

- Equipo responsable
- Indisponibilidad del servicio
- Resumen de la actividad
- Justificación de la actividad
- Arquitectura por intervenir
- Identificación de riesgo de la actividad
- Plan de trabajo
- Plan de Rollback
- Actas de entrega.

Estas actividades deben ser aprobadas por un comide de cambio que valore y certifique la actividad.

- Acceso físico no autorizado/indebido, se deben aplicar una serie de estrategias de control, como objetivo de prevenir el acceso, como las instalaciones deben estar monitoreadas para detectar desviaciones de las políticas de control de accesos y grabar los eventos específicos para proveer de evidencia en caso de incidentes de seguridad, establecer controles de perímetro como asistencia física vigilada, tarjetas HID con permisos establecidos a ciertas partes de las instalaciones, sensores conectados a centrales de alarmas, sistemas de rayos x, sistema biométricos fisiológicos, sistema biométrico conductual, estos controles deben estar habilitados todo el tiempo, y la revisión de los informes de acceso de personas cada semana, con esto se garantiza un amplio control de los accesos como el reporte de tiempo, encargado Transferencia interna (Una empresa seguridad).
- Ataque informático de tipo SQL Injection, se deben configurar herramientas de monitoreo sobre las instancias del base de datos, con el objetivo de monitorear su salubridad, consumos, plan de backup, procesamientos, consultas realizadas y los tiempos de duración, estas consolas deben ser monitoreadas todo el tiempo, y los informes deben contener salubridad y consumos por cada una de las instancias monitoreadas, para establecer normales procesamiento en líneas de tiempo, encargado: Desarrolladores de aplicaciones.
- Ataque informático de tipo DNS Reflexion/Amplication, se deben implementar soluciones de

seguridad, y con estas establecer las reglas y/o políticas necesarias para este tipo de ataques, lectura diaria de los logs de las consolas, revisión de salubridad de los servidores, estas consolas deben ser monitoreadas todo el tiempo, y los informes deben contener salubridad y consumos por cada una de las instancias monitoreadas, para establecer normal procesamiento en líneas de tiempo, encargado: Analistas de seguridad perimetral.

- Ataque informático de tipo DoS/DDoS, se deben implementas soluciones de consola de monitoreo para evidenciar solicitudes atendidas por la infraestructura, revisión de los volúmenes de peticiones, monitoreo de la granja de servidores como los balanceadores, establecer políticas y reglas constantes de peticiones repetitivas y desviarlas a sistemas controlados, banear los altos consumos evidenciados, estas consolas deben ser monitoreadas todo el tiempo, y los informes deben contener salubridad y consumos por cada una de las instancias monitoreadas, para establecer normal procesamiento en líneas de tiempo, encargado: Analistas de seguridad perimetral.
- Ataque informático de tipo Buffer overflow, configurar herramienta de monitoreo sobre los servidores sobre los servidores y ejecutar revisión de logs para determinar compartimentos anómalos y de intrusos, estas verificaciones deben ser aplicada todo el tiempo, y los informes semanales para revisión de comportamiento normal en el tiempo, encargado: Analistas de monitoreo del área de seguridad.
- Ataque informático de tipo Ramsomware, se deben ejecutar tareas diarias de escaneo sobre los equipos configurados, establecer políticas de seguridad sobre direcciones IP reportadas con posibles ataques de Ramsomware, revisión de comportamiento de integridad de los archivos, encargado: Analista de seguridad perimetral.

Se observa en función de lo planteado, que el modelo de seguridad que se diseñó e implemento (en cumplimiento del objetivo general) es un método que brinda una gestión de riesgos de seguridad informática, esto basado en la implementación de las políticas diseñadas y en las pruebas que se desarrollaron posterior a la implementación de los controles en los servicios del sistema BCI, donde se da un mejora en la seguridad, ya que al probar nuevamente los ataques se pudo evidenciar con los escaneos de vulnerabilidades y la calificación del mapa de riesgos,

que los niveles de afectación tuvieron una reducción en sus tablas de valoración de riesgos, estos se puede considerar un medio para la mitigación de brechas ya que la disponibilidad de los datos y su protección son ejes fundamentales para que el sistema cumpla a cabalidad sus objetivos.

4. Conclusiones, recomendaciones y trabajos futuros

Dentro de este orden de ideas, se parte desde el análisis del estado del arte sobre cómo se encuentra la seguridad en este tipo de sistemas y como este tipo de métodos analíticos que buscan evaluar la cantidad de vulnerabilidades que se pueden detectar puede beneficiar los niveles críticos de seguridad en entornos empresariales e investigativos. Esto se realiza a través de datos subjetivos, pruebas expertas y/o de técnicas de análisis. Las pruebas se realizan haciendo diferentes ataques en los procesos que cuenta la adquisición, clasificación y disponibilidad de los datos y/o servicios, logrando evidenciar, cual es el punto más débil asociado con este tipo de nuevas tecnologías, debido a sus limitaciones por sus diseños, ya sea de arquitecturas físicas de hardware o diseños de software, sistemas operativos, APIs y APPs, dado que los sistemas BCI, cuenta con datos y software de libre disponibilidad para su uso, donde se realizan diseños de algoritmos que pueden abrir las puertas a brechas de seguridad, es por eso que el analizar los impactos y documentar los ciberataques en sus diferentes fases tendrá en gran medida un impacto en la implementación de estos sistemas y como los agentes que hacen parte de los desarrollos deberán ser más cuidadosos.

Es por ello que se han visualizado diferentes mecanismos de ataques sobre las interfaces BCI ligados al listado de vulnerabilidades que se encontró en el mapa de riesgos, con éstos fue vulnerado el sistema y así extraer, limitar y disponer de servicios, datos e información. Se ha planteado la necesidad de establecer mecanismos de control que puedan reducir los niveles de riesgo ante estas situaciones de ciberseguridad, esta limitación en ciberseguridad afectan la integridad de los datos que son utilizados y procesados, dado que fue muy simple obtener información a través de diferentes pruebas y ataques utilizando la metodología de hacking ético, lo que implica que los sistemas no estaban preparados para ataques informáticos ni tampoco para comprender la importancia de reducir los niveles de exposición de los riesgos asociados a vulnerabilidades y amenazas.

Conclusiones, recomendaciones y trabajos futuros

En esta perspectiva, el modelo de seguridad que se implementa, encuentra base sólida para determinar que el uso de marcos de referencia como lo son la ISO 27000, ligado a los medidas ofrecidas exactamente por la ISO 27005 que tiene como objetivo contribuir en los parámetros relacionados con la infraestructura técnicas y tecnologías de proyectos para la gestión en las etapas del riesgo, junto la normativa ISO 27001 que es un manual con el que se puede generar procesos de gestión de seguridad, que plantean buenas prácticas para la prevención, gestión y solución ante ataques de seguridad Informática, ligado a unas políticas de ciberseguridad que promuevan el cuidado de la información, donde se tendría que analizar qué tan expuestos están los dispositivos que pueden ser utilizados para los sistemas BCI, controlar las brechas de seguridad en los agentes que hacen parte del ecosistema de los sistemas BCI como son computadores, celulares, servidores y dispositivos IoT, unido a los softwares diseñados para interactuar entre la maquina y el usuario que utiliza la solución, pueden dar cuenta de los impactos reales que se pueden generar en los diferentes componentes, cumple con un potencial para la mitigación de los impactos por problemas asociados en ciberseguridad, determinando las necesidades de integrar este tipo de modelos, como requisito de seguridad en la estructura y metodología para ser ejecutado, en los procesos de desarrollo de los sistemas BCI, definiendo nuevos estándares y requisitos de seguridad como objetivos. de estas nuevas tecnologías.

En relación con la idea anterior, se demuestra que el modelo de seguridad es potencialmente ajustable para proyectos futuros, donde el determinar nuevos niveles de seguridad, amenazas emergentes y entornos productivos puede dar un alcance de mejora continua, donde su rendimiento para la mitigación y exposición a riesgos pueda tener parámetros más aceptables para uso investigativos o comercial, convirtiéndose en un proceso ajustable para la seguridad en este tipo de tecnología.

Los proyectos futuros pueden estar ligados a modelos de seguridad en código fuente en el desarrollo de aplicaciones y configuración de los sistemas BCI, utilizando como marco de referencia las pautas de OWASP, donde se puedan validar, la identificación de vulnerabilidades

de software con pruebas IAST, DAST Y RAST. Seguido de evaluación de vulnerabilidades, plan de tratamiento en códigos fuentes y verificación del modelo.

5. Anexos

5.1 Anexo A Roles y responsabilidades

Área Dirección General:

Responsabilidad:

- Definir estrategias y procesos que garanticen la disponibilidad, confiabilidad, confidencialidad, integridad, eficiencia y eficacia de los productos TIC y de la infraestructura tecnológica sobre la cual operan
- Dirigir y coordinar la gestión científica, tecnológica y económica de los servicios ofrecidos.
- Cumplir y hacer cumplir las normas legales, los estatutos y los reglamentos institucionales.
- Dirigir el proceso de planeación de los procesos de la empresa.
- Diseñar política de seguridad de la información
- Diseñar proyectos de mejoramiento, ampliación y utilización racional y adecuada de la planta física disponible y proponerlos al gerente para su aprobación.
- Llevar a cabo mediante adjudicación por licitación, los proyectos de planta física que sean aprobados.
- Asesorar y prestar asistencia técnica a la Dirección de Gestión Humana en la preparación de los manuales de funciones y determinación de los perfiles de cargos.
- Conceptuar desde el punto de vista de impacto financiero y de recursos de apoyo, previo estudio y análisis de las dependencias correspondientes, sobre el diseño y la planificación de nuevos proyectos.
- Conceptuar sobre las implicaciones en recursos humanos, físicos y equipos requeridos, ocasionadas por cambios o modificaciones en los proyectos.
- Asesorar a las dependencias administrativas en la elaboración de documentos requeridos para la compra de equipos y licencias de funcionamiento, y suministrar la información requerida.

- Analizar responsabilidades del área organizaciones ligados a los procesos de gestión de la seguridad, estos agentes serán los que deberán gestionar los controles y monitores de las actividades que se realicen en el área
- Monitorear las políticas de control con el objetivo de tener servicios estables mitigando brechas abiertas por las cuales se pueden tener un desbordamiento de la seguridad, minimizando algún tipo de ataques.

Dirección de Investigación:

Responsabilidad:

- Fortalecer la investigación, la innovación y la creación de procesos.
- Fomentar la actividad de la Investigación en la empresa para creación de I+D+I.
- Analizar responsabilidades del área organizaciones ligadas a los procesos de gestión de la seguridad, estos agentes serán los que deberán gestionar los controles y monitores de las actividades que se realicen en el área
- Monitorear las políticas de control con el objetivo de tener servicios estables mitigando brechas abiertas por las cuales se pueden tener un desbordamiento de la seguridad, minimizando algún tipo de ataques.

Área de Dirección de Servicios Administrativos

Responsabilidad:

- Planear, programar, organizar, dirigir y controlar las actividades administrativas de contratación de bienes y servicios de la organización que permitan el óptimo funcionamiento de estos, con base en las políticas, objetivos, pautas y directrices internas de la empresa.
- Autorizar la elaboración de las pólizas de los equipos y materiales que la empresa adquiere, así como la exigibilidad de esta en caso de algún daño, en coordinación con la Oficina Jurídica.
- Propender por el buen manejo y control de los activos fijos de la institución. Realizar oportunamente la activación y actualización de movimientos de activos.

Anexos

- Planear y entregar oportunamente los requerimientos de los usuarios garantizando la preservación del producto y una adecuada prestación del servicio.
- Autorizar el cambio de empresa de vigilancia para garantizar la seguridad dentro de la organización.
- Coordinar y supervisar los gastos de la empresa e igualmente controlar el consumo en materia de eventos que se realicen.
- Autorizar las importaciones de bienes y servicios que la empresa requiera para su óptimo funcionamiento.
- Coordinar y supervisar el proceso de negociación con el exterior para la importación de bienes y servicios que se adquieran.
- Autorizar la ejecución de los Proyectos de Gestión Documental organizacional y los procedimientos para la prestación de los servicios de esta área.

Área de Dirección Financiera

***Responsabilidad**:*

- Administrar financieramente los recursos buscando la sostenibilidad económica de la institución en el corto plazo y su viabilidad en el largo plazo mediante un esquema de gestión eficiente y dinámico, orientado a brindar apoyo oportuno al que hacer organizacional
- Analizar y hacer las recomendaciones sobre los diferentes informes financieros que realizan las dependencias adscritas a la dirección y poder tomar decisiones pertinentes en cada caso.
- Planear y trabajar coordinadamente con las diferentes dependencias adscritas a la Dirección Financiera apoyándolos en las actividades inherentes a ellas mismas para obtener una mayor productividad en el logro de los objetivos propuestos conducentes al cumplimiento de los objetivos estratégicos.
- Apoyar y asesorar al área tecnológica en lo relacionado con trámites administrativos y financieros coadyuvando al cumplimiento de las funciones sustantivas de la organización

Anexos

- Coordinar con las diferentes Instituciones financieras el proceso de recaudo de pagos y otros ingresos de la organización para obtener una mayor efectividad en cada uno de dichos procesos.
- Colaborar activamente en el proceso de presupuestario anual de la Institución por medio de ideas, estrategias y sugerencias y así lograr en equipo un trabajo eficiente y eficaz en la elaboración de dicho presupuesto.

Área Gestión Humana

Responsabilidad:

- Diseñar, desarrollar, implementar, hacer seguimiento y controlar las políticas, planes, programas y procedimientos liderados por el área, promoviendo una eficaz y eficiente gestión del talento humano, a través de la planificación, dirección y control de los procesos y de la administración de adecuadas relaciones entre los trabajadores y la organización.
- Coordinar y supervisar que las actividades de las diferentes secciones de la Dirección de Gestión Humana se lleven a cabo de manera ágil, oportuna y efectiva.
- Ejercer supervisión y control permanente sobre el cumplimiento del reglamento interno de trabajo.
- Supervisar la ejecución de las políticas institucionales de selección, contratación, pagos, afiliación, capacitación, evaluación y salud ocupacional.

Área de diseño y desarrollo:

Responsabilidad:

- Establecer los lineamientos necesarios para el proceso de diseños de los aplicativos y servicios que la organización ofrece, teniendo Innovación Tecnológica a través de sus desarrollos
- Revisar, aprobar y tramitar ante la Sección de Presupuesto los traslados presupuestales necesarios para el normal desarrollo de los servicios para los usuarios.

Anexos

- Dar soporte a los aplicativos y hacer seguimiento al desarrollo de estos y preparar los respectivos informes de los procesos.
- Monitorear los procesos de las aplicaciones en las aplicaciones para asegurar el cumplimiento de las metas presupuestales que conlleven a la sostenibilidad financiera de la organización.

Área de informática.

Responsabilidad:

- Responder por la planeación, adquisición, actualización, implementación, operación y calidad de la infraestructura, procesos y productos relacionados con la tecnología informática y de comunicaciones; cuidando que las inversiones requeridas signifiquen un menor costo y un mayor beneficio organización.
- Participar, junto con las áreas Administrativas y Financieras, en la definición de políticas de desarrollo y seguridad en el área de informática y comunicaciones.
- Definir planes e implementar mediciones para el aseguramiento de la calidad de los productos, servicios y procesos de la Gestión de Tecnología Informática y de Comunicaciones.
- Evaluar y aprobar la adopción de nuevas tecnologías, marcos de referencia y mejores prácticas relacionadas con la implementación, operación y soporte de los servicios de tecnología informática y de comunicaciones.

Anexos

5.2 Anexo B Inventarío De Documentación Requerida Para Cada Dominio

Política de Seguridad: Documentos que especifican como se puede acceder a los datos y quien puede acceder a ellos, sus restricciones y comportamientos.

- Documento que de tareas dé cada empleado de la organización
- Documento de información para el acceso a la información organizacional (Bases de datos, adquisición de equipos, reportes de investigaciones)
- Documento de acceso a información importante de cada departamento
- Documento sobre la codificación de la documentación, organización en cada área departamento institucional.
- Documento de transporte de la documentación hasta las instalaciones de destrucción.
- Documento de destrucción de la documentación ya no necesaria
- Documento que certifica la destrucción al área de gestión
- Documento de seguridad de la información (Políticas de seguridad, donde todo el personal conozcan sobre la seguridad de la información y las consecuencias del mal uso de estas)
- Documento de control Calidad del riesgo
- Documento de control sobre evaluación del riesgo
- Actas de evaluaciones por cada problemática de riesgo
- Documento que determine las soluciones a corto y largo plazo
- Documento que determine el grupo o área encargada de la protección inmediata de la información.
- Documento de soluciones
- Documento Bitácora del proceso de evaluación de riegos
- Documento de control sobre categorías de riesgos

Anexos

Organización de la seguridad de la información: Establece un modelo de gobierno para la seguridad de la información para la organización.

- Documento que de roles dé cada empleado
- Documento que oriente las acciones que se deben tomar en una filtración de información
- Documento de la organización de gestión documental
- Digitalización de los documentos e información
- Documentación de las normas de archivo
- Documento sobre la organización del archivo, por roles y tareas del equipo encargado
- Documento de cómo se deberá guarda los archivos en los servidores de backup
- Documento sobre auditorias y seguridad de información en la organización

Seguridad De Los Recursos Humanos: El objetivo del presente dominio es la necesidad de educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de actividad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. Es necesario reducir los riesgos de error humano, comisión de actos ilícitos, uso inadecuado de instalaciones y recursos y manejo no autorizado de la Información, junto a la definición de posibles sanciones que se aplicarán en caso de incumplimiento.

- Documento Gestión del Recurso Humano
- Documento descripción básica de la interrelación de procesos
- Documento Selección de Personal
- Documento Contrato de Trabajo
- Documento Apertura De Convocatorias
- Documento convocatoria externa
- Documento Pruebas De Tendencias
- Actualización De Datos
- Acta Gestión de las Retribuciones y Cotizaciones del Personal

Anexos

- Documento Vigilancia de la Salud
- Documento Seguimiento de Accidentes de Trabajo

Gestión de activos: Es un inventario y esquema de clasificación para los bienes de información.

- Documentar los bienes organizacionales
- Documentar los equipos de la organización
- Documentar la sistemas de información
- Documento sobre Consultoría de aplicaciones informáticas y suministro de programas informáticos
- Documento sobre Mantenimiento y reparación maquinaria oficina e informática
- Documento sobre la infraestructuras tecnológicas de las universidad
- Documento sobre los protocolos de seguridad en los equipos y sistemas de la organización

Control de acceso: La actividad de control de accesos con autenticación, esta última tiene por misión identificar que verdaderamente “sea, quien dice ser”. El control de acceso es posterior a la autenticación y debe regular que el usuario autenticado, acceda únicamente a los recursos sobre los cuales tenga derecho y a ningún otro.

- Requerimientos de negocio para el control de accesos
- documento Administración de accesos de usuarios
- Acta Gestión de redes.
- Acta Controles de red.
- Acta Responsabilidades de usuarios
- documento Control de acceso a información y aplicaciones
- Seguridad en los servicios de red.
- Utilización y seguridad de los soportes de información.
- Gestión de soportes extraíbles.
- Acta reporte de soportes de acceso

Anexos

- Acta Procedimientos de utilización de acceso de la información.
- Seguridad acceso de la documentación de sistemas.

Criptografía: Ofrece las políticas de seguridad criptográficos y conexiones seguras a los servicios utilizando llaves.

- Solicitud de permisos de usuario
- Requerimiento de licencias
- Documentos de políticas de criptografía

Seguridad Física y del Entorno: Podemos definir como área segura aquel sitio donde se maneja información sensible o valiosos equipos informáticos, es decir, refugios con los que alcanzar los objetivos de la organización.

Dentro del contexto de la seguridad física, debemos entender el concepto “sitio” como edificio, habitación u oficina donde se albergan cada uno de los servicios o instalaciones.

- Documento de Perímetro y fronteras
- Documento Salidas y entradas seguras
- Documento físico y ambiental
- Documento de Controles de Seguridad del Ambiente
- Acta Valor de los Activos de la Información
- Acta Registro de activos de Información
- Documento Seguridad del Cableado Estructurado y Transmisión de Datos
- certificado Aplicación de Controles de Seguridad Ambiental sobre Activos
- Acta Establecimiento de normas y requisitos para la utilizar recursos ambiental

Seguridad de las Operaciones: Tiene como objetivo asegurar la correcta y segura operación de la información, comprende cuatro controles. Hace hincapié en documentar todos los procedimientos, manteniendo los mismos y disponibles a todos los usuarios que los necesiten, segregando adecuadamente los servicios y las responsabilidades para evitar uso inadecuado de los mismos.

Anexos

Procedimientos y responsabilidades de operación.

- Documentación de procedimientos operativo
- Control de cambios operacionales.
- Segregación de tareas.
- Separación de los recursos para desarrollo y producción.
- Acta Supervisión de los servicios contratados a terceros.
- Documento Planificación y aceptación del sistema.
- Documento Medidas y controles contra software malicioso.
- Gestión interna de soportes y recuperación.

Seguridad de Las Comunicaciones: Tiene como objetivo asegurar la correcta y segura operación de la información, en las redes de comunicaciones, donde se deberá tener control de las conexiones internas y externas, transmisión de datos y configuración de servicios de red.

- Documento de protección de información por cada rol de la organización
- Recuperación de la información, comunicaciones y operaciones
- certificado Planificación de capacidades
- Documento Validación de la Información
- Requerimientos de negocio para el control de accesos
- documento Administración de accesos de usuarios
- Acta Gestión de redes.
- Acta Controles de red.
- Acta Responsabilidades de usuarios
- documento Control de acceso a información y aplicaciones
- Seguridad en los servicios de red.
- Seguridad acceso de la documentación de sistemas.

Anexos

Adquisición, desarrollo y mantenimiento de los sistemas de información: Describe la integración de la seguridad a las aplicaciones.

- Inventario existencia de equipos en bodegas
- Inventario existencia de equipos en oficinas y aulas
- Requerimiento de compra de Hardware/software
- Protocolo de egresos e ingresos de hardware y software
- Manual de pruebas de recursos nuevos
- Plantilla de informe estado de los equipos
- Informe de mantenimiento de hardware y software
- Requerimiento de licencias
- Requerimiento instalación/desinstalación de software
- Solicitud de permisos de usuario

Relación con Proveedores: Describe los procesos de seguridad con terceros externos de organización, dende su enfoque está en los permisos y accesos a los sistemas, también la adquisición de servicios o equipos.

- Plantilla de cotización a proveedores
- Informe de compra de los equipos
- Informe de entrega e implementación de recursos
- Manual de compra de recursos nuevos
- Inventario de proveedores
- Manual para la creación del incidente de agentes externos
- Manual de conexión a servicios internos
- Plantilla protocolo de reporte
- Plantilla protocolo de avance
- Plantilla protocolo de cierre

Gestión de incidentes de seguridad de la información: Describe como anticipar y responder a las brechas de seguridad de la información.

Anexos

- Manual para la creación del incidente
- Guía para la clasificación del incidente
- Plantilla protocolo de reporte
- Plantilla protocolo de avance
- Plantilla protocolo de cierre
- Manual para consultar estado del incidente
- Formulario evaluativo ingreso-cierre del incidente
- Guía para el diseño de informe final del incidente
- Plantilla informe final de la incidencia
- Informe total de ingresos

Aspectos de seguridad de la información de la gestión continuidad de negocios: Describe la protección, mantenimiento y recuperación de procesos y sistemas críticos para los negocios.

- Acta de conformación del comité de riesgos
- Localización de la oficina de riesgos
- Plan de acción para la continuidad del negocio
- Documento de aprobación
- Documento de categorización del impacto del negocio
- Informe de análisis de los objetivos y alcance del negocio
- Acta de control y entrega de rendición de cuentas

Cumplimiento: Describe el proceso de asegurar conformidad con las regulaciones, los estándares y las políticas de seguridad de la información.

- Informe de cumplimiento de la norma de protección de la información
- Documento de verificación y cumplimiento de la ley 1581
- Informe auditorias institucionales
- Documento de toma de medidas pedagógicas y sancionatorias
- Documento de toma acciones correctiva.

Anexos

5.3 Anexo C Controles de seguridad de la información asociados a las amenazas

No de Control	Objetivo de control	Controles ISO 27001	Riesgos
A.5	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**		
A.5.1	**Orientación de la dirección para la gestión de la seguridad de la información**		
A.5.1.1	Políticas para la seguridad de la información	Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y las partes externas pertinentes.	•Acceso físico no autorizado/indebido, afecte el activo • Ataque informático de tipo SQL injection • Ataque informático de tipo DoS/DDoS • Ataque informático de tipo buffer overflow • Ataque informático de tipo Ingeniería social • Ataque informático de tipo tcp syn attack • Ataque informático de tipo The mar in the middle • Ataque informático de tipo spam • Ataque informático de tipo scanning • Ataque informático de tipo PASSWORD CRAKING • Ataque informático de tipo Exploit
A.5.1.2	Revisión de las políticas para la seguridad de la información	Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	
A.6			
A.6.1	**Organización interna**		

Anexos

A.6.1.1	Roles y responsabilidades para la seguridad de la información	Se debe definir y asignar todas las responsabilidades de la seguridad de la información.	• Acceso físico no autorizado/indebido, afecte el activo • Ataque informático de tipo SQL injection • Ataque informático de tipo DoS/DDoS • Ataque informático de tipo buffer overflow • Ataque informático de tipo Ingeniería social • Ataque informático de tipo tcp syn attack • Ataque informático de tipo The mar in the middle • Ataque informático de tipo spam • Ataque informático de tipo scanning • Ataque informático de tipo PASSWORD CRAKING • Ataque informático de tipo Exploit
A.6.1.2	Separación de deberes	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.	
A.6.1.3	Contacto con las autoridades	Se deben tener contactos apropiados con las autoridades pertinentes	
A.6.1.4	Contacto con grupos de interés especial	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	
A.6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	
A.6.2	**Dispositivos Móviles y teletrabajo**		
A.6.2.1	Política para dispositivos móviles	Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	• Acceso físico no autorizado/indebido, afecte el activo • Ataque informático de tipo SQL injection • Ataque informático de tipo

Anexos

A.6.2.2	Teletrabajo	Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	DoS/DDoS • Ataque informático de tipo buffer overflow • Ataque informático de tipo Ingeniería social • Ataque informático de tipo tcp syn attack • Ataque informático de tipo The mar in the middle • Ataque informático de tipo spam • Ataque informático de tipo scanning • Ataque informático de tipo PASSWORD CRAKING • Ataque informático de tipo Exploit
A.8.2	**Clasificación de la información**		
A.8.2.1	Clasificación de la información	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o modificación no autorizada.	• Acceso físico no autorizado/indebido, afecte el activo • Ataque informático de tipo SQL injection • Ataque informático de tipo DoS/DDoS • Ataque informático de tipo buffer overflow • Ataque informático de tipo Ingeniería social • Ataque informático de tipo tcp syn attack • Ataque informático de tipo The mar in the middle • Ataque informático de tipo spam
A.8.2.2	Etiquetado de la información	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con e esquema de clasificación de la información adoptado por la organización.	
A.8.2.3	Manejo de activos	Se deben desarrollar e implementar procedimientos para el manejo de activos de acuerdo con el esquema	

		de clasificación de información adoptado por la organización.	• Ataque informático de tipo scanning • Ataque informático de tipo PASSWORD CRAKING • Ataque informático de tipo Exploit
A.8.3	**Manejo de medios**		
A.8.3.1	Gestión de medios removibles	Se deben implementar procedimientos para la gestión de medios removibles de acuerdo con el esquema de clasificación adoptado por la organización.	
A.8.3.2	Disposición de los medios	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	
A.8.3.3	Transferencia de medios físicos	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	
A.9	**CONTROL DE ACCESOS**		
A.9.1	**Requisitos del negocio para control de accesos**		
A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	• Acceso físico no autorizado/indebido, afecte el activo • Ataque informático de tipo SQL injection • Ataque informático de tipo DoS/DDoS • Ataque informático de tipo buffer overflow • Ataque informático de tipo
A.9.1.2	Acceso a redes y a servicios en red	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	

Anexos

			Ingeniería social • Ataque informático de tipo tcp syn attack • Ataque informático de tipo The mar in the middle • Ataque informático de tipo spam • Ataque informático de tipo scanning • Ataque informático de tipo PASSWORD CRAKING • Ataque informático de tipo Exploit
A.9.2	**Gestión de acceso de usuarios**		
A.9.2.1	Registro y cancelación del registro de usuario	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	
A.9.2.2	Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	
A.9.2.3	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	
A.9.2.4	Gestión de información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	

Anexos

A.9.2.5	Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	
A.9.2.6	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	
A.9.3	**Responsabilidades de los usuarios**		
A.9.3.1	Uso de información de autenticación secreta	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	• Acceso físico no autorizado/indebido, afecte el activo • Ataque informático de tipo SQL injection • Ataque informático de tipo DoS/DDoS • Ataque informático de tipo buffer overflow • Ataque informático de tipo Ingeniería social • Ataque informático de tipo tcp syn attack • Ataque informático de tipo The mar in the middle • Ataque informático de tipo spam • Ataque informático de tipo scanning • Ataque informático de tipo

Anexos

			PASSWORD CRAKING • Ataque informático de tipo Exploit
A.9.4	**Control de acceso a sistemas y aplicaciones**		
A.9.4.1	Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	• Acceso físico no autorizado/indebido, afecte el activo • Ataque informático de tipo SQL injection • Ataque informático de tipo DoS/DDoS • Ataque informático de tipo buffer overflow • Ataque informático de tipo Ingeniería social • Ataque informático de tipo tcp syn attack • Ataque informático de tipo The mar in the middle • Ataque informático de tipo spam • Ataque informático de tipo scanning • Ataque informático de tipo PASSWORD CRAKING • Ataque informático de tipo Exploit
A.9.4.2	Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	
A.9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	
A.9.4.4	Uso de programas utilitarios privilegiados	Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	
A.9.4.5	Control de acceso a códigos fuente de programas	Se debe registrar el acceso a los códigos fuente de los programas.	
A.10	**CRIPTOGRAFIA**		
A.10.1	**Controles criptográficos**		
A.10.1.1	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de	• Acceso físico no autorizado/indebido, afecte el activo • Ataque informático de tipo SQL

		controles criptográficos para la protección de la información.	injection • Ataque informático de tipo DoS/DDoS • Ataque informático de tipo buffer overflow • Ataque informático de tipo Ingeniería social • Ataque informático de tipo tcp syn attack • Ataque informático de tipo The mar in the middle • Ataque informático de tipo spam • Ataque informático de tipo scanning • Ataque informático de tipo PASSWORD CRAKING • Ataque informático de tipo Exploit
A.10.1.2	Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante su ciclo de vida.	
A.11	**SEGURIDAD FÍSICA Y DEL ENTORNO**		
A.11.1	**Áreas seguras**		
A.11.1.1	Perímetro de seguridad física	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	• Acceso físico no autorizado/indebido, afecte el activo • Ataque informático de tipo SQL injection • Ataque informático de tipo DoS/DDoS • Ataque informático de tipo buffer overflow • Ataque informático de tipo Ingeniería social • Ataque informático de tipo tcp syn attack
A.11.1.2	Control de accesos físicos	Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite acceso a personal autorizado.	
A.11.1.3			

Anexos

	Seguridad de oficinas, recintos e instalacione	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	• Ataque informático de tipo The mar in the middle • Ataque informático de tipo spam • Ataque informático de tipo scanning • Ataque informático de tipo PASSWORD CRAKING • Ataque informático de tipo Exploit
A.11.1.4	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	
A.11.1.5	Trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	
A.11.1.6	Áreas de despacho y carga	Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	
A.11.2	**Equipos**		
A.11.2.1	Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	
A.11.2.2	Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras	

Anexos

		interrupciones causadas por fallas en los servicios de suministro.	
A.11.2.3	Seguridad del cableado	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	
A.11.2.4	Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	
A.11.2.5	Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	
A.11.2.6	Seguridad de activos y equipos fuera de la oficina	Se deben aplicar medidas de seguridad a los activos que se encuentran instalaciones fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	
A.11.2.7	Disposición segura o reutilización de equipos	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma	

		segura antes de su disposición o reusó.	
A.11.2.8	Equipos de usuario desatendido	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	
A.11.2.9	Políticas de escritorio y pantalla limpios	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	
A.12	**SEGURIDAD DE LAS OPERACIONES**		
A.12.1	**Procedimientos operacionales y responsabilidades**		
A.12.1.1	Procedimientos de operación documentados	Los procedimientos de operació se deben documentar y poner a disposición de todos los usuarios que los necesitan.	
A.12.1.2	Gestión de cambios	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	
A.12.1.3	Gestión de capacidad	Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	• Acceso físico no autorizado/indebido, afecte el activo • Ataque informático de tipo SQL injection • Ataque informático de tipo DoS/DDoS • Ataque informático de tipo buffer
A.12.1.4	Separación de los ambientes de	Se deben separar los ambientes de desarrollo, prueba y operación, para	

	desarrollo, pruebas, y operación	reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	overflow • Ataque informático de tipo Ingeniería social • Ataque informático de tipo tcp syn attack • Ataque informático de tipo The mar in the middle • Ataque informático de tipo spam • Ataque informático de tipo scanning • Ataque informático de tipo PASSWORD CRAKING • Ataque informático de tipo Exploit
A.12.2	**Protección contra códigos maliciosos**		
A.12.2.1	Controles contra códigos maliciosos	Se deben implementar controles de detección, de prevención y de recuperación combinados con la toma de conciencia apropiada de lo usuarios para proteger contra códigos maliciosos.	
A.12.3	**Proteger contra la perdida de datos**		
A.12.3.1	Respaldo de la información	Se deben hacer copias de respaldo de información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	• Acceso físico no autorizado/indebido, afecte el activo • Ataque informático de tipo SQL injection • Ataque informático de tipo DoS/DDoS • Ataque informático de tipo buffer overflow • Ataque informático de tipo Ingeniería social

Anexos

			• Ataque informático de tipo tcp syn attack • Ataque informático de tipo The mar in the middle • Ataque informático de tipo spam • Ataque informático de tipo scanning • Ataque informático de tipo PASSWORD CRAKING • Ataque informático de tipo Exploit
A.12.4	**Registro y seguimiento**		
A.12.4.1	Registro de eventos	Se deben elaborar, conservar y revisar regularmente los registros a cerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información	• Acceso físico no autorizado/indebido, afecte el activo • Ataque informático de tipo SQL injection • Ataque informático de tipo DoS/DDoS • Ataque informático de tipo buffer overflow • Ataque informático de tipo Ingeniería social • Ataque informático de tipo tcp syn attack • Ataque informático de tipo The mar in the middle • Ataque informático de tipo spam • Ataque informático de tipo scanning • Ataque informático de tipo PASSWORD CRAKING • Ataque informático de tipo Exploit
A.12.4.2	Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado	
A.12.4.3	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	

Anexos

A.12.4.4	Sincronización de reloj	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	
A.12.5	**Control de software operacional**		
A.12.5.1	Instalación de software en sistemas operativos	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	
A.12.6	**Gestión de la vulnerabilidad técnica**		
A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	• Acceso físico no autorizado/indebido, afecte el activo • Ataque informático de tipo SQL injection • Ataque informático de tipo DoS/DDoS • Ataque informático de tipo buffer overflow • Ataque informático de tipo Ingeniería social • Ataque informático de tipo tcp syn attack • Ataque informático de tipo The mar in the middle • Ataque informático de tipo spam • Ataque informático de tipo scanning
A.12.6.2	Restricciones sobre la instalación de software	Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	

Anexos

			• Ataque informático de tipo PASSWORD CRAKING • Ataque informático de tipo Exploit
A.12.7	**Consideraciones sobre auditorías de sistemas de información**		
A.12.7.1	Controles de auditorías de sistemas de información	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	
A.13	**SEGURIDAD DE LAS COMUNICACIONES**		
A.13.1	**Gestión de la seguridad de las redes**		
A.13.1.1	Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	• Acceso físico no autorizado/indebido, afecte el activo • Ataque informático de tipo SQL injection • Ataque informático de tipo DoS/DDoS • Ataque informático de tipo buffer overflow • Ataque informático de tipo Ingeniería social • Ataque informático de tipo tcp syn attack • Ataque informático de tipo The mar in the middle
A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	

Anexos

			• Ataque informático de tipo spam • Ataque informático de tipo scanning • Ataque informático de tipo PASSWORD CRAKING • Ataque informático de tipo Exploit
A.13.1.3	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	
A.13.2	**Transferencia de información**		
A.13.2.1	Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	• Acceso físico no autorizado/indebido, afecte el activo • Ataque informático de tipo SQL injection • Ataque informático de tipo DoS/DDoS • Ataque informático de tipo buffer overflow • Ataque informático de tipo Ingeniería social • Ataque informático de tipo tcp syn attack • Ataque informático de tipo The man in the middle • Ataque informático de tipo spam • Ataque informático de tipo scanning • Ataque informático de tipo PASSWORD CRAKING • Ataque informático de tipo Exploit
A.13.2.2	Acuerdos sobre transferencia de información	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	

Anexos

A.13.2.3	Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**		
A.14.1	**Requisitos de seguridad de los sistemas de información**		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	• Acceso físico no autorizado/indebido, afecte el activo • Ataque informático de tipo SQL injection • Ataque informático de tipo DoS/DDoS • Ataque informático de tipo buffer overflow • Ataque informático de tipo Ingeniería social • Ataque informático de tipo tcp syn attack • Ataque informático de tipo The mar in the middle • Ataque informático de tipo spam • Ataque informático de tipo scanning • Ataque informático de tipo
A.14.1.2	Seguridad de servicio de las aplicaciones en redes publicas	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado la alteración	

Anexos

		no autorizada de mensajes, la divulgación no autorizada y la divulgación o reproducción de mensajes no autorizados.	PASSWORD CRAKING • Ataque informático de tipo Exploit
A.14.2	**Seguridad en los procesos de desarrollo y soporte**		
A.14.2.1	Políticas de desarrollo seguro	Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	• Acceso físico no autorizado/indebido, afecte el activo • Ataque informático de tipo SQL injection • Ataque informático de tipo DoS/DDoS • Ataque informático de tipo buffer overflow • Ataque informático de tipo Ingeniería social • Ataque informático de tipo tcp syn attack • Ataque informático de tipo The mar in the middle • Ataque informático de tipo spam • Ataque informático de tipo scanning • Ataque informático de tipo PASSWORD CRAKING • Ataque informático de tipo Exploit
A.14.2.2	Procedimiento de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	
A.14.2.4	Restricción en los cambios a los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	

Anexos

A.14.2.5	Principios de construcción de los sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	
A.14.2.6	Ambiente seguro de desarrollo	Las organizaciones deben establece y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	
A.14.2.7	Desarrollo externamente contratado	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	
A.14.2.8	Pruebas de seguridad de sistemas	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	
A.14.2.9	Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	
A.14.3	**Datos de pruebas**		

Anexos

A.14.3.1	Protección de datos de pruebas	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	• Acceso físico no autorizado/indebido, afecte el activo • Ataque informático de tipo SQL injection • Ataque informático de tipo DoS/DDoS • Ataque informático de tipo buffer overflow • Ataque informático de tipo Ingeniería social • Ataque informático de tipo tcp syn attack • Ataque informático de tipo The mar in the middle • Ataque informático de tipo spam • Ataque informático de tipo scanning • Ataque informático de tipo PASSWORD CRAKING • Ataque informático de tipo Exploit
A.15	**RELACIONES CON LOS PROVEEDORES**		
A.15.1	**Seguridad de la información en las relaciones con los proveedores**		
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar.	
A.15.1.2	Tratamiento de la seguridad dentro de	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada	

	los acuerdos con proveedores	proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	
A.15.2	**Gestión de la prestación de servicios de proveedores**		
A.15.2.1	Seguimiento y revisión a los servicios proveedores	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	
A.15.2.2	Gestión de cambios en los servicios de los proveedores	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.	
A.16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**		
A.16.1	**Gestión de incidentes y mejoras en la seguridad de la información**		

Anexos

A.16.1.1	Responsabilidades y procedimientos	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	• Acceso físico no autorizado/indebido, afecte el activo • Ataque informático de tipo SQL injection • Ataque informático de tipo DoS/DDoS • Ataque informático de tipo buffer overflow • Ataque informático de tipo Ingeniería social • Ataque informático de tipo tcp syn attack • Ataque informático de tipo The mar in the middle • Ataque informático de tipo spam • Ataque informático de tipo scanning • Ataque informático de tipo PASSWORD CRAKING • Ataque informático de tipo Exploit
A.16.1.2	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	
A.16.1.3	Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad de la información se deben evaluar y se debe decir si se van a clasificar como incidentes de seguridad de la información.	
A.16.1.5	Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	

Anexos

A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	
A.16.1.7	Recolección de evidencia	La organización debe definir y aplica procedimientos para la identificación, recolección adquisición y preservación de la información que puede servir como evidencia.	
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO**		
A.17.1	**Continuidad de seguridad de la información**		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debe determinar sus requisitos para la seguridad de la y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres.	• Acceso físico no autorizado/indebido, afecte el activo • Ataque informático de tipo SQL injection • Ataque informático de tipo DoS/DDoS • Ataque informático de tipo buffer overflow • Ataque informático de tipo Ingeniería social • Ataque informático de tipo tcp syn attack • Ataque informático de tipo The mar in the middle • Ataque informático de tipo spam • Ataque informático de tipo scanning • Ataque informático de tipo
A.17.1.2	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e	

Anexos

	seguridad de la información	implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	PASSWORD CRAKING • Ataque informático de tipo Exploit
A.17.2	**Redundancia**		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	
A.18	**CUMPLIMIENTO**		
A.18.1	**Cumplimiento de requisitos legales y contractuales**		
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización.	
A.18.1.2	Derechos de propiedad intelectual	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	• Acceso físico no autorizado/indebido, afecte el activo • Ataque informático de tipo SQL injection • Ataque informático de tipo DoS/DDoS • Ataque informático de tipo buffer overflow • Ataque informático de tipo Ingeniería social
A.18.1.3	Protección de registros	Los registros se deben proteger contra pérdida, destrucción,	

Anexos

		falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	• Ataque informático de tipo tcp syn attack • Ataque informático de tipo The mar in the middle • Ataque informático de tipo spam • Ataque informático de tipo scanning • Ataque informático de tipo PASSWORD CRAKING • Ataque informático de tipo Exploit
A.18.1.4	Privacidad y protección de información de datos personales	Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	
A.18.1.5	Reglamentación de controles criptográficos	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	
A.18.2	**Revisiones de seguridad de la información**		
A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (e decir, los objetivos de control, lo controles, las políticas, los proceso y los procedimientos para seguridad de la información) se deben revisa independientemente a intervalo planificados o cuando ocurra cambios significativos.	• Acceso físico no autorizado/indebido, afecte el activo • Ataque informático de tipo SQL injection • Ataque informático de tipo DoS/DDoS • Ataque informático de tipo buffer overflow • Ataque informático de tipo Ingeniería social
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Los directores deben revisar cor regularidad el cumplimiento de procesamiento y procedimientos de información dentro de su área de	• Ataque informático de tipo tcp syn attack • Ataque informático de tipo The mar in the middle

		responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	• Ataque informático de tipo spam • Ataque informático de tipo scanning • Ataque informático de tipo PASSWORD CRAKING • Ataque informático de tipo Exploit
A.18.2.3	Revisión de cumplimiento técnico	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con la políticas y normas de seguridad de la información.	

Tabla 13 Controles de seguridad de la información asociados a las amenazas - Fuente propia [25]

5.4 Anexo D Plan de Tratamiento

No del Control	Objetivo de control	Plan de Tratamiento Propuesto para los Controles de la ISO 27001
A.5	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	
A.5.1	**Orientación de la dirección para la gestión de la seguridad de la información**	
A.5.1.1	Políticas para la seguridad de la información	•Desarrollar un conjunto de políticas ligado a la protección de los sistemas BCI, utilizando un marco de referencia. •Verificar la eficacia de los controles del plan de tratamiento
A.5.1.2	Revisión de las políticas para la seguridad de la información	•Identificar posibles fallos de las medidas implementadas en el plan de tratamiento. •Auditar el modelo de seguridad del sistema BCI
A.6.1	**Organización interna**	
A.6.1.1	Roles y responsabilidades para la seguridad de la información	•Definir roles en los actores que hacen parte en los procesos de gestión e interacción de los sistemas BCI •Determinar las responsabilidades para la protección del sistema BCI

Anexos

		•Auditar la valides de las responsabilidades diseñadas en el plan de tratamiento
A.6.1.2	Separación de deberes	•Determinar protocolos de exclusión para el uso de los diferentes servicios del sistema BCI •Establecer permisos necesarios sobre las aplicaciones y sistemas de información caracterizado por roles, donde se minimice posibles fallos de uso •Comprobar la efectividad de los permisos en los servicios de los aplicativos que hacen parte de las diferentes etapas del sistema BCI
A.6.1.3	Contacto con las autoridades	Consolidar líneas de comunicación con los diferentes organismos gubernamentales de protección de la información •Generar espacios de comunicación por medio de eventos donde se compartan lineamientos y protocolos de seguridad informática
A.6.1.4	Contacto con grupos de interés especial	•Ingresar a grupos ligados a la presentación de delitos cibernéticos para la prevención de delitos de seguridad informática •Buscar alianzas con actores de desarrollo de sistemas BCI, donde se compartan experiencias de seguridad informática •Comunicación directa con los grupos de respuestas de incidentes de seguridad SOC y CERT
A.6.1.5	Seguridad de la información en la gestión de proyectos	•Formular objetivos medibles para la gestión de la seguridad información en los sistemas BCI •Realizar un mapa de gestión de riesgos y auditorías a los procesos internos
A.6.2	**Dispositivos Móviles y teletrabajo**	

Anexos

A.6.2.1	Política para dispositivos móviles	•Crear reglas de permisos incide sobre los servicios prestados, donde se registre la IPs públicas de los usuarios y uso de los aplicativos •Definir las configuraciones de los equipos móviles para el ingreso a las plataformas del sistema BCI •Evaluar los mecanismos implementados en los dispositivos móviles donde se valide los niveles de seguridad informática
A.6.2.2	Teletrabajo	•Implementar controles de seguridad para las conexiones remotas de los servicios BCI •Determinar políticas de accesos a los servicios donde se cree conexiones seguras, con control de tiempo en uso de aplicativos. •Auditar las conexiones a los servidores y servicios BCI
A.8	**GESTIÓN DE ACTIVOS**	
A.8.2.1	Clasificación de la información	•Realizar un inventario de activos físico y lógico donde se determine quién es el encargado de la organización, protección de éstos y lugar de donde se guardarán •Diseñar políticas de uso de los diferentes activos de la organización, por medio de documentación y listas de acceso •Mantener control de los activos en su uso, donde se determine que cumplen las políticas de uso de éstos
A.8.2.2	Etiquetado de la información	•Realizar un inventario de activos físico y lógico donde se determine quién es el encargado de la organización, protección de éstos y lugar de donde se guardarán •Diseñar políticas de uso de los diferentes activos de la organización, por medio de documentación y listas de acceso

Anexos

		•Mantener control de los activos en su uso, donde se determine que cumplen las políticas de uso de éstos
A.9	**CONTROL DE ACCESOS**	
A.9.1	**Requisitos del negocio para control de accesos**	
A.9.1.1	Política de control de acceso	•Desarrollar un conjunto de políticas para el uso sobre las redes, aplicaciones y/o sistemas de información •Comprobar la efectividad de los permisos en los servicios de los aplicativos que hacen parte de las diferentes etapas del sistema BCI •Auditar la efectividad de las políticas desarrolladas para el control de acceso de los activos de información
A.9.1.2	Acceso a redes y a servicios en red	•Crear protocolos de registro de empleado que utilizaran los servicios del sistema BCI •Crear protocolos de exclusión de los no empleados de las bases de datos y aplicativos •Definir los accesos a servicios establecidos por roles •Auditar las bases de datos donde se verifiquen el estado de los usuarios y no usuarios del sistema BCI
A.9.2	**Gestión de acceso de usuarios**	
A.9.2.1	Registro y cancelación del registro de usuarios	•Crear protocolos de registro de usuarios que utilizaran los servicios del sistema BCI •Crear protocolos de exclusión de los no usuarios de las bases de datos y aplicativos •Auditar las bases de datos donde se verifiquen el estado de los usuarios y no usuarios del sistema BCI
A.9.2.2	Suministro de acceso de usuarios	•Establecer los permisos necesarios sobre las redes, aplicaciones y/o sistemas de información categorizados por rol •Auditar las bases de datos donde se verifiquen el estado de los usuarios y no usuarios del sistema BCI

Anexos

A.9.2.3	Gestión de derechos de acceso privilegiado	•Establecer los permisos necesarios sobre las redes, aplicaciones y/o sistemas de información categorizados por rol •Auditar las bases de datos donde se verifiquen el estado de los usuarios y no usuarios del sistema BCI
A.9.2.4	Gestión de información de autenticación secreta de usuarios	•Determinar que las contraseñas deben de tener como mínimo 12 caracteres alfanuméricos, sobre las redes, aplicaciones y/o sistemas de información. •Definir los accesos a servicios establecidos por roles •Auditar las bases de datos donde se verifiquen el estado de los usuarios y no usuarios del sistema BCI
A.9.2.5	Revisión de los derechos de acceso de usuarios	•Establecer los permisos necesarios sobre las redes, aplicaciones y/o sistemas de información categorizados por rol •Definir los accesos a servicios establecidos por roles •Auditar las bases de datos donde se verifiquen el estado de los usuarios y no usuarios del sistema BCI
A.9.2.6	Retiro o ajuste de los derechos de acceso	•Crear protocolos de registro de empleado que utilizaran los servicios del sistema BCI •Crear protocolos de exclusión de los no empleados de las bases de datos y aplicativos •Establecer los permisos necesarios sobre las redes, aplicaciones y/o sistemas de información categorizados por rol •Auditar las bases de datos donde se verifiquen el estado de los usuarios y no usuarios del sistema BCI
A.9.3	**Responsabilidades de los usuarios**	

Anexos

A.9.3.1	Uso de información de autenticación secreta	•Capacitar y concientizar a los usuarios regularmente en temas de seguridad de la información, convenientes para realizar sus actividades. •Generar espacios de aprendizaje sobre las políticas de cuidado de los activos de información
A.9.4	**Control de acceso a sistemas y aplicaciones**	
A.9.4.1	Restricción de acceso a la información	•Determinar que las contraseñas deben de tener como mínimo 12 caracteres alfanuméricos, sobre las redes, aplicaciones y/o sistemas de información. •Establecer los permisos necesarios sobre las redes, aplicaciones y/o sistemas de información categorizados por rol •Definir los accesos a perímetros establecidos por roles y dependencias.
A.9.4.2	Procedimiento de ingreso seguro	•Determinar que las contraseñas deben de tener como mínimo 12 caracteres alfanuméricos, sobre las redes, aplicaciones y/o sistemas de información. •Definir los accesos a perímetros establecidos por roles y dependencias.
A.9.4.3	Sistema de gestión de contraseñas	•Determinar que las contraseñas deben de tener como mínimo 12 caracteres alfanuméricos, sobre las redes, aplicaciones y/o sistemas de información. •Definir politicas de cambio de claves cada semana para minimizar posibles casos ligados a ciberseguridad.
A.9.4.4	Uso de programas utilitarios privilegiados	•Definir los accesos a perímetros establecidos por roles y departamentos

Anexos

		•Establecer una política de permisos necesarios sobre la instalación de softwares de terceros en los sistemas BCI •Definir los accesos a perímetros establecidos por role y dependencias. •Establecer políticas de actualización del software donde se minimicen posibles fallos de seguridad por dependencias.
A.9.4.5	Control de acceso a códigos fuente de programas	•Establecer una política de permisos necesarios sobre la instalación de softwares de terceros en los sistemas BCI donde se bloquee código malicioso •Establecer políticas de actualización del software donde se minimicen posibles fallos de seguridad
A.10	**CRIPTOGRAFIA**	
A.10.1	**Controles criptográficos**	
A.10.1.1	Política sobre el uso de controles criptográficos	•Establecer controles en las tablas sensibles con algoritmos de hash •Establecer los permisos necesarios sobre las redes, aplicaciones y/o sistemas de información para las conexiones externas donde el uso de VPN debe ser encriptado extremo a extremo
A.10.1.2	Gestión de llaves	•Establecer controles en las tablas sensibles con algoritmos de hash •Establecer los permisos necesarios sobre las redes, aplicaciones y/o sistemas de información para las conexiones externas donde el uso de VPN debe ser encriptado extremo a extremo •Implementar certificados por control perimetral
A.11	**SEGURIDAD FÍSICA Y DEL ENTORNO**	
A.11.1	**Áreas seguras**	

Anexos

A.11.1.1	Perímetro de seguridad física	•Implementar un sistema de seguridad de gestión de seguridad en el trabajo •Determinar control de Accesos con tarjeta HID y Fingerprint •Implementar un sistemas de seguridad físico con sensores de calor, movimiento y cámaras CCTV
A.11.1.2	Control de accesos físicos	•Implementar un sistema de seguridad de gestión de seguridad en el trabajo •Determinar control de Accesos con tarjeta HID y Fingerprint •Implementar un sistemas de seguridad físico con sensores de calor, movimiento y cámaras CCTV
A.11.1.3	Seguridad de oficinas recintos e instalaciones	•Implementar un sistema de seguridad de gestión de seguridad en el trabajo •Determinar control de Accesos con tarjeta HID y Fingerprint •Implementar un sistemas de seguridad físico con sensores de calor, movimiento y cámaras CCTV
A.12	**SEGURIDAD DE LAS OPERACIONES**	
A.12.1	**Procedimientos operacionales y responsabilidades**	
A.12.1.3	Gestión de capacidad	•Crear ambientes controlados para la implementación de los servicios de prueba de los aplicativos diseñados •Implementar un conjunto de prácticas de desarrollo de software como DevOps, junto a su ciclo de vida de la metodología implementada •Validar el ciclo de vida de las practicas implementadas •Documentar los hallazgos, implementación de cambios y mejoras de los sistemas
A.12.1.4	Separación de los ambientes de	•Crear ambientes controlados para la implementación de los servicios de prueba de los aplicativos diseñados

Anexos

	desarrollo, pruebas, y operación	•Implementar un conjunto de prácticas de desarrollo de software como DevOps, junto a su ciclo de vida de la metodología implementada •Validar el ciclo de vida de las practicas implementadas •Documentar los hallazgos, implementación de cambios y mejoras de los sistemas
A.12.2	**Protección contra códigos maliciosos**	
A.12.2.1	Controles contra códigos maliciosos	•Realizar controles de configuración de software y herramientas lógicas en los diferentes sistemas de la entidad •Diseñar políticas de uso de software donde se determinen las formas de instalación, actualización y control de los aplicativos. •Implementar un pool de herramientas que controlen, gestionen, administren y detecten acciones maliciosas producto de instalación de software en los diferentes equipos.
A.12.3	**Proteger contra la perdida de datos**	
A.12.3.1	Respaldo de la información	•Elaborar controles para el almacenamiento de la información que se van a utilizar, donde se protejan los datos en las aplicativos y servicios donde serán •Elaborar políticas de procedimientos en el almacenamiento de las bases de datos y las características de estos donde la información sensible se guarde de manera idónea. •Implementar infraestructura para realización de back ups de la información
A.12.4	**Registro y seguimiento**	

Anexos

A.12.4.1	Registro de eventos	•Elaborar controles para el almacenamiento de la información que se van a utilizar, donde se protejan los datos en las aplicativos y servicios donde serán •Elaborar políticas de procedimientos en el uso de las bases de datos y servicios de los sistemas, donde la información sensible sea utilizada de manera idónea. •Realizar controles en quien son los usuarios que pueden ingresar, cambiar y usar la información •Monitorear el acceso y uso de los aplicativos donde la información debe ser preservada de manera idónea para su uso sin tener ninguna irregularidad •Formular el uso de software que recoja información de como eventos, logs y trazas en servicios y red •Administrar servicios de recolección y registros de eventos
A.12.4.2	Protección de la información de registro	•Elaborar controles para el almacenamiento de la información que se van a utilizar, donde se protejan los datos en las aplicativos y servicios donde serán •Elaborar políticas de procedimientos en el uso de las bases de datos y servicios de los sistemas, donde la información sensible sea utilizada de manera idónea. •Realizar controles en quien son los usuarios que pueden ingresar, cambiar y usar la información •Monitorear el acceso y uso de los aplicativos donde la información debe ser preservada de manera idónea para su uso sin tener ninguna irregularidad •Formular el uso de software que recoja información de como eventos, logs y trazas en servicios y red •Administrar servicios de recolección y registros de eventos

A.12.4.3	Registros del administrador y del operador	•Elaborar controles para el almacenamiento de la información que se van a utilizar, donde se protejan los datos en las aplicativos y servicios donde serán •Elaborar políticas de procedimientos en el uso de las bases de datos y servicios de los sistemas, donde la información sensible sea utilizada de manera idónea. •Realizar controles en quien son los usuarios que pueden ingresar, cambiar y usar la información •Monitorear el acceso y uso de los aplicativos donde la información debe ser preservada de manera idónea para su uso sin tener ninguna irregularidad •Formular el uso de software que recoja información de como eventos, logs y trazas en servicios y red •Administrar servicios de recolección y registros de eventos
A.12.5	**Control de software operacional**	
A.12.5.1	Instalación de software en sistemas operativos	•Realizar controles de configuración de software y herramientas lógicas en los diferentes sistemas de la entidad •Diseñar políticas de uso de software donde se determinen las formas de instalación, actualización y control de los aplicativos. •Implementar un pool de herramientas que controlen, gestionen, administren y detecten acciones maliciosas producto de instalación de software en los diferentes equipos
A.12.6	**Gestión de la vulnerabilidad técnica**	

Anexos

A.12.6.1	Gestión de las vulnerabilidades técnicas	•Crear comités de control de vulnerabilidades en los sistemas donde la seguridad de la información que verifiquen la efectividad de las políticas y controles establecidos •Desarrollar unas políticas de control de vulnerabilidades tecnológicas •Documentar los hallazgos, implementación de cambios y mejoras de los sistemas relacionadas a las políticas de control de vulnerabilidades •Generar informe de la auditoria de las políticas de control de vulnerabilidades con el objetivo de mejoras a futuro de los procesos y controles establecidos
A.12.6.2	Restricciones sobre la instalación de software	•Realizar controles de configuración de software y herramientas lógicas en los diferentes sistemas de la entidad •Diseñar políticas de uso de software donde se determinen las formas de instalación, actualización y control de los aplicativos. •Implementar un pool de herramientas que controlen, gestionen, administren y detecten acciones maliciosas producto de instalación de software en los diferentes equipos
A.12.7	**Consideraciones sobre auditorías de sistemas de información**	
A.12.7.1	Controles de auditorías de sistemas de información	•Implementar la agenda de auditorías de los sistemas donde se de control a las diferentes actividades que se los diferentes equipos •Documentar los hallazgos, implementación de cambios y mejoras de los sistemas relacionadas a las auditorías internas y externas

Anexos

		•Realizar auditorías por cada uno de los controles desarrollados para la seguridad de la información •Crear comités de revisión de la seguridad de la información que verifiquen la efectividad de las políticas y controles establecidos •Generar informe de la auditoria con el objetivo de mejoras a futuro de los procesos y controles establecidos
A.13	**SEGURIDAD DE LAS COMUNICACIONES**	
A.13.1	**Gestión de la seguridad de las redes**	
A.13.1.1	Controles de redes	•Monitorear el acceso y uso de las redes donde la información debe ser preservada encriptada por medio de segmentación, control de accesos, DMZ, firewall, sandbox y honeypots y segmentación de redes por Vlans, roles y ACL •Administrar servicios de recolección y registros de eventos ligados a las redes
A.13.1.2	Seguridad de los servicios de red	•Monitorear el acceso y uso de las redes donde la información debe ser preservada encriptada por medio de segmentación, control de accesos, DMZ, firewall, sandbox y honeypots y segmentación de redes por Vlans, roles y ACL •Administrar servicios de recolección y registros de eventos ligados a las redes
		•Monitorear el acceso y uso de las redes donde la información debe ser preservada encriptada por medio de segmentación, control de accesos, DMZ, firewall, sandbox y honeypots y segmentación de redes por Vlans, roles y ACL

Anexos

		•Administrar servicios de recolección y registros de eventos ligados a las redes
A.13.2	**Transferencia de información**	
A.13.2.1	Políticas y procedimientos de transferencia de información	•Formular las políticas de transferencia de la información de acuerdo con normas y leyes que reglamentan la propiedad intelectual, la protección de datos personales y el uso de éstas. •Implementar políticas de seguridad de la transferencia de la información dentro y fuera de organización •Mantener control de las políticas de transferencia de información, donde se determine que cumplen las políticas y se documente el estado del control
A.13.2.2	Acuerdos sobre transferencia de información	•Explicar a los empleados y usuarios del uso como se da en la transferencia de la información personal y de la organización dentro y fuera de ésta •Formular las políticas de seguridad en la transferencia de información de acuerdo con normas y leyes que reglamentan la propiedad intelectual, la protección de datos personales y el uso de éstas
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**	
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	•Desarrollar una política de compras de equipos los cuales mejoren la gestión de los activos empresarial para la seguridad de la información •Implementar una lista técnica de requerimientos técnicos donde se evalué las características de hardware y software para un desarrollo de la seguridad •Validar la seguridad informática ligada a la adquisición de nuevo hardware y software.

Anexos

A.14.1.2	Seguridad de servicio de las aplicaciones en redes publicas	•Implementar políticas donde los equipos que se conecten a la red pública deben contar con antivirus. •Implementar un sistema de firewall perimetral •Realizar pruebas técnicas de ataques de software a los servicios que serán expuestos a la red pública donde se puedan diagnosticas posibles casos de seguridad
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	•Establecer controles en las tablas sensibles con algoritmos de hash •Establecer los permisos necesarios sobre las redes, aplicaciones y/o sistemas de información para las conexiones externas donde el uso de VPN debe ser encriptado extremo a extremo •Implementar certificados por control perimetral
A.14.2	**Seguridad en los procesos de desarrollo y soporte**	
A.14.2.1	Políticas de desarrollo seguro	•Implementar un conjunto de prácticas de desarrollo de software como DevOps, junto a su ciclo de vida de la metodología implementada •Implementar un conjunto de prácticas de seguridad como DevSecOps, junto a su ciclo de vida de la metodología implementada •Validar el ciclo de vida de las practicas implementadas •Documentar los hallazgos, implementación de cambios y mejoras de los sistemas
A.14.2.2	Procedimiento de control de cambios en sistemas	•Implementar un conjunto de prácticas de desarrollo de software como DevOps, junto a su ciclo de vida de la metodología implementada •Implementar un conjunto de prácticas de seguridad como DevSecOps, junto a su ciclo de vida de la metodología implementada

Anexos

		•Validar el ciclo de vida de las practicas implementadas •Documentar los hallazgos, implementación de cambios y mejoras de los sistemas
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	•Implementar un conjunto de prácticas de desarrollo de software como DevOps, junto a su ciclo de vida de la metodología implementada •Implementar un conjunto de prácticas de seguridad como DevSecOps, junto a su ciclo de vida de la metodología implementada •Validar el ciclo de vida de las practicas implementadas •Documentar los hallazgos, implementación de cambios y mejoras de los sistemas
A.14.2.4	Restricción en los cambios a los paquetes de software	•Implementar un conjunto de prácticas de desarrollo de software como DevOps, junto a su ciclo de vida de la metodología implementada •Implementar un conjunto de prácticas de seguridad como DevSecOps, junto a su ciclo de vida de la metodología implementada •Validar el ciclo de vida de las practicas implementadas •Documentar los hallazgos, implementación de cambios y mejoras de los sistemas
A.14.2.5	Principios de construcción de los sistemas seguros	•Implementar un conjunto de prácticas de desarrollo de software como DevOps, junto a su ciclo de vida de la metodología implementada •Implementar un conjunto de prácticas de seguridad como DevSecOps, junto a su ciclo de vida de la metodología implementada •Validar el ciclo de vida de las practicas implementadas •Documentar los hallazgos, implementación de cambios y mejoras de los sistemas

Anexos

A.14.2.6	Ambiente seguro de desarrollo	•Implementar un conjunto de prácticas de desarrollo de software como DevOps, junto a su ciclo de vida de la metodología implementada •Implementar un conjunto de prácticas de seguridad como DevSecOps, junto a su ciclo de vida de la metodología implementada •Validar el ciclo de vida de las practicas implementadas •Documentar los hallazgos, implementación de cambios y mejoras de los sistemas
A.14.2.7	Desarrollo externamente contratado	•Implementar un conjunto de prácticas de desarrollo de software como DevOps, junto a su ciclo de vida de la metodología implementada •Implementar un conjunto de prácticas de seguridad como DevSecOps, junto a su ciclo de vida de la metodología implementada •Validar el ciclo de vida de las practicas implementadas •Documentar los hallazgos, implementación de cambios y mejoras de los sistemas
A.14.2.8	Pruebas de seguridad de sistemas	•Implementar un conjunto de prácticas de desarrollo de software como DevOps, junto a su ciclo de vida de la metodología implementada •Implementar un conjunto de prácticas de seguridad como DevSecOps, junto a su ciclo de vida de la metodología implementada •Validar el ciclo de vida de las practicas implementadas •Documentar los hallazgos, implementación de cambios y mejoras de los sistemas
A.14.2.9	Prueba de aceptación de sistemas	•Implementar un conjunto de prácticas de desarrollo de software como DevOps, junto a su ciclo de vida de la metodología implementada

		•Implementar un conjunto de prácticas de seguridad como DevSecOps, junto a su ciclo de vida de la metodología implementada •Validar el ciclo de vida de las practicas implementadas •Documentar los hallazgos, implementación de cambios y mejoras de los sistemas
A.14.3.1	Protección de datos de pruebas	•Elaborar controles de las bases de datos que se van a utilizar, donde se protejan los datos en las aplicativos y servicios donde serán utilizadas •Certificar el origen y permisos de las bases de datos de prueba para no tener conflictos de uso •Elaborar políticas de buen uso de las bases de datos y las características de estos donde la información sensible se protegida de manera idónea.
A.16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**	
A.16.1	**Gestión de incidentes y mejoras en la seguridad de la información**	
A.16.1.1	Responsabilidades y procedimientos	•Diseñar protocolos en caso de posibles intrusiones de seguridad, donde se den soluciones a dichos casos •Crear procesos de documentación de los casos donde se reporten los eventos sucedidos en las posibles intrusiones de seguridad •Definir roles en las diferentes áreas técnicas y administrativas ante posibles casos de seguridad con los cuales puedan dar soluciones prácticas a los eventos •Crear el informe técnico y ejecutivo forense de la intrusiones de seguridad en los sistemas donde se dé la información relevante del caso

Anexos

A.16.1.2	Reporte de eventos de seguridad de la información	•Diseñar protocolos en caso de posibles intrusiones de seguridad, donde se den soluciones a dichos casos •Crear procesos de documentación de los casos donde se reporten los eventos sucedidos en las posibles intrusiones de seguridad •Definir roles en las diferentes áreas técnicas y administrativas ante posibles casos de seguridad con los cuales puedan dar soluciones prácticas a los eventos •Crear el informe técnico y ejecutivo forense de la intrusiones de seguridad en los sistemas donde se dé la información relevante del caso
A.16.1.3	Reporte de debilidades de seguridad de la información	•Diseñar protocolos en caso de posibles intrusiones de seguridad, donde se den soluciones a dichos casos •Crear procesos de documentación de los casos donde se reporten los eventos sucedidos en las posibles intrusiones de seguridad •Definir roles en las diferentes áreas técnicas y administrativas ante posibles casos de seguridad con los cuales puedan dar soluciones prácticas a los eventos •Crear el informe técnico y ejecutivo forense de la intrusiones de seguridad en los sistemas donde se dé la información relevante del caso
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	•Diseñar protocolos en caso de posibles intrusiones de seguridad, donde se den soluciones a dichos casos •Crear procesos de documentación de los casos donde se reporten los eventos sucedidos en las posibles intrusiones de seguridad

Anexos

		•Definir roles en las diferentes áreas técnicas y administrativas ante posibles casos de seguridad con los cuales puedan dar soluciones prácticas a los eventos •Crear el informe técnico y ejecutivo forense de la intrusiones de seguridad en los sistemas donde se dé la información relevante del caso
A.16.1.5	Respuesta a incidentes de seguridad de la información	•Diseñar protocolos en caso de posibles intrusiones de seguridad, donde se den soluciones a dichos casos •Crear procesos de documentación de los casos donde se reporten los eventos sucedidos en las posibles intrusiones de seguridad •Definir roles en las diferentes áreas técnicas y administrativas ante posibles casos de seguridad con los cuales puedan dar soluciones prácticas a los eventos •Crear el informe técnico y ejecutivo forense de la intrusiones de seguridad en los sistemas donde se dé la información relevante del caso
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	•Diseñar protocolos en caso de posibles intrusiones de seguridad, donde se den soluciones a dichos casos •Crear procesos de documentación de los casos donde se reporten los eventos sucedidos en las posibles intrusiones de seguridad •Definir roles en las diferentes áreas técnicas y administrativas ante posibles casos de seguridad con los cuales puedan dar soluciones prácticas a los eventos

		•Crear el informe técnico y ejecutivo forense de la intrusiones de seguridad en los sistemas donde se dé la información relevante del caso
A.16.1.7	Recolección de evidencia	•Diseñar protocolos en caso de posibles intrusiones de seguridad, donde se den soluciones a dichos casos •Crear procesos de documentación de los casos donde se reporten los eventos sucedidos en las posibles intrusiones de seguridad •Definir roles en las diferentes áreas técnicas y administrativas ante posibles casos de seguridad con los cuales puedan dar soluciones prácticas a los eventos •Crear el informe técnico y ejecutivo forense de la intrusiones de seguridad en los sistemas donde se dé la información relevante del caso
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO**	
A.17.1	**Continuidad de seguridad de la información**	
A.17.1.1	Planificación de la continuidad de la seguridad de la información	•Determinar posibles causas de los fallos de seguridad para tener control a posibles casos futuros •Determinar el plan de mejoramiento de seguridad a casos futuros •Evaluar la seguridad de los sistemas y de los controles establecidos
A.17.1.2	Implementación de la continuidad de la seguridad de la información	•Determinar posibles causas de los fallos de seguridad para tener control a posibles casos futuros •Determinar el plan de mejoramiento de seguridad a casos futuros •Evaluar la seguridad de los sistemas y de los controles establecidos

Anexos

A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	•Determinar posibles causas de los fallos de seguridad para tener control a posibles casos futuros •Determinar el plan de mejoramiento de seguridad a casos futuros •Evaluar la seguridad de los sistemas y de los controles establecidos
A.18	**CUMPLIMIENTO**	
A.18.1	**Cumplimiento de requisitos legales y contractuales**	
A.18.1.2	Derechos de propiedad intelectual	•Definir los acuerdos contractuales de los empleados del uso de la información sujeta a los procesos institucionales •Formular las políticas de seguridad de acuerdo con normas y leyes que reglamentan la propiedad intelectual, la protección de datos personales y el uso de éstas. •Explicar a los empleados y usuarios del uso como se da uso de la información personal y como esta será guardada y protegida.
A.18.1.3	Protección de registros	•Definir los acuerdos contractuales de los empleados del uso de la información sujeta a los procesos institucionales •Formular las políticas de seguridad de acuerdo con normas y leyes que reglamentan la propiedad intelectual, la protección de datos personales y el uso de éstas. •Explicar a los empleados y usuarios del uso como se da uso de la información personal y como esta será guardada y protegida.

Anexos

A.18.1.4	Privacidad y protección de información de datos personales	•Definir los acuerdos contractuales de los empleados del uso de la información sujeta a los procesos institucionales •Formular las políticas de seguridad de acuerdo con normas y leyes que reglamentan la propiedad intelectual, la protección de datos personales y el uso de éstas. •Explicar a los empleados y usuarios del uso como se da uso de la información personal y como esta será guardada y protegida.
A.18.1.5	Reglamentación de controles criptográficos	•Establecer controles en las tablas sensibles con algoritmos de hash •Establecer los permisos necesarios sobre las redes, aplicaciones y/o sistemas de información para las conexiones externas donde el uso de VPN debe ser encriptado extremo a extremo •Auditar los controles criptográficos establecidos en las políticas de seguridad
A.18.2	**Revisiones de seguridad de la información**	
A.18.2.1	Revisión independiente de la seguridad de la información	•Contratar auditorías externas que determinen el nivel de sistema de seguridad de información •Generar informe de la auditoria con el objetivo de mejoras a futuro de los procesos y controles establecidos s
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	•Realizar auditorías por cada uno de los controles desarrollados para la seguridad de la información •Crear comités de revisión de la seguridad de la información que verifiquen la efectividad de las políticas y controles establecidos

		•Generar informe de la auditoria con el objetivo de mejoras a futuro de los procesos y controles establecidos
A.18.2.3	Revisión del cumplimiento técnico	•Realizar auditorías por cada uno de los controles desarrollados para la seguridad de la información •Crear comités de revisión de la seguridad de la información que verifiquen la efectividad de las políticas y controles establecidos • Generar informe de la auditoria con el objetivo de mejoras a futuro de los procesos y controles establecidos

Tabla 14 Plan de Tratamiento Propuesto para los Controles de la ISO 27001

6. Bibliografía

[1] 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.

[2] M. Alansari, M. Kamel, B. Hakim, and Y. Kadah, “Study of Wavelet-Based Performance Enhancement for Motor Imagery Brain-Computer Interface,” 2018.

[3] Andrés F. Pérez, Andrés F. Cardona, Jorge A. Jaramillo, and Gloria M. Díaz, “Deep Convolutional Neural Networks and Power Spectral Density Features for Motor Imagery Classification of EEG Signals,” 2018.

[4] P. Ballarin Usieto y J. Minguez. "La importancia de la ciberseguridad en brain-computer interfaces". (2018). https://www.bitbrain.com/es/blog/ciberseguridad-cerebro-computadora

[5] S. L. Bernal, A. H. Celdrán, G. M. Pérez, M. T. Barros, and S. Balasubramaniam, “Cybersecurity in Brain-Computer Interfaces: State-of-the-art, opportunities, and future challenges,” 2019, [Online]. Available: http://arxiv.org/abs/1908.03536

[6] J. Britto, V. Chaudhari, D. Mehta, A. Kale, and J. Ramteke, *International Conference on Computer Networks and Communication Technologies*, vol. 15. Springer Singapore, 2019.

[7] S. Burwell, M. Sample, and E. Racine, “Ethical aspects of brain computer interfaces: A scoping review,” *BMC Med. Ethics*, vol. 18, no. 1, pp. 1–11, 2017, doi: 10.1186/s12910-017-0220-y.

[8] J. J. Cano M., “Seguridad de la información y ciberseguridad empresarial,” *Rev. Sist.*, no. 155, pp. 4–7, 2020, doi: 10.29236/sistemas.n155a1.

[9] P. Chaudhary and R. Agrawal, “Emerging Threats to Security and Privacy in Brain Computer Interface,” *Int. J. Adv. Stud. Sci. Res.*, vol. 3, no. 12, pp. 340–344, 2018, [Online]. Available: https://ssrn.com/abstract=3326692

Bibliografía

[10] H. Cho, M. Ahn, S. Ahn, M. Kwon, and S. Chan, “EEG datasets for motor imagery brain computer interface,” *Gigascience*, 2017, doi: 10.1093/gigascience/gix034.

[11] I. Choi, I. Rhiu, Y. Lee, M. H. Yun, and C. S. Nam, *A systematic review of hybrid brain-computer interfaces: Taxonomy and usability perspectives*, vol. 12, no. 4. 2017.

[12] Congreso de la República, “Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [CODIGO_COMERCIO],” *D. Of. No. 45.628 2 agosto 2004*, no. 51, p. 1, 2004, [Online]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_0143_1994.html%0Ahttp://www.secretariasenado.gov.co/senado/basedoc/codigo_comercio.html%0Ahttp://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991_pr007.html%0Ahttp://www.secretaria

[13] Congreso de la República, “Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [CODIGO_COMERCIO],” *D. Of. No. 45.628 2 agosto 2004*, no. 51, p. 1, 2004, [Online]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_0143_1994.html%0Ahttp://www.secretariasenado.gov.co/senado/basedoc/codigo_comercio.html%0Ahttp://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991_pr007.html%0Ahttp://www.secretaria

[14] CONGRESO DE LA REPÚBLICA, “Acceso abusivo a un sistema informático.,” no. 51965, pp. 1–3, 2022.

[15] 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. (2020) https://repositorio.itm.edu.co/handle/20.500.12622/4456

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

Bibliografía

[17] T. A. Deuel, J. Pampin, J. Sundstrom, and F. Darvas, “The Encephalophone: A Novel Musical Biofeedback Device using Conscious Control of Electroencephalogram (EEG),” vol. 11, no. April, pp. 1–8, 2017, doi: 10.3389/fnhum.2017.00213.

[18] L. Duan, M. Bao, S. Cui, Y. Qiao, and J. Miao, “Motor Imagery EEG Classification Based on Kernel Hierarchical Extreme Learning Machine,” 2017, doi: 10.1007/s12559-017-9494-0.

[19] O. D. Eva, “Feature Extraction and Classification Methods for a Motor Task Brain Computer Interface: A Comparative Evaluation for Two Databases,” vol. 8, no. 8, pp. 263–269, 2017.

[20] S. F. Fraga and J. R. Mondragón, “Comparativo De Los Algoritmos De Dimensión Fractal Higuchi, Katz Y Multiresolución De Conteo De Cajas Por Eventos Comparison of Higuchi, Katz and Multiresolution Box-Counting Fractal Dimension Algorithms for Eeg Waveform Signals Based on Event-Related P,” pp. 73–83, 2017.

[21] R. Goosen, A. Rontojannis, S. Deutscher, J. Rogg, W. Bohmayr, and D. Mkrtchian, “Artificial Intelligence Is a Threat to Cybersecurity. It’s Also a Solution.,” p. 6, 2018, [Online]. Available:http://image-src.bcg.com/Images/BCG-Artificial-Intelligence-Is-a-Threat-to-Cyber-Security-Its-Also-a-Solution-Nov-2018_tcm9-207468.pdf

[22] G. S. Gupta, S. Ghosh, and R. K. Sinha, “General Concepts on Electroencephalography-Based Brain-Computer Interface Systems,” *J. Clin. Eng.*, vol. 42, no. 4, pp. 170–188, 2017, doi: 10.1097/JCE.0000000000000238.

[23] K. S. Hong and M. J. Khan, “Hybrid brain-computer interface techniques for improved classification accuracy and increased number of commands: A review,” *Front. Neurorobot.*, vol. 11, no. JUL 2017, doi: 10.3389/fnbot.2017.00035.

[24] ICONTEC, “PROYECTO DE NORMA TÉCNICA COLOMBIANA DE 362/13 NTC-ISO-IEC 27002 (Primera actualización),” *Icontec*, vol. 263/13, pp. 1–114.

[25] Instituto Colombiano de Normas Técnicas y Certificación, “NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001 Requisitos Ntc-Iso/Iec 27001,” *Icontec*, no. 571, p. 37, 2013.

Bibliografía

[26] Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) and de Normas Técnicas y Certificación (ICONTEC), "Norma Técnica NTC-ISO/IEC 27005 colombiana," no. 571, p. 74, 2009, [Online]. Available: https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf

[27] Instituto Nacional de Ciberseguridad, "Glosario de Términos de Ciberseguridad," *Una guía aproximación para el Empres.*, pp. 1–41, 2017.

[28] Instituto Nacional de Ciberseguridad. "El ataque del 'Man in the middle' en la empresa, riesgos y formas de evitarlo". (2020). https://www.incibe.es/protege-tu-empresa/blog/el-ataque-del-man-middle-empresa-riesgos-y-formas-evitarlo

[29] Z. Jin, G. Zhou, D. Gao, and Y. Zhang, "EEG classification using sparse Bayesian extreme learning machine for brain – computer interface," *Neural Compute. Appl.*, vol. 3, 2018, doi: 10.1007/s00521-018-3735-3.

[30] MD, Joadder, J. Myszewski, M. Rahman & 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

[31] V. Jusas, "Application of Convolutional Neural Networks to Four-Class Motor Imagery Classification Problem," no. November 2017, doi: 10.5755/j01.itc.46.2.17528.

[32] S. Kalagi, J. Machado, V. Carvalho, F. Soares, and D. Matos, "Brain Computer Interface Systems Using Non- Invasive Electroencephalogram Signal: A Literature Review," *Int. Conf. Eng. Technol. Innov.*, pp. 1050–1055, 2017.

[33] B. Kerous, F. Skola, and F. Liarokapis, "EEG-based BCI and video games: a progress report," *Virtual Real.*, no. 0123456789, pp. 1–17, 2017, doi: 10.1007/s10055-017-0328-x.

[34] J. Kevric and A. Subasi, "Comparison of signal decomposition methods in classification of EEG signals for motor-imagery BCI system," *Biomed. Signal Process. Control*, vol. 31, pp. 398–406, 2017, doi: 10.1016/j.bspc.2016.09.007.

Bibliografía

[35] O. Landau, R. Puzis, and N. Nissim, “Mind your mind: EEG-based brain-computer interfaces and their security in cyber space,” *ACM Comput. Surv.*, 2020, doi: 10.1145/3372043.

[36] W. F. Lawless, R. Mittu, S. Russell, and D. Sofge, *Autonomy, and artificial intelligence: A Threat or Savior?* 2017.

[37] I. Lazarou, S. Nikolopoulos, P. C. Petrantonakis, I. Kompatsiaris, and M. Tsolaki, “EEG-Based Brain–Computer Interfaces for Communication and Rehabilitation of People with Motor Impairment: A Novel Approach of the 21st Century,” *Front. Hum. Neurosci.*, vol. 12, no. January, pp. 1–18, 2018, doi: 10.3389/fnhum.2018.00014.

[38] J. hua Li, “Cyber security meets artificial intelligence: a survey,” *Front. Inf. Technol. Electron. Eng.*, vol. 19, no. 12, pp. 1462–1474, 2018, doi: 10.1631/FITEE.1800573.

[39] F. Lotte *et al.*, “Introduction: Evolution of Brain-Computer Interfaces To cite this version: HAL Id: hal-01656743,” 2017, [Online]. Available: https://hal.inria.fr/hal-01656743/

[40] R. Martín-Clemente, J. Olias, D. B. Thiyam, A. Cichocki, and S. Cruces, “Information theoretic approaches for motor-imagery BCI systems: Review and experimental comparison,” *Entropy*, vol. 20, no. 1, 2018, doi: 10.3390/e20010007.

[41] N. Masood, “Selection of Electrodes Based on Spatial Filter Weights,” vol. 58, no. Mi, p. 5395, 2011.

[42] D. J. McFarland and J. R. Wolpaw, “EEG-based brain–computer interfaces,” *Curr. Opin. Biomed. Eng.*, vol. 4, pp. 194–200, 2017, doi: 10.1016/j.cobme.2017.11.004.

[43] M. S. A. Megat Ali, A. H. Jahidin, M. N. Taib, and N. Md Tahir, “Eeg Sub-Band Spectral Centroid Frequency and Amplitude Ratio Features: A Comparative Study in Learning Style Classification,” *J. Teknol.*, vol. 78, no. 2, Feb. 2016, doi: 10.11113/jt. v78.4100.

[44] Ministerio de Tecnologías de la Información y las Comunicaciones, “Modelo de Seguridad y Privacidad de La Información - Guía de Mejora Continua,” D. Of., p. 58, 2016, [Online]. Available: https://www.mintic.gov.co/gestionti/615/articles-

Bibliografía

5482_Modelo_de_Seguridad_Privacidad.pdf%0Ahttps://www.mintic.gov.co/gestionti/615/articles-5482_G17_Mejora_continua.pdf.

[45] E. A. Mohamed, M. Z. Yusoff, A. S. Malik, M. R. Bahloul, D. M. Adam, and I. K. Adam, “Comparison of EEG signal decomposition methods in classification of motor-imagery BCI,” 2018.

[46] K. Mrozik, “S Pa 2017 Comparison of selected electroencephalographic signal classification methods,” pp. 36–41, 2017.

[47] National Institute of Standards and Technology. "Guide for Conducting Risk Assessments - NIST 800-30". (2012). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[48] Nick Maynard, “Demystifying brain machine interfaces,” in *Juniper Research*, 2019.

[49] D. Novak *et al.*, “Benchmarking Brain-Computer Interfaces Outside the Laboratory: The Cybathlon 2016,” *Front. Neurosci.*, vol. 11, no. January, p. 756, 2018, doi: 10.3389/fnins.2017.00756.

[50] V. P. Oikonomou, K. Georgiadis, G. Liaros, S. Nikolopoulos, and I. Kompatsiaris, “A comparison study on EEG signal processing techniques using motor imagery EEG data,” *IEEE J. Transl. Eng. Heal. Med.*, no. 1, 2017, doi: 10.1109/CBMS.2017.113.

[51] 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". Vol. 19, n.° 3, pp. 131-142. Revista UIS Ingenierías. (2020) revistas.uis.edu.co/index.php/revistauisingenierias/

[52] C. Pandarinath *et al.*, “High performance communication by people with paralysis using an intracortical brain-computer interface,” pp. 1–27, 2017, doi: 10.7554/eLife.18554.

[53] P. K. Pattnaik and J. Sarraf, “Brain Computer Interface issues on hand movement,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 30, no. 1, pp. 18–24, 2018, doi: 10.1016/j.jksuci.2016.09.006.

Bibliografía

[54] C. N. de Política Económica y Social, R. de Colombia, and D. N. de Planeación, "Documento Conpes 3854," p. 91, 2016, [Online]. Available: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

[55] L. Meng *et al.*, "EEG-Based Brain-Computer Interfaces Are Vulnerable to Backdoor Attacks," pp. 1–11, 2020, [Online]. Available: http://arxiv.org/abs/2011.00101

[56] Presidencia de la República, "Documento Conpes 3701, Lineamientos de política para ciberseguridad y ciberdefensa," *Lineamientos Política Para Ciberseguridad Y Ciberdefensa*, p. 43, 2011, [Online]. Available: https://www.mintic.gov.co/portal/inicio/3510:Conpes-3701-de-2011

[57] presidente de la República de Colombia, "DECRETO 1377 DE 2013 (junio," pp. 1–9, 2013, [Online]. Available: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

[58] M. K. Rahman and M. A. M. Joadder, "A Review on the Components of EEG-based Motor Imagery Classification with Quantitative Comparison," *Appl. Theory Comput. Technol.*, vol. 2, no. 2, p. 1, 2017, doi: 10.22496/atct20170122133.

[59] M. A. Roldan Alvarez & H.F. Vargas Montoya. "Ciberseguridad en las redes móviles de telecomunicaciones y su gestión de riesgos". Revista Científica Ingeniería Y Desarrollo, 38(2), 279–297. (Julio, 2021). https://doi.org/10.14482/inde.38.2.006.31

[60] A. C. Ramos, M. Vellasco, and P. Vellasco, "Ensemble of Classifiers Applied to Motor Imagery Task Classification for BCI Applications," pp. 2995–3002, 2017.

[61] Secretaría del Senado, república de Colombia. "Ley Estatutaria 1581 De 2012". (2012). http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[62] S. Sakhavi and C. Guan, "Convolutional neural network-based transfer learning and knowledge distillation using multi-subject data in motor imagery BCI," *Int. IEEE/EMBS Conf. Neural Eng. NER*, pp. 588–591, 2017, doi: 10.1109/NER.2017.8008420.

Bibliografía

[63] R. T. Schirrmeister *et al.*, “Deep Learning with Convolutional Neural Networks for EEG Decoding and Visualization,” vol. 5420, no. August, pp. 5391–5420, 2017, doi: 10.1002/hbm.23730.

[64] S. Pazouki, A. Aydeger, and S. M. Kazemi-Razi, “False Data Injection Cyberattacks to Human Brain Implants’ Power Source,” Int. Conf. Electr. Comput. Energy Technol. ICECET 2021, no. December, pp. 9–10, 2021, doi: 10.1109/ICECET52533.2021.9698569.

[65] Y. R. Tabar and U. Halici, “A novel deep learning approach for classification of EEG motor imagery signals,” *J. Neural Eng.*, vol. 14, no. 1, p. 16003, 2017, doi: 10.1088/1741-2560/14/1/016003.

[66] C. B. Tabernig, L. C. Carrere, L. Escher, and G. Gentiletti, “Evaluación de Desempeño de un Sistema Basado en Interfaz Cerebro Computadora por Imaginería Motora y Realidad Virtual: Cambios entre y las Basado en Interfaz Cerebro Computadora por Imaginación Motora Y Realidad Virtual,” no. September 2017.

[67] H. Takabi, “Firewall for brain: Towards a privacy preserving ecosystem for BCI applications,” *2016 IEEE Conf. Commun. Netw. Secur. CNS 2016*, pp. 370–371, 2017, doi: 10.1109/CNS.2016.7860516.

[68] H. Takabi, A. Bhalotiya, and M. Alohaly, “Brain computer interface (BCI) applications: Privacy threats and countermeasures,” *Proc. - 2016 IEEE 2nd Int. Conf. Collab. Internet Comput. IEEE CIC 2016*, no. c, pp. 102–111, 2017, doi: 10.1109/CIC.2016.24.

[69] L. Vareka and P. Mautner, “Stacked autoencoders for the P300 component detection,” *Front. Neurosci.*, vol. 11, no. MAY, pp. 1–9, 2017, doi: 10.3389/fnins.2017.00302.

[70] Dobosz, Krzysztof & Wittchen, Piotr.” Brain-Computer Interface for mobile devices. Journal of Medical Informatics & Technologies”. 2015. Vol 24. pp 215-222.