VOLUMEN 6 / Nº 1
Enero - Abril de 2022
ISSN IMPRESO: 2528-8008
ISSN ELECTRÓNICO: 2588-0888

KILLKANA

TÉCNICA

REVISTA DE INVESTIGACIÓN CIENTÍFICA

Universidad Católica de Cuenca

KILLKANA

TÉCNICA

Volumen 6, Número 1,
ISSN impreso: 2528-8024
ISSN electrónico: 2588-0888

Universidad Católica de Cuenca

Cuenca, enero de 2022

Revista Killkana Técnica

ISSN IMPRESO: 2528-8008
ISSN ELECTRÓNICO: 2588-0888

Departamento de Posgrado, Investigación
Vinculación con la Sociedad y Publicaciones
de la Universidad Católica de Cuenca
Av. de Las Américas y Humbolt

Código Postal 010101, Cuenca–Ecuador
killkana.investigacion@ucacue.edu.ec

Central telefónica:
+593 (7) 2-830-751
+593 (7) 2-824-365
+593 (7) 2-826-563

http://www.ucacue.edu.ec
http://killkana.ucacue.edu.ec

Volumen 6, Número 1
Publicación trianual

Diseño y diagramación
Dis. Alexander Campoverde Jaramillo

English texts revision/edition
Lic. Tania Cecilia Bustamante Saavedra, Mgs.

Versión digital
Editorial Universitaria Católica (EDUNICA)

Gestión Editorial de la Revista Killkana Técnica

Editora

- Ing. Sist. Aura del Cisne Guerrero Luzuriaga MsC.

Comité Científico

Miembros

Big Data y su importancia en la actualidad

Ing. Aura Guerrero-Luzuriaga[1,2*]

[1] Universidad Católica de Cuenca
[2] Universidad Internacional Iberoamericana
* Autor para correspondencia: ing.auragl@gmail.com

DOI: https://doi.org/10.26871/killkanatecnica.v6i1.1002
ORCID: https://orcid.org/0000-0003-0734-7691

Editorial

El universo digital ha ido evolucionando desde hace varias décadas. Desde 1948, cuando Claude Shannon creó la palabra *byte* para denominar la medida de una unidad de información, la sociedad a nivel mundial inició su incursión en este ámbito. Desde entonces, el camino ha sido largo, difícil, pero lleno de satisfacciones que van en beneficio del conocimiento y la automatización de procesos. En esta trayectoria se han gestado varios términos como *big data, cloud computing, dataset*, entre otros; todos ellos con un fin común, hablar sobre el manejo de grandes cantidades de información.

Big data es importante no solo por los desafíos tecnológicos que implica, sino también por los impactos a menudo invisibles que transformarán la forma en que trabajamos y vivimos. En este mismo campo, se destacan tanto los CIO (*Chief Information Officer*) como los CDO (*Chief Data Officer*), responsables de administrar la tecnología y la infraestructura a través de las cuales se procesan y generan los flujos de datos e información. Dicho esto, la ola del *big data* indica

que son más los factores que se encargan de generar conocimiento para la acción, denotando importancia en la calidad de los datos y la transformación de la información para que este conocimiento sea procesable [1].

Y ¿qué hace un CIO -director de información o un CDO- director de datos dentro del mundo del *big data*? Ahora daremos respuesta a la misma y se analizará su importancia en la actualidad. El primero hace referencia al responsable de las tecnologías de la información y sistemas utilizados de la empresa. Su rol se basa en planificar los procesos y definir los canales de comunicación especialmente a nivel de comunicación interna [2].

Si se analiza la incidencia de este cargo en una empresa, se podría visibilizar su importancia en la consecución de resultados a corto, mediano y largo plazos, ya que una comunicación efectiva se basa un sistema de comunicación cuyos procesos sean claros, cimentados siempre en el buen uso de las tecnologías de la empresa. Concerniente a la información que maneja, ya no solo deberá pensar en almacenar la información, sino también en el volumen de la misma, y, sobre este, prever la cantidad de datos generados por segundo, minuto y día. Esta es la característica más relevante del *big data*, ya que se refiere a una gran cantidad de datos que se almacenan para procesar dicha información, convirtiendo los datos en acción y esta en resultados.

Ahora, el CDO es un cargo especialmente creado para las empresas *online* o digitales. Esta persona es quien fija la estrategia a nivel digital para que la empresa no quede obsoleta respecto a su competencia [3]. Este ingeniero deberá, por lo tanto, de la gestión de los datos masivos, incluir acciones intelectuales que permitan ganar un peso relevante en su desempeño, como la gestión, el análisis y la creación de valor. Por eso, varios perfiles profesionales ya existentes están involucrados en la gestión de los datos masivos (ingenieros informáticos, estadistas, matemáticos, gestores de la información, archiveros, bibliotecarios y analistas). Debe tener la capacidad transversalmente de gestionar los datos masivos a lo largo de toda la cadena de valor, este aspecto es el diferenciador radical del CIO; pero, para llegar a desarrollar este tipo de perfil, se debe trabajar en la autoformación que complemente todo este bagaje de conocimientos y poder cubrir este tipo de vacantes que, en la posteridad, serán claves en las empresas [3].

Así, asumiendo que ya se tiene nociones de lo que hacen las personas de estos dos cargos (parte fundamental del argot de ingeniería en sistemas y similares), se continuará con un breve análisis sobre otros factores importantes de *big data* y otros términos que conectan aún más al mundo 2.0, un escenario que está gobernado por la generación de más y más datos. En este sentido, para algunas empresas, es obligatorio estar en el mundo digital, ya que la generación de datos es de manera exponencial. Por ejemplo, citemos una empresa que oferta sus productos de manera física y *online*: a simple vista, le convendría implementar tecnología *big data* para procesar

toda aquella información que recoge su personal en planta y su página web, debiendo rastrear todas las acciones que lleva a cabo su personal y el cliente; conocer dónde cliquean más veces, cuántas veces han pasado el carrito de compra, cuáles son los productos más vistos, cuáles son los insumos más utilizados y aquellos que perecen con mayor rapidez, etc.[4], todo ello es más fácil de manejar, si se cuenta con el personal idóneo para el tratamiento de esta información. Ahí, las técnicas de manejo de datos a gran escala caen "como anillo al dedo", logrando un manejo eficiente de los recursos de la empresa: es este el secreto para que gerentes, inversionistas y clientes logren sus proyecciones.

Los cambios que la sociedad experimenta gracias a las bondades que brinda el manejo de *big data* pueden ayudar a gerentes y administradores de los diferentes tipos de empresa en la anticipación de la demanda de los clientes y de su personal interno, en lo concerniente a insumos de producción. ¿Cómo lo hacen? Los profesionales que manejan técnicas para el manejo masivo de datos primero clasifican los atributos clave del pasado y productos actuales; si el profesional domina también las técnicas de modelado y inteligencia artificial, su siguiente paso es modelar la relación entre esos atributos y el comercial éxito de las ofertas, y, en el caso de los insumo, relacionaría atributos con temporadas; con todos los atributos listos, relacionados y disponibles, podrá crear modelos predictivos para nuevos productos y servicios. Con ello deberá sumergirse en lo más profundo mediante el uso de datos y análisis de grupos focales, redes sociales, mercados de prueba y primeros lanzamientos de tiendas para planificar, producir y lanzar nuevos productos.

Desde otras luces, es necesario dar otro enfoque al manejo masivo de información, desde la óptica de la medicina en que las organizaciones de atención médica están utilizando *big data* para la inmensa mayoría de sus procesos, desde mejorar la rentabilidad para ayudar a salvar vidas hasta la gestión de insumos en empresas sanitarias y centros de atención médica como hospitales; se recopilan cantidades masivas de datos en cuestión de horas. Sin embargo, todos estos datos no son útiles de forma aislada. Eso se vuelve importante cuando los datos se analizan para resaltar tendencias y amenazas en patrones y crear modelos predictivos que vayan en pro del cuidado de la salud en toda su cadena de abastecimiento.

En la industria del petróleo y el gas, durante los últimos años, se ha estado aprovechando el *big data* para encontrar nuevas formas de innovar. La industria ha utilizado durante mucho tiempo sensores de datos para rastrear y monitorear el desempeño de pozos petroleros, maquinaria y operaciones. Estas empresas han podido aprovechar estos datos para monitorear la actividad de los pozos, crear modelos para encontrar nuevas fuentes de petróleo y realizar muchas otras tareas de valor agregado.

Las organizaciones pueden acceder a datos hoy más que nunca. Pero no tiene valor a menos que sepa cómo dar funcionamiento a su *big data*. La entrega de herramientas que las empresas están aprovechando estima sus datos para mejorar la toma de decisiones, ingresar a nuevos mercados y ofrecer experiencias más favorables de sus clientes internos y externos es el fin del *big data*; por ello, cada vez más, los profesionales en el área tecnológica deben capacitarse, enfrentar las malas noches e incluso "dos que tres peleas en casa", por aprender este fascinante mundo y ser un medio entre lo que un gerente o administrador quiere y lo que los datos ofrecen.

Referencias bibliográficas

[1] M. G. Alsina, "Los profesionales del big data: ¿de los gestores de la información a los científicos de datos?," *COMeIN*, no. 56. 2016. doi: 10.7238/c.n56.1645.

[2] Jorge, "Las 8 siglas de los altos cargos de empresa: CEO, COO, CMO, CFO, CIO, CTO, CCO y CDO," *Watch & Act*, Jul. 23, 2021. https://watchandact.eu/8-siglas-altos-cargos-empresas/ (accessed Mar. 30, 2022).

[3] Universitat Oberta de Catalunya, "Los profesionales del big data: ¿de los gestores de la información a los científicos de datos?" https://comein.uoc.edu/divulgacio/comein/es/numero56/articles/Article-Montserrat-Garcia-Alsina.html (accessed Mar. 30, 2022).

[4] "Las 7 V del Big data: Características más importantes - IIC," *Instituto de Ingeniería del Conocimiento*, Jun. 28, 2016. https://www.iic.uam.es/innovacion/big-data-caracteristicas-mas-importantes-7-v/ (accessed Mar. 30, 2022).

Contenido

Artículo de Investigación. Revista Killkana Técnica. Vol. 6, No. 1, pp. 1-20, enero-abril, 2022.
ISSN 2528-8024. ISSN Elect. 2588-0888. Universidad Católica de Cuenca

Incidencia de la implementación de los sistemas de gestión de calidad en los resultados de la función sustantiva de investigación de la Universidad Católica de Cuenca

The Impact of the implementing quality management systems on the substantive function research's results at The Catholic University of Cuenca

Santiago Moscoso Bernal[1, 2]*, Raymundo Forradelas Martinez[2]*, Jaime Tinto Arandes[1]*, Orlando Álvarez LLamoza *, Henry Cabrera Vintimilla[1]

[1] Universidad Católica de Cuenca – Ecuador
[2] Universidad Nacional del Cuyo – Argentina

* smoscoso@ucacue.edu.ec
DOI: https://doi.org/ 10.26871/killkanatecnica.v6i1.887

Resumen

Las dinámicas que conllevan los procesos de enseñanza – aprendizaje, en conjunto con las exigencias de la sociedad, la globalización y la internacionalización demandan altos estándares de calidad y la dirección eficiente de las (IES)[1], esto ha originado aplicación de procesos innovadores para el desarrollo de sus funciones sustantivas y de modelos de gestión interna. En este contexto, los (SGC)[2] implementados en la industria han sido adaptadas a las IES como herramienta para fortalecer su modelo de gestión. El objetivo de la investigación es determinar los beneficios que conlleva la implementación de los SGC en la producción científica de los docentes. La investigación es de tipo exploratoria y descriptiva. Para el caso de la Universidad Católica de Cuenca, la implementación de los SGC en los procesos de investigación, ha permitido garantizar una estructura orgánica y una adecuada planificación de las actividades enfocadas al desarrollo de programas y proyectos de investigación, contribuyendo a establecer un conjunto de políticas que se ven reflejadas en un incremento de la tasa de producción científica de los profesores. El estudio comprende el período entre los años 2015 y 2020.

Palabras clave: *Sistemas de Gestión de la Calidad, Investigación, Procesos, Universidades, Calidad de la Educación, Educación Superior.*

Abstract

The teaching-learning process dynamics, along with the demands of society, globalization and internationalization, require high-quality standards and efficient management of Higher Education Institutions (HEIs), originating the application of innovative processes to develop their substantive functions and internal management models. In this context, the Quality Management System implemented in the industrial sector have been adapted to HEIs as a strengthening tool for their management model. This research aims to determine the benefits of implementing the QMS on the teachers' scientific production. This research is exploratory and descriptive. The implementation of the QMS in the research processes at the Catholic University of Cuenca has allowed guaranteeing an organic structure and adequate planning of the activities oriented to the development of research programs and projects; contributing to establishing a set of policies evidenced in the rate increment of the professors' scientific production. The study comprises the period between 2015 and 2020.

Keywords*: Quality Management Systems, Research, Processes, Universities, Education Quality, Higher Education*

[1] *Las Instituciones de Educación Superior (IES) son las entidades que cuentan, con arreglo a las normas legales, con el reconocimiento oficial como prestadoras del servicio de educación superior en el territorio ecuatoriano; e incluyen: i) Las universidades, escuelas politécnicas públicas y particulares; ii) Los institutos superiores técnicos, tecnológicos, pedagógicos y de artes, y, iii) Los conservatorios superiores. Ya sean públicos como particulares y debidamente evaluados y acreditados, conforme la presente Ley. [4]*

[2] Un sistema de gestión de calidad es un sistema formal que permite documentar procesos, procedimientos y asignaciones de responsabilidades para que sea posible lograr y alcanzar políticas y objetivos de calidad. [23]

Introducción

Varias universidades en el mundo y específicamente en el Ecuador, buscan imperiosa e incansablemente garantizar altos niveles de calidad en sus funciones sustantivas y procesos internos; el problema, radica en la implementación y afianzamiento de sus sistemas internos de aseguramiento de la calidad y que estos sean duraderos en el tiempo. En este contexto Alarcón, et al (2019) señala que:

> *Elaborar el mapa de procesos es para muchas universidades y organizaciones de todo tipo el inicio del cambio de gestión e inclusive el inicio del diseño de su sistema de calidad, por lo tanto, su correcta elaboración influenciará en el resto de documentos del o los sistemas que a partir de este se elaboren. Identificar adecuadamente cada proceso y cuál es su tipo también es fundamental, pues pudiera establecer la atención que se le brinde a estos, ya que los procesos claves son por lo general a quienes se da más cuidado e incluso la destinación de recursos es prioritaria, pues elaboran y prestan el servicio que el cliente consumidor recibe; al identificarlos incorrectamente podríamos ser ineficientes en esta asignación. [1]*

En este mismo contexto Orozco, et al (2020) señala que el aseguramiento externo de la calidad, centrado en los procesos de acreditación, y su contrapartida, la gestión de la calidad en las IES cimentada en los sistemas internos de gestión de calidad, son aspectos que se interrelacionan y se enfocan a la mejora continua. [2]. Por otra parte Rojas, et al (2019) señalan que:

> *Después de haber analizado los modelos de evaluación institucional y de carreras propuestos por el CEAACES y el SGC basado en ISO 9001, se concluye que; aunque el origen y la naturaleza del SGC basado en ISO 9001 y el promovido por las entidades oficiales ecuatorianas para la gestión de la calidad de la educación superior son distintos, no se contraponen ni se excluyen, por el contrario, ambos sistemas de gestión son complementarios. [3]*

Con lo antes señalado, se puede indicar que los cambios constantes en la educación de manera general, y más aún en la educación superior, provocados por los vertiginosos avances tecnológicos, nuevos métodos y técnicas de enseñanza - aprendizaje, modelos de evaluación, requerimientos y exigencias del sector productivo y demandas de la sociedad, ha ocasionado que las universidades deban acondicionar sus procesos y modelos de gestión para atender las necesidades de la colectividad, y transformarse, para dar cumplimiento a lo que contempla el marco normativo en el Ecuador, específicamente lo que señala en el principio de pertinencia de la Ley Orgánica de Educación Superior (LOES):

> *La educación superior responda a las expectativas y necesidades de la sociedad, a la planificación nacional, y al régimen de desarrollo, a la prospectiva de desarrollo científico, humanístico y tecnológico mundial, y a la diversidad cultural. Para ello, las instituciones de educación superior articularán su oferta docente, de investigación y actividades de vinculación con la sociedad, a la demanda académica, a las necesidades de desarrollo local, regional y nacional, a la innovación y diversificación de profesiones y grados académicos, a las tendencias del mercado ocupacional local, regional y nacional, a las tendencias demográficas locales, provinciales y regionales; a la vinculación con la estructura productiva actual y potencial de la provincia y la región, y a las políticas nacionales de ciencia y tecnología [4, p. 43].*

En base a lo anterior, se requiere que las (IES), articulen las tres funciones sustantivas: docencia, investigación y vinculación con la sociedad. Para esto es necesario estandarizar y fortalecer el desarrollo de las actividades realizadas al interior de la institución, siendo de gran importancia, la implementación de un sistema de gestión de calidad (SGC). Según mencionan Acuña & López (2016) [5], los SGC son necesarios para garantizar el óptimo funcionamiento de las IES y contribuir a la correcta interacción de las partes que la conforman (autoridades, docentes, estudiantes y sociedad), a través de la definición de políticas, objetivos e implementación de procesos y procedimientos que permitan alcanzar las metas establecidas en su planificación estratégica [5].

El desarrollo de la investigación en las IES, permite cumplir su legado << dar solución a los problemas de su entorno>>, a más de otorgar reconocimiento social por parte de la comunidad y posicionamiento en rankings internacionales, ya que el denominador común de ellos es valorar la contribución que realizan las mismas, para coadyuvar a la solución de problemas que aquejan. Es por ello la importancia de una adecuada y eficiente gestión de la función sustantiva de investigación permitirá garantizar adecuados niveles de cumplimiento en los objetivos propuestos, todo ello, apalancados en un sistema de gestión de calidad.

El objetivo de la presente investigación consiste en el análisis de la implementación de un sistema de gestión de calidad y los resultados observados en los procesos de evaluación externa con fines de acreditación, adicional a ello cómo la implementación de un sistema de gestión de calidad (SGC) basado en procesos y procedimientos, los mismos que se encuentran alineados a la Norma ISO: 9001-2015 favorecen o benefician a la tasa de producción per cápita de los docentes y en general de todos los actores de la comunidad universitaria. El estudio se aplica en la Universidad Católica de Cuenca, ubicada en la sierra sur del Ecuador, con presencia en las provincias de Azuay, Cañar y Morona Santiago.

En este contexto, y de acuerdo a lo señalado en párrafos anteriores, la evaluación de la calidad en la Educación Superior ha adquirido especial importancia a nivel mundial. En el caso específico de Ecuador, las evaluaciones de las IES han representado un proceso de gran significancia y repercusión en los últimos 10 años. La importancia de estos procesos viene dada por diversos factores entre los que resaltan:

- Interés público por acrecentar los niveles de calidad a través de la implementación de mecanismos garantía de la calidad a partir de la evaluación externa en sus distintas figuras: evaluación de programas, acreditación, auditorías de calidad, sistemas de indicadores, etc.;
- Presencia internacional a través de la consideración y aplicación en los rankings o clasificaciones de universidades, y;
- Exigencia de la sociedad de tener una garantía de la calidad de las distintas carreras de grado y programas de posgrado [6].

Luego de los resultados obtenidos en el proceso de evaluación externa con fines de acreditación, realizado en el año 2014 por el entonces denominado Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior (CEAACES), la Universidad Católica de Cuenca, inicia con el modelamiento de su SGC alineado a la Norma ISO (International Organization for Standardization). En esa oportunidad la IES obtuvo la categoría D (penúltima categoría) y como una estrategia para mejorar los resultados obtenidos, fortalecer y consolidar la ejecución de la planificación y el desarrollo de sus funciones sustantivas, la institución inicia con la aplicación

de la norma ISO en su versión 9001:2008, para luego migrar su SGC a la norma ISO 9001:2015, logrando cumplir los requisitos normativos establecidos.

Metodología

La investigación se desarrolló utilizando un estudio observacional descripto de las normas ISO 9001 versión 2015 y su relación con un sistema de gestión de la calidad en la función sustantiva de la Universidad Católica de Cuenca. El propósito se fundamenta en la complementariedad del SGC y los modelos de evaluación institucional de universidades y escuelas politécnicas definidos por el Consejo de Aseguramiento de la Calidad de la Educación Superior (CACES)[3].

La investigación es de tipo exploratoria y descriptiva. Se considera exploratoria debido a que no existen antecedentes de un SGC en la institución objeto de estudio, y se determinan las variables desconocidas que intervienen en el proceso de mejora continua. Es descriptiva debido a que se describen las dinámicas que deben ser incorporadas a las variables dentro de la construcción del SGC, con el fin de evaluar el efecto producido en una línea de tiempo.

El diseño de la investigación se realiza en dos fases:

- Contextualización de la puesta en funcionamiento del SGC dentro de la función sustantiva de investigación de la UC y el establecimiento de la cultura de la calidad en la institución.
- Analizar la incidencia de la implementación del SGC en los resultados de los indicadores de evaluación externa con fines de acreditación y sus autoevaluaciones.

Para la recolección de los datos se procedió a solicitar un reporte generado por el sistema ERP UNIVERSITY[4], utilizado por la institución durante el período 2015- 2020 y, se contrastó la información con la técnica de la entrevista in situ, realizada en cada uno de los departamentos que competen al área de investigación. En este sentido se diseñó y aplicó una guía de entrevista y una de observación.

La población en el momento que se efectúo la investigación fue de 17345 estudiantes, 832 docentes de los cuales 87 son investigadores y 81 autoridades.

Estado del arte

A. Importancia del desarrollo de actividades de investigación en las ies

Los procesos de mejora continua en las IES constituyen no solo un reto, sino un compromiso con la actual y futura sociedad; sin embargo, la implementación de un sistema de gestión de la calidad moderno, objetivo y pertinente, a más de las exigencias normativas y requisitos del cliente <<estudiante>>, adquiere especial connotación para una universidad que se proclama proactiva.

[3] *CACES (Consejo de Aseguramiento de la Calidad de la Educación Superior de Ecuador): es el organismo público, que tiene a su cargo la regulación, planificación y coordinación del sistema de aseguramiento de la calidad de la educación superior; tendrá por objetivo garantizar el desarrollo de una cultura de la calidad en las instituciones de educación superior.*

[4] *El sistema ERP University es una plataforma informática de software de la UC, para la planificación y gestión de recursos empresariales, principalmente recursos financieros, recurso humano, gestión de clientes y gestión del servicio prestado (gestión académica). El sistema está concebido bajo dos ejes generales que son: el eje academia y el eje administración, los cuales obedecen a normativas, procesos, estándares y necesidades internas y externas de la Institución. Funciona bajo un sistema web, lo cual permite la distribución y actualización de forma rápida y ligera. Como cliente es necesario únicamente un navegador web y acceso a internet [16]*

Desde hace algunos años, las universidades ecuatorianas han comenzado a robustecer el desarrollo e institucionalización de la investigación de acuerdo a sus fortalezas y dominios académicos. Esta acción ha tenido un impulso vertiginoso a partir del año 2008, a raíz de la instauración de la nueva constitución y del consiguiente inicio de los procesos de evaluación y acreditación de las IES de manera obligatoria.

Durante la década de los 2010, gracias a los procesos de evaluación a las que fueron sometidas las IES, se produjo la reorientación hacia nuevas políticas encaminadas a la mejora continua de la calidad académica. Durante este tiempo de cambio, las entidades rectoras de la Educación Superior Ecuatoriana establecieron indicadores con el propósito de guiar, apoyar y monitorear la acción de los actores del sistema educativo.

Dentro de este proceso, la función sustantiva de investigación cuenta con los estándares de planificación, ejecución y resultados de la misma, y, cada uno de estos estándares cuentan a su vez con sus indicadores, elementos fundamentales y fuentes de información.

B. Sistema de gestión de calidad

Un Sistema de Gestión de Calidad puede ser elaborado y ejecutado de acuerdo a varios enfoques, el más relevante y utilizado actualmente es apegándose a la norma ISO 9001: 2015. Esta norma internacional tiene como uno de sus principios fundamentales la gestión por procesos que permitan la toma de decisiones de forma oportuna y una mejora continua y sistemática de sus funciones sustantivas, controlando los resultados a través del manejo de indicadores apropiados.

Un SGC ayuda a las instituciones a definir y delimitar las responsabilidades de los diferentes actores, incorporar una cultura de la calidad en la organización y aporta un mayor conocimiento de las necesidades y expectativas de los clientes, entre otros aspectos [7].

Al mismo tiempo, el SGC se convierte en una herramienta metodológica importante que contribuye a la eficacia y eficiencia. Mejora la calidad a través de la regularización y ordenamiento de las actividades que contemplan los diferentes procesos y el manejo de indicadores de gestión, que ayudan a obtener métricas de manera sistémica e integrada, favoreciendo la toma de decisiones y a elevar el desempeño de los procesos, así como sus resultados [8].

Los modelos más difundidos y establecidos a nivel mundial para la implantación de los SGC, son el Modelo ISO y EFQM.

a) Modelo (ISO 9000)

La Organización Internacional para la Estandarización (International Standard Organization - ISO) ha contribuido con diferentes modelos para la implantación y evaluación de los SGC. Destacan las normas ISO-9001, las cuales están destinadas a la certificación de la calidad en el sector empresarial y en los últimos años también ha incluido el sector educativo. El objetivo primordial es el de articular la gestión de la calidad con los procesos, procedimientos y acciones de la organización, contemplando siempre la mejora continua y sistemática, y por, sobre todo, la satisfacción del cliente. Existen diferentes grupos de normas ISO que se especifican de acuerdo al contexto:

i. Norma ISO 9001:2015.

Es la de mayor divulgación e implementación. En sus inicios se centró en empresas del sector industrial, pero en la actualidad cualquier clase de organización puede implementarla. Sus principales características son: a) genérica y fácilmente aplicable en las organizaciones de cualquier tipo de

índole; b) se centra en el enfoque basado en procesos; c) permite analizar los riesgos y efectuar acciones preventivas; d) contempla información documentada, y; e) realiza un control minucioso de la provisión de bienes y servicios externos.

ii. Norma ISO 21001:2018.

Aplica exclusivamente a instituciones educativas. Se encuentra parcialmente alineada con la norma ISO 9001:2015 y suministra una herramienta de gestión habitual para las organizaciones educativas, con el propósito de perfeccionar sus procesos y atender todas las necesidades e intereses de las personas que utilizan sus servicios.

b) Modelo EFQM:

Es un modelo de Calidad y Excelencia que se enfatiza en actividades y metodologías para el desarrollo de los procesos de mejora continua en entornos empresariales tanto privados como públicos. Los principales conceptos o características que conforman el modelo EFQM son: a) orientación hacia los resultados; b) orientación al cliente; c) liderazgo y coherencia; d) gestión por procesos y hechos; e) desarrollo e implicación de las personas; f) proceso continuo de aprendizaje; g) innovación, mejora y desarrollo de alianzas, y; h) responsabilidad social de la organización. [9].

C. Indicadores de la función sustantiva de investigación

La función sustantiva de Investigación comprende uno de los pilares fundamentales en la generación del conocimiento y en contribuir en la solución de los problemas que aquejan a la sociedad. En base a lo anterior, el modelo de evaluación de universidades y escuelas politécnicas define tres dimensiones para el desarrollo de la investigación: planificación, ejecución y resultados.

a) Planificación de los procesos de investigación:

Esta atapa comprende la planificación anual de los proyectos o programas de investigación, orientado a las líneas de investigación y dominios académicos. Debe tener en cuenta la normativa para la selección, seguimiento y evaluación de dichos programas o proyectos, la asignación de los recursos necesarios para el desarrollo de los mismos, y el respeto de la normativa que garantiza la ética en la investigación, así como la de sus actores.

b) Ejecución de los procesos de investigación

La ejecución comprende los procedimientos de arbitraje y evaluación de los programas y proyectos, la asignación de los recursos económicos a los proyectos aprobados, la determinación de la carga horaria de los docentes investigadores para la ejecución del proyecto y, la aplicación de la normativa ética en el desarrollo de las actividades de investigación.

c) Resultados de los procesos de investigación

Esta dimensión comprende los resultados de la investigación científica y/o tecnológica y/o de creación artística, plasmados en obras de relevancia, valoradas por pares internos y externos a la institución, que cumplen con requisitos básicos de publicación, exposición y/o registro, y están articuladas a sus líneas de investigación y/o proyectos de creación artística [10]. También considera el nivel de impacto de los resultados publicados, dependiendo de la base indizada que lo contenga y el número de citaciones que se ha hecho a cada obra. Los resultados de investigación pueden ser plasmados en artículos publicados en revistas indizadas pertenecientes a bases de datos científicas; libros y capítulos de libros evaluados por pares expertos; participación en eventos académicos; patentes de invención; prototipos

de software; propiedad industrial y; obtención de vegetales.

Cada institución debe demostrar y garantizar la plena realización de la planificación en la investigación, la aplicación de procedimientos de evaluación de programas, proyectos y resultados, así como una adecuada ejecución de los fondos asignados, asegurando la fluidez en los diversos procesos contemplados.

D. Evolución del sgc en la universida católica de cuenca

La Universidad Católica de Cuenca comienza sus procesos de evaluación y acreditación en el año 2012, obteniendo la categoría C de 5 categorías existentes (A, B, C, D, E) [11]; en el año 2014 esta no acreditó y se la ubicó en la categoría D de 5 categorías existentes (A, B, C, D, E) [12], lo que le obligó a diseñar y ejecutar un plan de fortalecimiento institucional que contemplaba la ejecución de estrategias para corregir las debilidades evidenciadas. En el año 2016, la Universidad Católica de Cuenca se presenta a una nueva evaluación luego de haber concluido su plan de fortalecimiento institucional, logrando ubicarse en la categoría B [13] dentro de las 5 categorías ya mencionadas.

Para el año 2019, el organismo gubernamental de control CACES, genera un nuevo modelo de evaluación externa con fines de acreditación, en donde se elimina la clasificación anterior y solo contempla universidades acreditadas y universidades en proceso de acreditación.

Con lo antes mencionado y en función de la implementación del sistema de gestión de calidad como una herramienta que contempla procesos y procedimientos con todas sus especificaciones, su estructura documental (manuales, registros, formatos, instructivos, etc.) ha permitido tener una mejora importante en los resultados de todas las funciones sustantivas, específicamente en investigación.

Bajo este contexto la Universidad Católica de Cuenca, con sus Unidades Académicas y Carreras, distribuidas en su matriz en Cuenca; las sedes en Azogues y Santiago de Macas; sus extensiones de Cañar, y San Pablo de la Troncal; y, sus centros de apoyo en Zamora, Tena, Puyo, y Quito, propició a inicios del año 2014 un acelerado incremento de nuevos roles de la gestión académica y administrativa. Las actividades de gestión debían enmarcarse dentro de la institucionalización universitaria, requerimientos normativos, legales, y los modelos de acreditación de universidades. Adicionalmente, se establecieron nuevas funciones centradas en las actividades que realizan los docentes, tales como capacitaciones, vinculación con la comunidad, investigación, gestión académica entre los de mayor relevancia.

La serie de nuevas actividades, roles y funciones produjo una gran cantidad de procesos que no tenían directrices claras, y la particularidad de que la UC se encuentra dispersa geográficamente, generó la necesidad de homogenizar el accionar institucional y crear un mecanismo de obtención de datos para lograr la toma de decisiones oportuna y basada en evidencias objetivas, lo que a su vez permitiría consolidar el cumplimiento de los objetivos y políticas universitarias.

Este contexto motivó la creación del Sistema de Gestión de Calidad como herramienta que aporte a la homogeneización, articulación de funciones y al monitoreo de indicadores que conllevarían al cumplimiento de las metas, objetivos, y de las políticas que necesita la Universidad para llevar a cabo su misión.

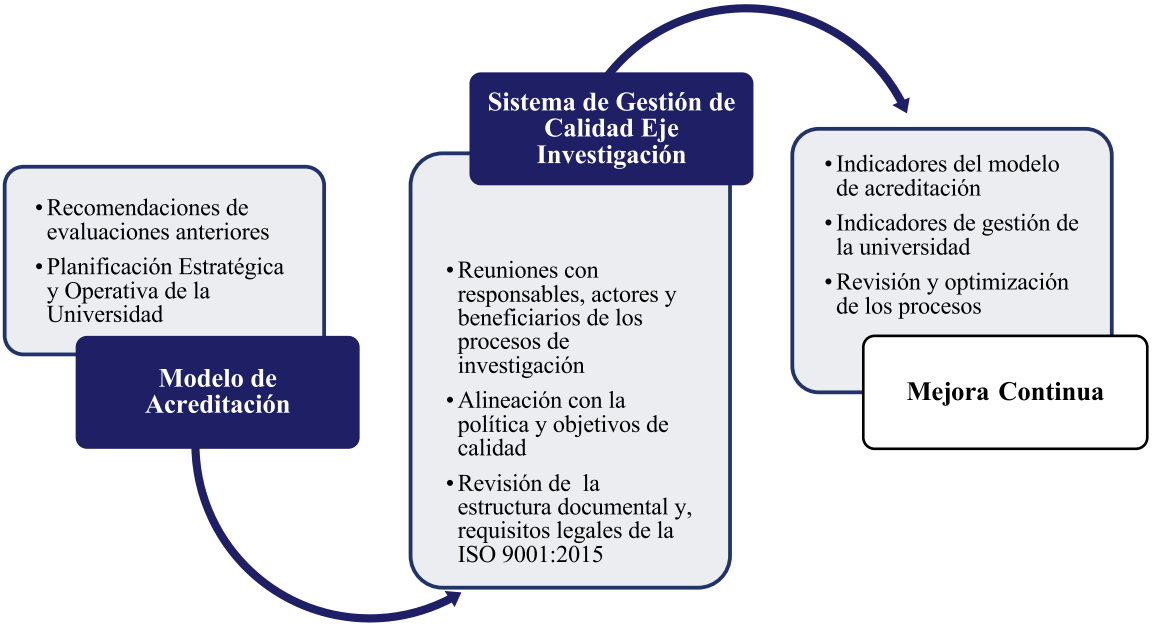


Figura 1: Estructuración del sistema de gestión de calidad para la función sustantiva de investigación.

Resultados

Como primer resultado de la presente investigación, fue la construcción del mapa de procesos para la función sustantiva de investigación, la misma que se detalla en la figura 2, en donde se aprecian las entradas y salidas. La función sustantiva de investigación contempla seis procesos con sus respectivos formatos, instructivos y manuales.

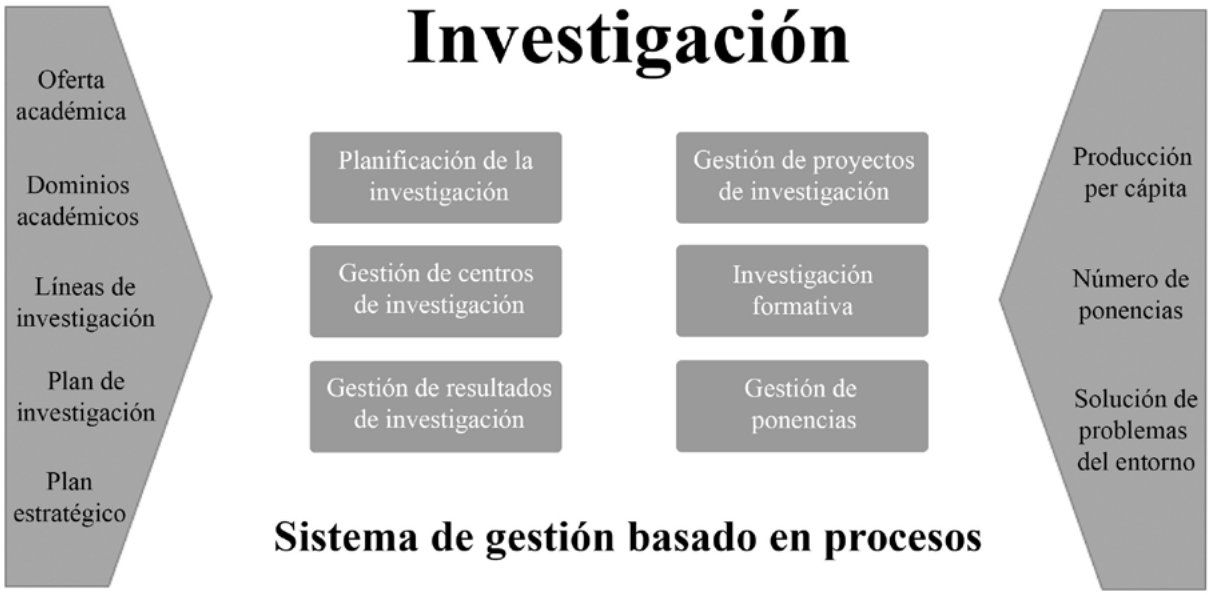


Figura 2: Mapa de procesos de la función sustantiva de investigación.

En la construcción de los procesos de investigación se contemplaron actividades como: reuniones con los responsables y actores de los procesos, revisión de la planificación estratégica y operativa, alineación con la política y objetivos de calidad, modelo de acreditación de universidades y escuelas politécnicas, el modelo genérico de evaluación de carreras de grado vigentes, la estructura documental y, requisitos legales de la Norma ISO 9001:2015, a más de considerar las recomendaciones del proceso de acreditación del año 2016.

El macro proceso de investigación pertenece a los procesos misionales de la institución, y su objetivo es: *establecer los lineamientos para la aprobación, ejecución, supervisión, difusión, priorización y promoción de las actividades y estudios de investigación a ser desarrolladas en la UCACUE con el fin de generar nuevo conocimiento y ayudar a solventar las necesidades de la sociedad actual* [14]. El macro proceso de investigación, contempla los siguientes procesos, mismos que se describen a continuación:

- **Proceso de Planificación de la investigacón:**

  Su objetivo es Elaborar y aprobar la planificación de investigación que contemple las actividades a realizarse en la institución. Contempla como entradas: Modelo Educativo[5], PEDI Institucional[6], Plan de Investigación (anterior) y la oferta académica[7]. Los componentes de este proceso se describen en la tabla 1, y el flujo del mismo, con el detalle de las actividades, responsables, etc., se observa en el anexo Nro. 1.

TABLA I

Caracterización del procedimiento de planificación de la investigación

PROVEEDOR	ENTRADAS	PROCESO	SALIDA	CLIENTES	INDICADOR
Jefatura de Docencia Jefatura de Planificación y Desarrollo Jefatura de Investigación	Modelo Educativo PEDI Institucional Plan de Investigación Oferta académica	Planificación de la Investigación	Plan de Investigación Resolución de Consejo Universitario	Jefatura de Docencia Jefatura de Vinculación	Existencia del Plan de Investigación debidamente aprobado

- **Subproceso de Convocatorias a Proyectos de investigación científica:**

  Su objetivo es anunciar públicamente el llamamiento de docentes investigadores a participar en proyectos de investigación. Incluye las etapas de: determinación de bases de los proyectos, ejecución de la convocatoria, revisión con rigurosidad científica por pares académicos y comunicación de los resultados de los proyectos. Los componentes de este subproceso se describen en la tabla 2, y el flujo del mismo, con el detalle de las actividades, responsables, etc., se observa en el anexo Nro. 2.

[5] El Modelos Educativo es una visión que sintetiza las teorías o enfoques pedagógicos que orientan a los especialistas y a los profesores en la elaboración y análisis de los programas de estudios; en la sistematización del proceso de enseñanza-aprendizaje [22].

[6] El Plan Estratégico de Desarrollo Institucional (PEDI) es un documento de planificación estratégica que recoge los elementos orientadores de la Universidad Central del Ecuador (visión, misión, valores, políticas), a partir de un conjunto de estrategias para alcanzar sus grandes objetivos.

[7] La oferta académica es el conjunto de carreras o programas de estudio, las cuales se tienen que caracterizar atendiendo la institución y la naturaleza de la formación como respuesta para satisfacer las necesidades específicas de la sociedad [21].

TABLA II

Caracterización del procedimiento de planificación de la investigación

PROVEEDOR	ENTRADAS	PROCESO	SALIDA	CLIENTES	INDICADOR
Jefatura de Investigación Coordinación de los Centros de Investigación, Innovación y Transferencia de Tecnolía (CIITT)	Plan de Investigación	Procedimiento de Planificación de la Investigación	Proyectos de investigación aproados, con revisión de pares académicos	Unidades Académicas Docentes Investigadores Estudiantes	Porcentaje de Proyectos de Investigación Aprobados

- **Subproceso de Asignación de recursos a los Proyectos de investigación científica:**

  Su objetivo es conceder los recursos necesarios (económicos, tecnológicos y humanos) a los proyectos de investigación aprobados. Los componentes de este subproceso se describen en la tabla 3, y el flujo del mismo, con el detalle de actividades, responsables, etc., se observa en el anexo Nro. 3.

TABLA III

Caracterización del procedimiento de planificación de la investigación

PROVEEDOR	ENTRADAS	PROCESO	SALIDA	CLIENTES	INDICADOR
Jefatura de Investigación Jefatura de Planificación y Desarrollo Jefatura Financiera	Listado de proyectos de investigación aprobados Actores: docentes, investigadores y estudiantes que intervienen en la ejecución de los proyectos de investigación.	Procedimiento de Asignación de recursos a los proyectos de investigación	Recursos asignados a los proyectos de investigación	Directores y codirectores de los proyectos de investigación Docentes Investigadores Estudiantes	Presupuesto ejecutado a los proyectos de investigación

- **Subproceso de seguimiento a los proyectos de investigación científica:**

Su objetivo es controlar la ejecución de recursos y los avances de los proyectos de investigación aprobados, así como determinar acciones correctivas en caso de presentar desviaciones en función de su planificación. Los componentes de este subproceso se describen en la tabla 4, y el flujo del mismo, con el detalle de actividades, responsables, etc., se observa en el anexo Nro. 4.

TABLA IV

Caracterización del seguimiento a los proyectos de investigación científica

PROVEEDOR	ENTRADAS	PROCESO	SALIDA	CLIENTES	INDICADOR
Jefatura de Investigación Jefatura Financiera Coordinación de los Centros de Investigación, Innovación y Transferencia Tecnológica (CIITT) Director del Proyecto de Investigación	Listado de proyectos de investigación aprobados Recursos a ser ejecutados	Procedimiento de Seguimiento a los Proyectos de Investigación científica	Informes de ejecución y avance de proyectos Informe de cierre de proyectos	Comunidad: El desarrollo de la función sustantiva de investigación permite dar solución a los problemas de la misma. Docentes Estudiantes	Porcentaje de proyectos que han cumplido con los hitos de las actividades contempladas en su planificación

Con la implementación de los procesos en la UC, y en base a las debilidades encontradas en los procesos de evaluación externa, se logró organizar y ordenar las actividades para la construcción del Plan Estratégico de Desarrollo Institucional (PEDI), el cual contempla el fortalecimiento del eje de investigación. A partir del PEDI se elabora un plan de investigación que guarda concordancia con los dominios académicos, líneas y sublíneas de investigación institucionales y la oferta académica tanto de grado como de posgrado.

Lo indicado anteriormente condujo a la revisión y actualización de la normativa para el desarrollo de los proyectos y programas de investigación, teniendo así un marco legal para el accionar de las partes involucradas. Se detectó la necesidad de definir funciones, jerarquías, procedimientos, recursos y mecanismos de coordinación, debido a la presencia de obstáculos observados y conflictos a la hora de generar la gestión.

Concomitante a ello, desde las autoridades universitarias se define e implementan políticas acadé-

micas que garantizan el desarrollo de la investigación en la UC. Entre las más importantes, está la asignación de una carga horaria adecuada a los docentes, para el desarrollo de los proyectos de investigación en los que se encuentran inmersos.

Adicional a lo descrito, se definen y ejecutan procesos de formación de docentes tanto en maestría como en doctorados, y se desarrollan programas de capacitación sobre metodologías de investigación y escritura académica, que permiten a los docentes incrementar su producción per cápita a nivel de publicaciones.

Los procesos son revisados en torno a los resultados obtenidos y en base a ello se actualizan teniendo en cuenta la eficacia y eficiencia de los mismos, buscando la mejora en la agilidad de la gestión y la obtención de nuevos niveles de calidad.

En cuanto a los resultados, se pueden observar las siguientes gráficas del número de docentes y las publicaciones.

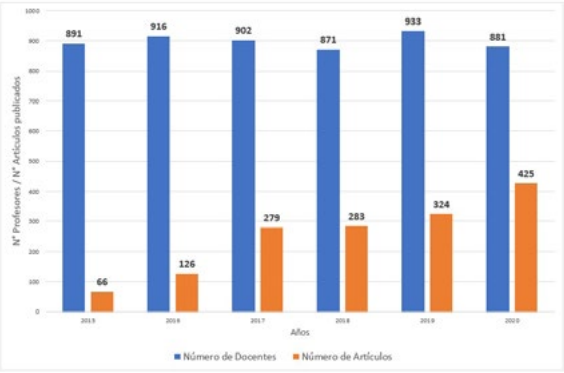


Figura 3: Histograma de resultados de la producción científica: Número de Profesores y de artículos publicados anualmente en revistas científicas en el período comprendido entre los años 2015 al 2020

Adicionalmente, en función de la implementación del SGC y la incorporación de políticas que favorecen los resultados de la investigación, la tasa de producción científica per cápita de los docentes ha subido significativamente. La ecuación utilizada para determinar la producción per cápita es la siguiente:

$$[1]\ TPCPC = \frac{NP}{NTD},$$

donde:
TPCPC: Tasa de producción científica per cápita.
NP: Número de publicaciones.
NTD: Número total de docentes.

La figura 4 muestra la cantidad TPCPC determinada por la ecuación (1) calculada anualmente para el período comprendido entre 2015 y 2020.

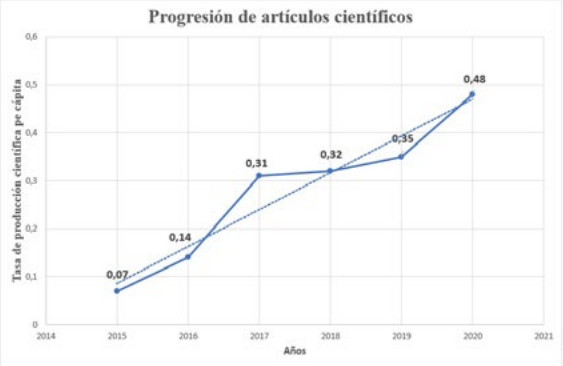


Figura 4. Tasa de producción científica per cápita, Ecuación (1) calculada anualmente en el período 2015-2020.

Conclusiones

La implementación de un SGC en la Universidad Católica de Cuencs ha permitido mejorar significativamente los indicadores en el eje de investigación, lo que asegura y garantiza la calidad de dicha función sustantiva, además la institución ha logrado la acreditación y el reconocimiento de parte de los organismos de evaluación y control en Ecuador en el año 2020. En relación a la producción se evidencia un crecimiento considerado y sostenido en el transcurso del tiempo.

La identificación y la documentación de los procesos en el eje de investigación ha permitido la consecución de objetivos concretos para cada una de las dimensiones: planificación, ejecución y resultados; los mismos que son coherentes con el Plan Estratégico de Desarrollo Institucional, el Plan de Investigación, la Política de Calidad de la UC y los indicadores diseñados para los procesos.

Estandarizar y sistematizar procedimientos con el propósito de asegurar altos niveles de calidad ha constituido el involucramiento de las autoridades, del personal docente y administrativo, fomentando su interacción y contribución positiva, sentido de pertinencia y mayor motivación.

Del análisis efectuado, se observa un crecimiento y una tasa de producción científica per cápita del año 2015 de 0.07 a 0.48 para el año 2020, con un promedio del número total de docentes de 899 en el período de estudio.

La calidad para las instituciones de educación superior se ha convertido en una filosofía institucional, no sólo desde el punto de vista del reconocimiento de la sociedad, sino desde la sostenibilidad y la garantía de cumplir el legado de responsabilidad social orientada a la generación de conocimientos y la resolución de problemas del entorno.

La estructuración y normalización de los procesos de investigación, y la mejora que ha sido evidenciada en la presente investigación, motiva a realizar investigaciones futuras sobre la incidencia de la implementación de los SGC en los indicadores y resultados de las funciones sustantivas de docencia, vinculación con la sociedad, y condiciones institucionales.

Agradecimientos

Emitimos un agradecimiento especial a Ing. Leopoldo Pauta, decano de la Unidad Académica de TIC, al Dr. Enrique Pozo Cabrera, Rector de la Universidad Católica de Cuenca por su liderazgo y apoyo constante en la implementación y mejora del SGC, y orientación a un modelo de gestión por resultados (GPR), Y Al Ing. Pedro Álvarez Guzhñay Supervisor de Calidad de la Universidad Católica de Cuenca por su ayuda para la realización de la presente investigación.

Referencias

[1] G. J. ALARCÓN, P. I. ALARCÓN y S. E. GUADALUPE, «La elaboración del mapa de procesos para una universidad ecuatoriana,» *ESPACIOS*, vol. 40, nº 19, pp. 4-18, 2019.

[2] E. E. Orozco Inca, A. I. Jaya Escobar, F. J. Ramos Azcuy y R. M. Guerra Bretaña, «Retos a la gestión de la calidad en las instituciones de educación superior en Ecuador,» *Educación Médica Superior*, vol. 34, nº 2, p. 14, 2020.

[3] W. ROJAS Preciado, L. B. CAPA Beníte y M. E. SÁNCHEZ Cuenca, «Complementariedad del sistema de gestión de la calidad (SGC) de la educación superior ecuatoriana y el SGC ISO 9001,» *ESPACIOS*, vol. 40, nº 2, p. 19, 2019.

[4] Consejo de Educación Superior (CES), «LEY ORGANICA DE EDUCACION SUPERIOR, LOES,» Quito - Ecuador, 2018.

[5] D. Acuña, C. Romero y D. López , «SISTEMA INTEGRAL DE GESTIÓN DE CALIDAD EN LA UNIVERSIDAD DE LA,» Telos, Maracaibo, 2016.

[6] S. Moscoso Bernal, E. Pozo Cabrera, A. Cañizares Medina y P. Álvarez Guzhñay, Modelos de Autoevaluación, Cuenca - Ecuador: Centro de Esrudios Sociales de América Latina CESAL, 2021.

[7] J. Alvarez, J. Fraiz y M. Del Río, «Implantación de un sistema de gestión de la calidad: beneficios percibidos.,» *Revista Venezolana de Gerencia*, pp. 379-407, 2013.

[8] A. Ortiz Pérez, Procedimiento para la implantación de un sistema de gestión en universidades. Aplicación en la Universidad

de Holguín (Master's thesis, Universidad de Holguín, Facultad de Ciencias Empresariales y Administración, Departamento de Ingeniería Industrial)., 2013.

[9] Fundación Europea para la Gestión de la Calidad (EFQM), «Modelo EFQM de Excelencia y Calidad en la gestión empresarial,» 2019. [En línea]. Available: http://www.efqm.es/.

[10] CACES, Modelo de Evaluación Externa de Universidades y Escuelas Politécnicas 2019., Quito: Consejo de Aseguramiento de la Calidad de la Educación Superior., 2019.

[11] Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior del Ecuador(CONEA), «Informe de Evaluación de Universidades,» CONEA, Quito, 2012.

[12] Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad en la Educación Superión (CEAACES), «Informe de Evalaución de Universidades y Escuelas Politécnicas,» CEAACES, Quito, 2014.

[13] Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior (CEACES), «Informe de Evaluación Universidad Catolica de Cuenca,» CEAACES, Quito, 2016.

[14] Universidad Católica de Cuenca (UCACUE), «Manual de Procesos Misionales,» Cuenca - Ecuador, 2019.

[15] Consejo de Aseguramiento de la Calidad de la Educación Superior (CACES), «Informe de Evaluación Universidad Catolica de Cuenca,» CACES, Quito, 2020.

[16] Universidad Católica de Cuenca (UCACUE), «MANUAL DE USO DEL SISTEMA ERP UNIVERSITY,» Cuenca - Ecuador, 201.

[17] ISO, «Norma ISO 9001:2015,» ISO, 2015.

[18] ISO TOOLS, «ISO TOOL EXCELLENCE,» Abril 2021. [En línea]. Available: https://www.isotools.org/2017/03/30/iso-21001-nuevo-estandar-sistema-gestion-organizaciones-educativas/.

[19] S. Moscoso Bernal, E. Pozo Cabrera, P. Álvarez Guzhñay y L. Pauta Ayabaca, «Implementation of quality management systems as proposal towards academic quality. Case study: Universidad Católica de Cuenca,» *International Symposium on Engineering Accreditation* (ICACIT), 14 Mayo 2018.

[20] Universidad Católica de Cuenca (UCACUE), «Universidad Católica de Cuenca,» Jefatura de Acreditación y Aseguramiento de la Calidad, 2020. [En línea]. Available: https://www.ucacue.edu.ec/ejes/administrativo/acreditacion-y-aseguramiento-de-la-calidad/. [Último acceso: 2021].

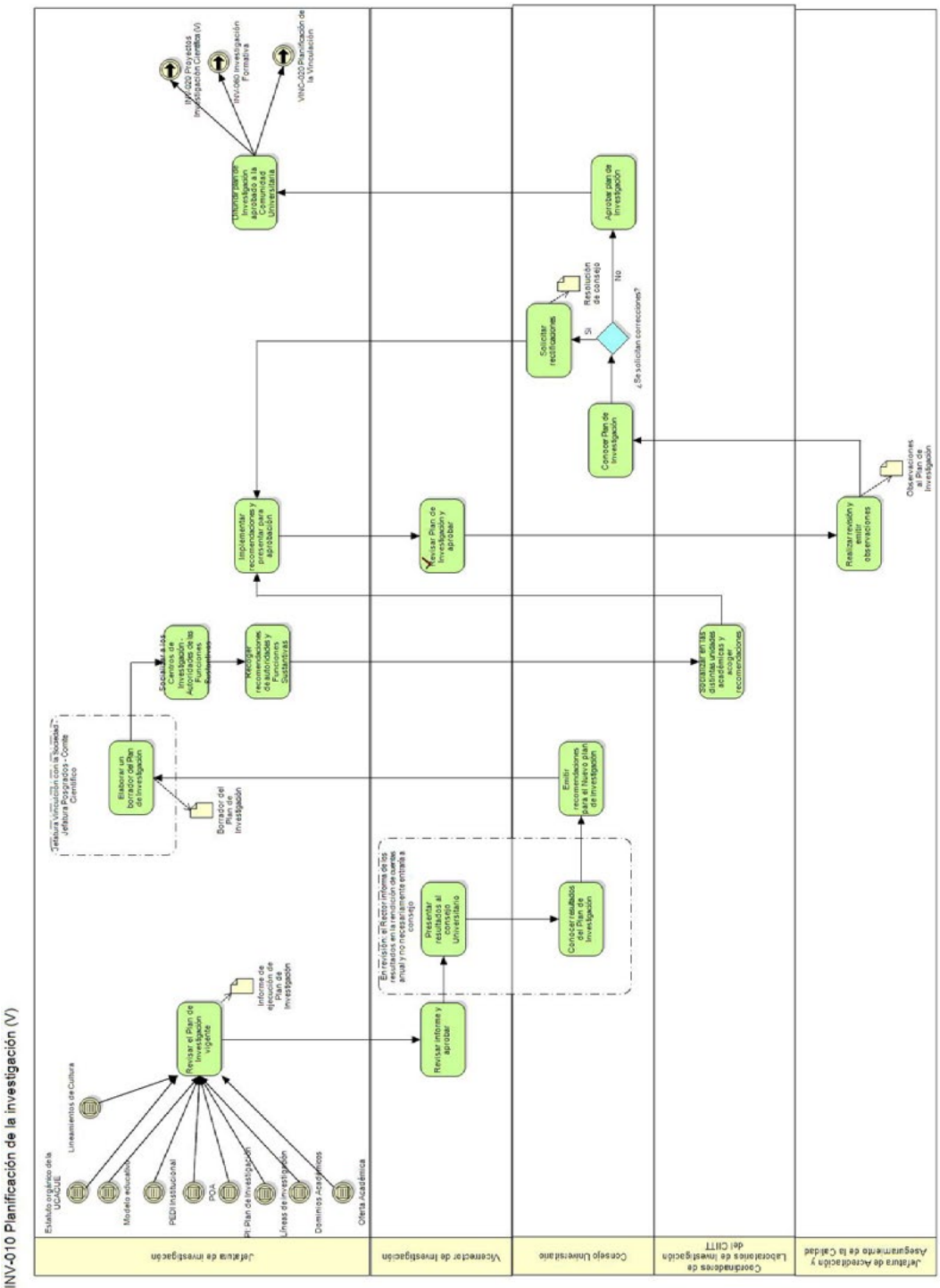
[21] J. Saravia, Y. Eguigure y M. Méndez, «La Pertinencia de la Oferta Académica de la Carrera de Educación Tecnológica en la Universidad Pedagógica Nacional Francisco Morazán,» *Paradigma> Revista de Investigación Educativa*, vol. 39, pp. 11-30, 2018.

[22] Universidad Autónoma de Nuevo León, «Modelo Académico a Nivel Superior,» UANL, México, 2008.

[23] DATADEC, «GESTIÓN DE CALIDAD Y GESTIÓN POR PROCESOS,» 13 Noviembre 2017. [En línea]. Available: https://www.datadec.es/gestion-de-calidad-y-gestion-por-procesos. [Último acceso: 11 Enero 2022].

Anexo 1.

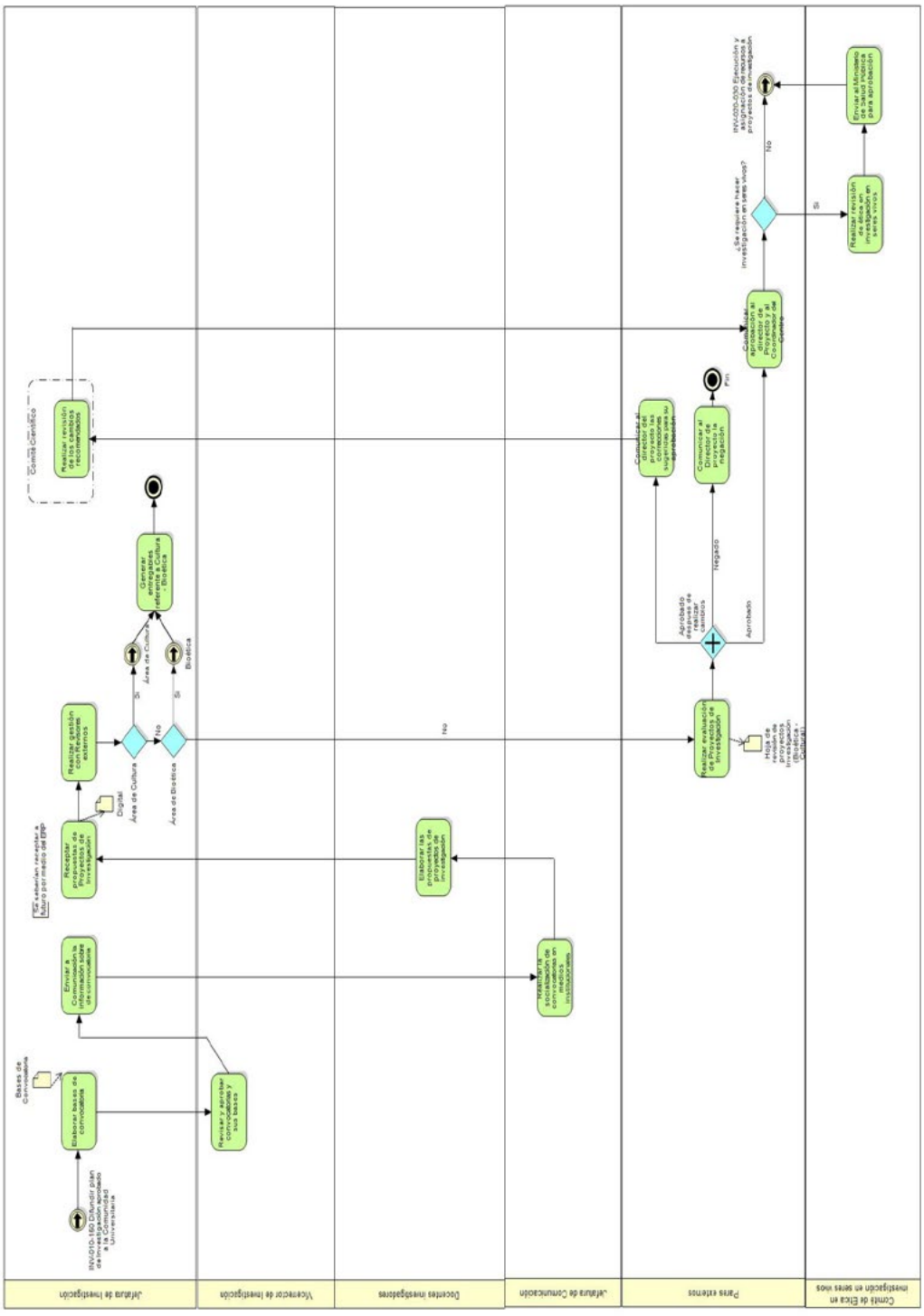
Procedimiento: Planificación de la investigación.



Nota: *Fuente: SGC UCACUE.* https://www.ucacue.edu.ec/ejes/administrativo/acreditacion-y-aseguramiento-de-la-calidad/

Anexo 2.

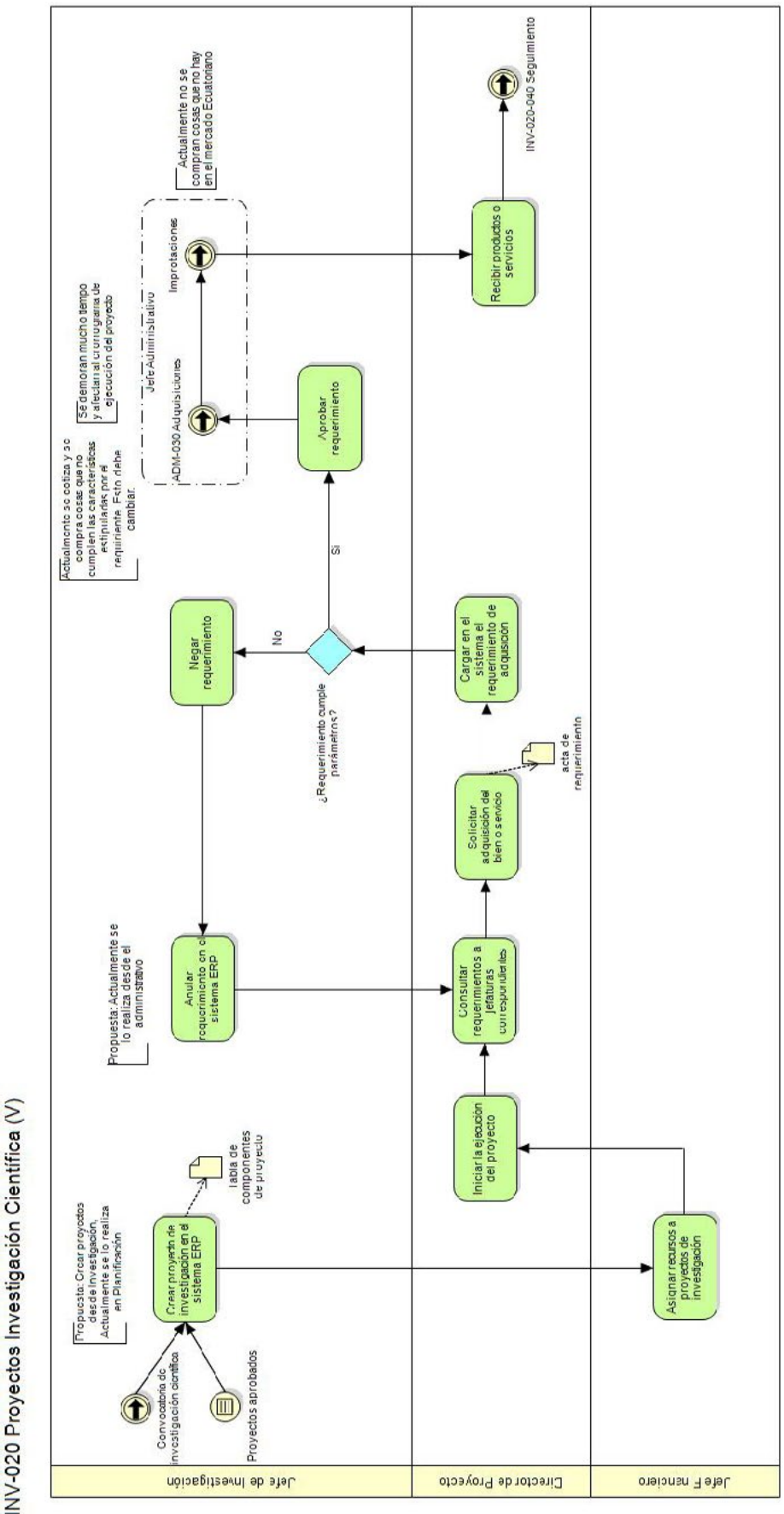
Subproceso de convocatoria de investigación científica.



Nota: *Fuente: SGC UCACUE.* https://www.ucacue.edu.ec/ejes/administrativo/acreditacion-y-aseguramiento-de-la-calidad/

Anexo 3.

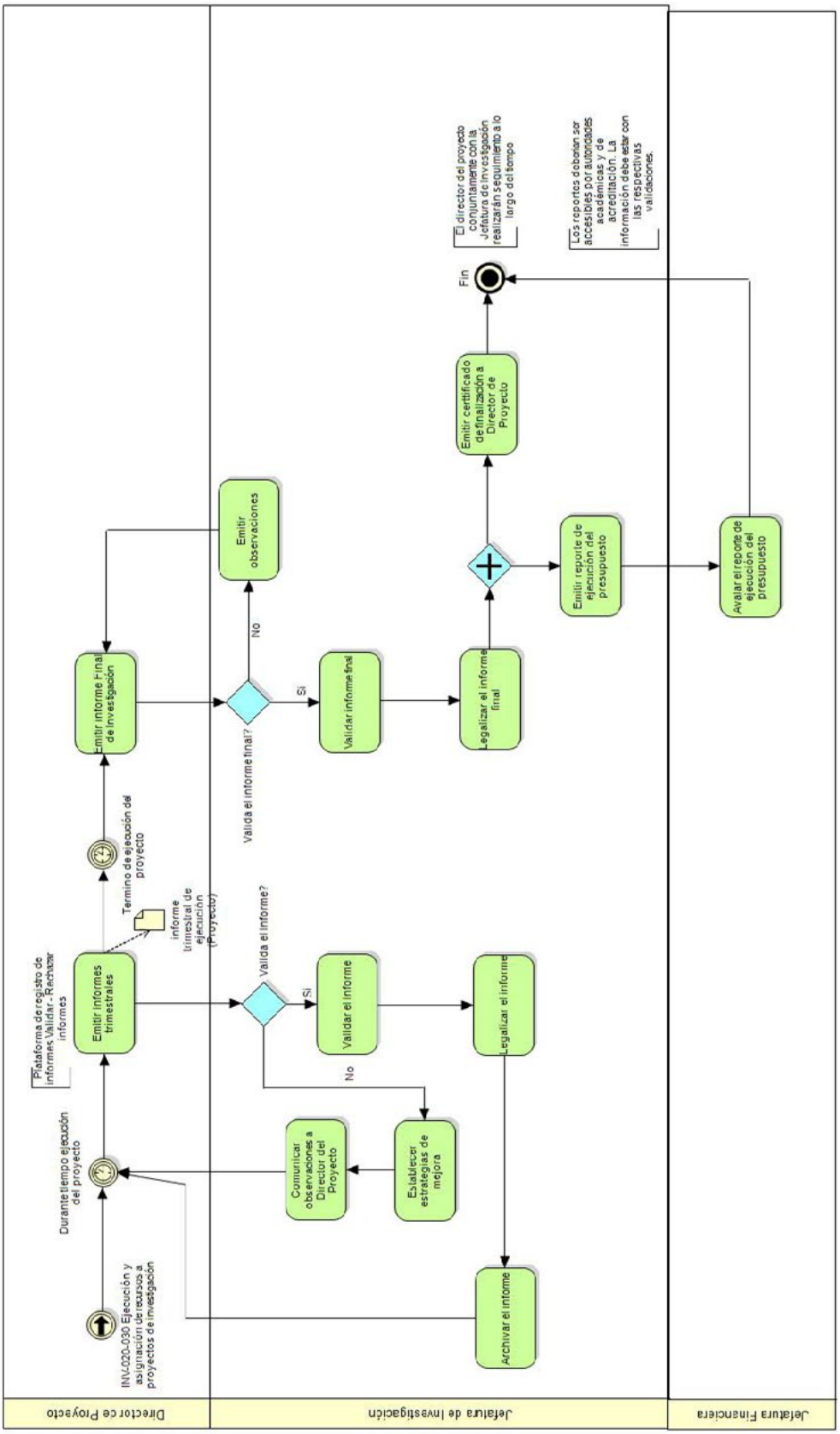
Subproceso de ejecución y asignación de recursos.



Nota: *Fuente: SGC UCACUE.* https://www.ucacue.edu.ec/ejes/administrativo/acreditacion-y-aseguramiento-de-la-calidad/

Anexo 4.

Subproceso de seguimiento de investigación científica.



Nota: *Fuente: SGC UCACUE.* https://www.ucacue.edu.ec/ejes/administrativo/acreditacion-y-aseguramiento-de-la-calidad/

Recibido: *10 de enero de 2022*
Aprobado: *31 de enero 2022*

Santiago Arturo Moscoso Bernal

Ingeniero Eléctrico y Especialista en Docencia Universitaria por la Universidad Católica de Cuenca, Magister en Aprendizaje de la Física por la Universidad Nacional de Chimborazo, Magister en Energías Renovables por la Universidad Europea del Atlántico (España), egresado de la Maestría en Gerencia de la Calidad por la Universidad Internacional del Ecuador (UIDE), candidato a Doctor del Programa de Doctorado en Ingeniería Industrial de la Universidad Nacional del Cuyo, Auditor internacional ISO 9001:2015, Par evaluador certificado para el Consejo de Aseguramiento de la Calidad en el Ecuador (CACES), Docente titular de la Universidad Católica de Cuenca, docente invitado de programas de posgrado, Jefe de Acreditación y Aseguramiento de la Calidad de la Universidad Católica de Cuenca.

● ● ●

Raymundo Quilez Forradellas Martinez

Doctor Ingeniero, Programa de Inteligencia Artificial en la Universidad Politécnica de Madrid, Post Doctorado, Programa I+D Torres Quevedo del Ministerio de Ciencia y Tecnología de España, Ingeniero en Telecomunicación, Ministerio de Educación y Ciencias de España, - Ingeniero en Electrónica, Universidad Tecnológica Nacional, FR Buenos Aires, Profesor Titular Ordinario Efectivo en la Universidad Nacional del Cuyo y la Universidad Nacional de San Juan, Profesor y Coordinador del, Área Informática Industrial en el Posgrado Master de Logística Industrial, Director del Doctorado en Ingeniería Industrial, Investigador Acreditado Categoría I, en el Programa Nacional de Incentivos, autor y coautor de múltiples artículos de investigación, director de tesis de carreras de grado, programas de maestría y de doctorados.

Jaime Tinto Arandes

Economista-Universidad de Los Andes- Venezuela. Especialista en muestreo y control Centro Investigación Estadística Chile-OEA. Msc. en Empresariales y Dr. en Ciencias Económicas y Empresariales de la Universitat de Barcelona- España. Coordinador de Centro de Investigación de Ciencias Económicas y Sociales, y de la Red de Investigación y Observatorios de la Universidad Católica de Cuenca (RIOUC). Ha ejercido como Profesor de Pregrado, Postgrado y Doctorado en la Universidad de Los Andes. Profesor Titular Principal de Pregrado y Posgrado en la Universidad Católica de Cuenca.

● ● ●

Orlando Alvarez Llamoza:

Magister y Dr. en Física Fundamental. Tiene más de 20 años de experiencia universitaria. Ha realizado investigaciones computacionales y teóricas en sistemas complejos, dinámica no lineal, física estadística, y aplicaciones interdisciplinarias, cuyos resultados se ven reflejados en más de 20 publicaciones en revistas indizadas. Profesor Titular Principal, Coordinador de Laboratorio de Cálculo Computacional, Modelado y Analítica de Datos del CIITT, Universidad Católica de Cuenca.

● ● ●

Henry Paul Cabrera Vintimilla

Magister en Investigación Integrativa en la Multiversidad Mundo Real Edgar Morín - México, Master in Integrative Research in the California University - EEUU, Egresado de la Maestría de Gerencia de la Calidad e Innovación España, Cursando el Master de Administración de Empresas Universidad Católica de Cuenca, Diplomado en Sistemas de Gestión de Calidad ISO 21001 Colombia, Auditor Internacional ISO 9001, Ingeniero de Sistemas, Responsable de Auditoria del SGC de la Universidad Católica de Cuenca.

Artículo de Investigación. Revista Killkana Técnica. Vol. 6, No. 1, pp. 21-30, enero-abril, 2022.
ISSN 2528-8024. ISSN Elect. 2588-0888. Universidad Católica de Cuenca

Architectural Neurology: Is It Possible To Design Architecture Through Emotions?

Ana Carolina López[1,2]

[1] University of Melbourne
[2] Universidad Regional Amazónica-Ikiam

* Ana.lopez@ikiam.edu.ec
DOI: https://doi.org/10.26871/killkanatecnica.v6i1.931

Abstract

This paper aims to propose implementing an innovative digital system for architectural design. This new method, based on the interpretation of human emotions for music composition, and the analysis of dreams, will be able to translate images based on architects' memories, emotions, and learning to design architectural spaces. If this system can build, how will it affect architectural design? Different investigations, studies, and analyses are needed to support and answer this thesis. The invention of a system for musical composition in London, based on the analysis of neural impulses and brain waves; the comparison between the process used for musical composition and architectural design through the explanation of renowned musicians and architects' methods; and the study of dreams through brain wave analysis would provide with results and possible benefits for a more straightforward method to design architectural areas. This implementation

will offer three benefits: accelerate the design process, automatically associate images and concepts, and have a pure and natural architectural design. Also, the system, capable of linking different images, concepts, emotions, and experiences, would provide various options of spaces produced by the architect. However, understanding that technology will keep advancing with time, human being labor is always needed to refine the method. An architect would be needed to define and choose between the different options of spaces that the system produced.

Keywords: *Brainwave, Emotions, Spaces, Technology*

Introduction

Technology can bring numerous benefits for improving the quality of life, improving processes, defining strategies for things conceived impossible, and mixing methods from different faculties to create innovative systems. Using the analysis and studies produced by professionals through technology discoveries would offer us possibilities to propose improvements in the different faculties. In this case, this document will study the possible implementation of an innovative digital system for architectural design. Applying this innovative method, based on the interpretation of human emotions for music composition and the analysis of dreams, would provide us with possible benefits to ease the process to design architectural areas.

Musical neurology: brainwave analysis

A revolutionary system of musical composition was created in London, which analyses neural impulses and brain waves for musical composition [1]. The brain-computer musical interface (BCMI) creates music in response to the brain's electrical impulses. The part of the brain that is analyzed is where the person can find brain waves produced through emotions. Emotions will depend on the activity of the different senses. Eduardo Miranda, a composer and computer music specialist at the University of Plymouth in the United Kingdom who participated in developing the system, created a sequence of patterns on a screen for the development of the study [1]. This programming consisted of a sequence of specific points based on colors, different patterns, and repetition to activate neuronal movement [2]. Thus, the outcome is a musical composition based on experience and emotion.

Figure 1: Subject's test [11].

This method of composing music is essentially digital and has been named "listening to the Symphony of Minds" [3]. Miranda uses a brain hat as the primary tool for his study, filled with electrodes and wires, picking brainwave visual cortex and ruling out any noise in the background to create music. The computer analyzes the

brainwave movement and sends them to another device that transforms this movement into musical notes [1]. Finally, this information is sent to a piano, which makes the sound created by the movement of the analyzed brain waves.

Miranda's study aimed to help disabled people through music. This way, music would be their therapeutic method. The development of brain-computer interfaces (BCI) allows users to control computer functions with the mind. These interfaces are generally based on the user's ability to learn certain mental states that brain-scanning technologies can detect. Miranda and his colleagues have used electroencephalography (EEG), one of the oldest of these systems: the electrodes in the skull for weak neural signals [2]. EEG signals can be processed quickly, enabling rapid response. Is it possible to use a similar method to create architectural designs through the study and analysis of emotions?

Musical composition and architectural design: musical composition

Musical composition and architectural design are related in several ways. Both are based on structure, dependent on the mathematics use, rhythm, context, culture, repetition, hierarchy, but primarily relying on emotions. On the one hand, we have the musical composition. There are different tools and methods which depend on the artist. For example, Beethoven used a technique based on repetition patterns to create the effect of predictable vs unpredictable. The unpredictable part became the song's climax and was its end [12]. The repetition and patterns part is called anticipation. Whereas, the part where the climax arrives, in architectural language the hierarchy, is called experience [4]. People who listen to Beethoven's songs choose this part as their favorite because they remember it due to its climax.

Stephanie Khalfa, a neuroscience researcher, analyzes the different emotions created by music, and vice versa, how emotions influence music composition [11]. She investigates several artists' musical composition processes according to their emotions. After analyzing several artists, she concludes that: Music consists of a finite set of parameters that can be arranged in different ways, following predefined rules [5]. These parameters are tempo, patterns of stress-relaxation, tone, intensity or volume. Music characterized by a fast tempo and a major key is associated with positive emotions, while music with a slow and minor key often causes negative responses [6].

Musical composition and architectural design: architectural design

On the other hand, there is architectural design. There are many methods, styles, tools and concepts for architectural design. For some architects, landscape, context, functionality, or structure would be the most important thing for the project. However, some architects focus on emotions to convey sensations and feelings [7]. One of them is the Mexican architect Luis Barragán, winner of the Pritzker Award, who focused the meaning of all his work on emotions [7]. As well as music composition, emotions would be involved in both the process and work outcome; this experience would be generated from users. Barragán manages to convey and be influenced by emotions through light and shadow effects, different materials, colors, and water, but above all, he focuses on photographic architecture [7]. Using these tools, he transmits his emotions in every space, strategically connecting them up to the main space, the garden (climax/ hierarchy).

Figure 2: Luis Barragan's Emotional Architecture [7].

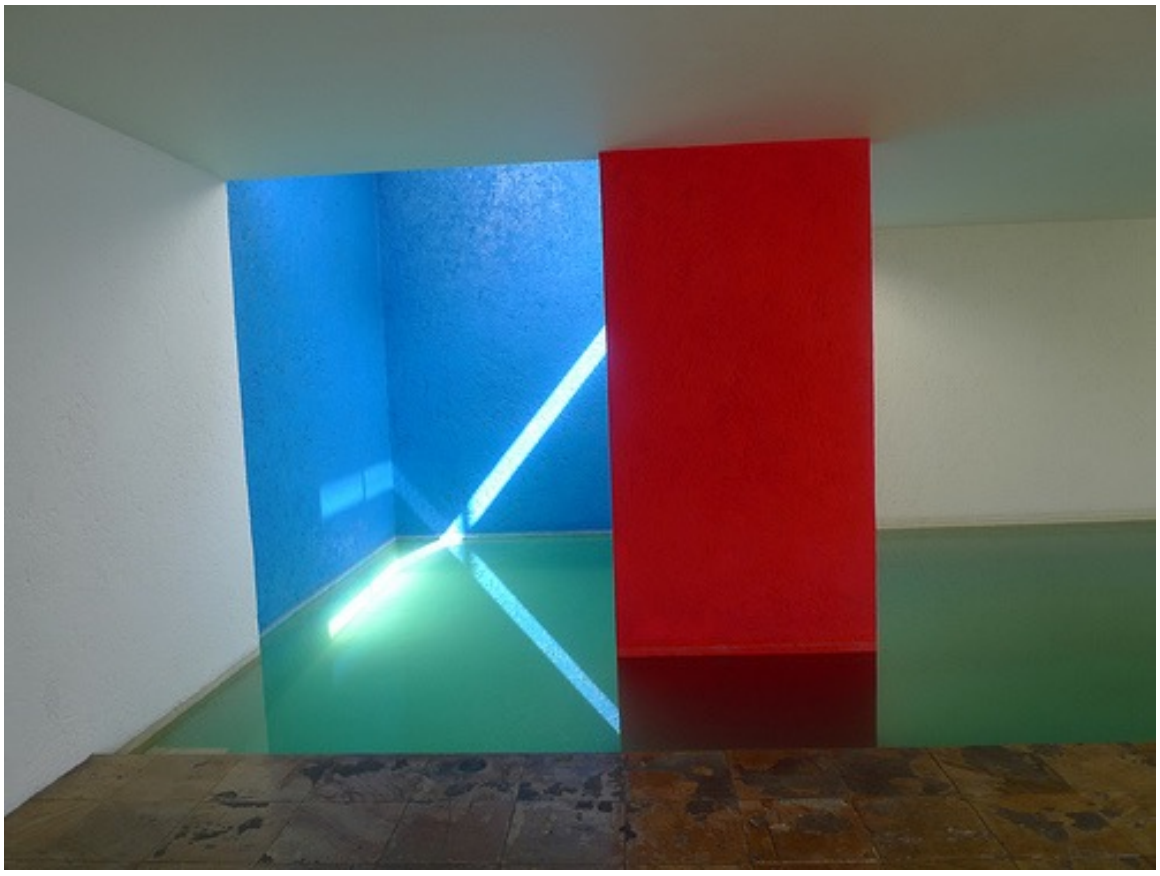


Figure 3: Luis Barragan's Emotional Architecture [7].

Architects usually begin their design with one sketch based on one or more images of their imagination. However, these sketches are only translated into lines and perhaps colors. Architects locate themselves in a specific scenario depending on the context and site of the project [8]. Thus, they focus on people's emotions, sensations, and movements inside and outside the establishment. Of course, for each person, the meaning will be something different, but the essence and meaning of each space will be the same. Architectural design is based on a concepts' compilation and preconceived images of different styles, shapes, materials and traditions, customized and manipulated by the architect to transmit the project's main idea [8].

Musical composition and architectural design: comparison between architectural design and musical composition

Currently, music composition and architectural design can be transmitted digitally. However, lots of information is lost during the process and is difficult to recover [12]. There are many emotions involved in composing music, and they vary through time quickly. That is why it has been so difficult for artists to compose in a completely natural way. This system has proved that a person can compose while his or her emotions are manifesting [5]. In architecture, architects make their sketches, but they miss many details from the original idea. That is because the images and emotions also vary with time. What would happen if a new system could translate the architects' images and emotions to design spaces?

Architects work with a photographic memory, so their designs are translations of the images they have in mind. The images stored inside their minds result from their past and daily experience [8]. Thus, the combination of these illustrations will be a personalized design in its details and global in its conformation. For example, Aldo Rossi's design method was collage [8]. He gathered some images, both past and current works, to organize all the information in his mind. Given the physical tools and preconceived experience, a space containing history, experience and emotions can be designed with a better approach [8].

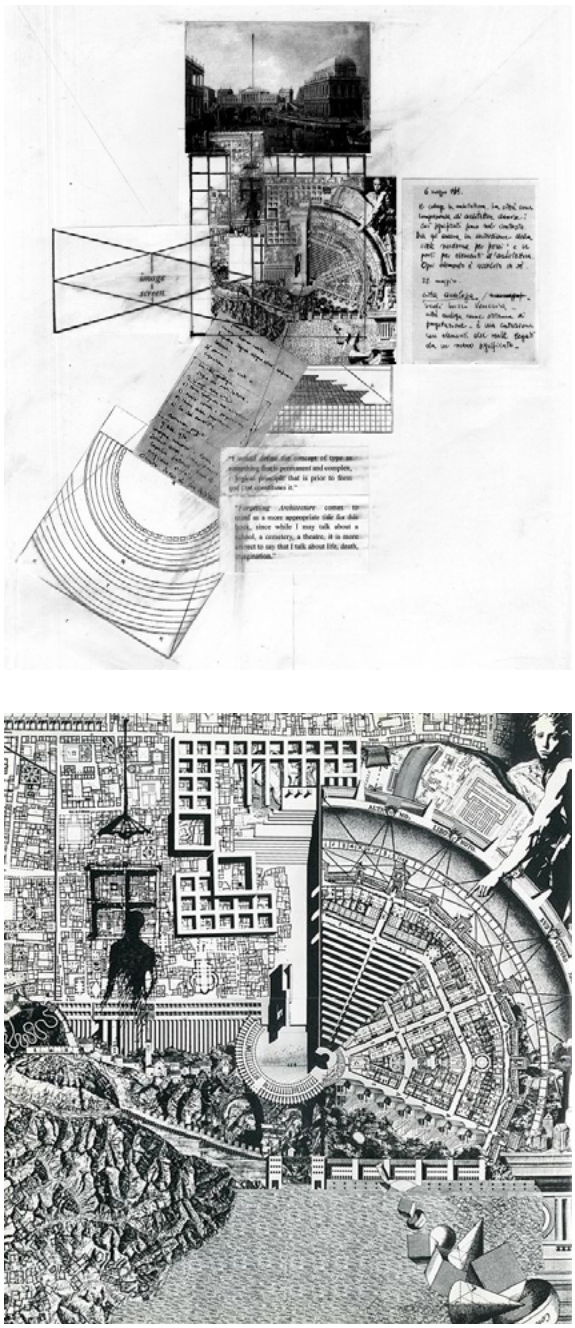


Figure 4: Aldo Rossi's design method (collage) [8].

Dream analysis: brain wave interpretation of dreams

In contrast, Jack Gallant, psychologist and professor of neuroscience at UC Berkeley, executed a study about dreams [9]. The analysis consisted of a brain wave analysis of volunteers while watching videos and images, followed by these projections' dreams' analysis. As a result, specific image associations appeared based on color, light, shadow and lines. Of course, these images consisted of not defined, blurry elements and were customized by each subject. It means that each person had certain detailed changes in the dream composition, such as the colors, the inclination and the size of the object or person in the video [9]. Thus, it can be confirmed that it is possible to convey people's emotions taking into account the experience and preconceived knowledge about various topics [9].

Figure 5: Jack Gallant's dreams study (Real video vs. subject's dream) [9]

Architectural neurology: system functionality

The proposed specialized software would be based on the concepts used in both Miranda's emotion interpretation and Gallant's dream analysis. The mixture of these two analysis methods gives us several results in an easier way to design architectural spaces. By interpretation, not only of brain waves but also of past, current and imaginative images, it could produce patterns of ideas translated into architectural spaces. These patterns will be recognized by connecting images projected in the head according to the emotions architects feel at the time. As mentioned above, architects usually locate themselves in an imaginary scenario before designing to recognize the emotions they wish to transmit with the project. Inside human memory, conscious and unconscious, specific elements call or call our attention in our lives the "climax" of important events. This system will collect and connect repetitive elements of the projected images. Thus, the system can provide various options of spaces produced by the architect. For example, the system can recognize that a Doric, gray or concrete column or a square window with a white frame is repeated in several images. These elements will be introduced to one of the final images of produced spaces. As a result, several

scenarios would be composed of different patterns: colors, materials, shapes, sizes, among others.

The machines that would make this possible would analyze the brain waves by separated processes, sharing the same space. First, as Miranda did, computers would analyze brain waves, tones, intensities, and variations. In this way, a specialized staff may make associations to analyze emotions. Then, there would be computers, which project images of architects' dreams, as in Gallant's studio. Finally, a person will guide architects to help them move within the project. After this process, the system would connect patterns using the information from both studies to produce several possible images for the different areas of a project.

Architectural neurology: architectural neurology benefits

Imagining that a system capable of linking different images, concepts, emotions and experiences to design an architectural space can be created, it could provide several benefits for architects. One benefit is accelerating the design process, so once architects have a defined image in their minds, it will automatically transform it into a digital form. It would save time on the production and design process. In addition, no information would be lost while the image is in their mind. Thus, the system will calculate Aldo Rossi's method, which puts together a collage of past and current images and experiences. The result would not be only one outcome but several. Just as Augustine Wing [10] states in his article, comparing technology with physical and social life, the person, in this case, would need to choose one result due to the most appropriate solution for their design.

The second benefit, related to the previous one, would be having an automatic association of images and concepts, which will depend on the memory and the changes within the architects' brain waves due to their emotions [9]. As previously mentioned, emotions are measured through brain waves, which can be identified especially through strong emotions, for instance, fear, happiness, loneliness, sadness, among others [11]. Similarly, as emotions can be recognized through the tone and speed of the music, in architecture, they can be associated with certain emotional spaces. For example, fear can be associated with a dark space. In contrast, happiness can be recognized by a bright and bold colors space. Sadness could identify using a neutral space with no color or contrast. There are several emotions a space can perceive, but not necessarily all people would identify themselves with that association.

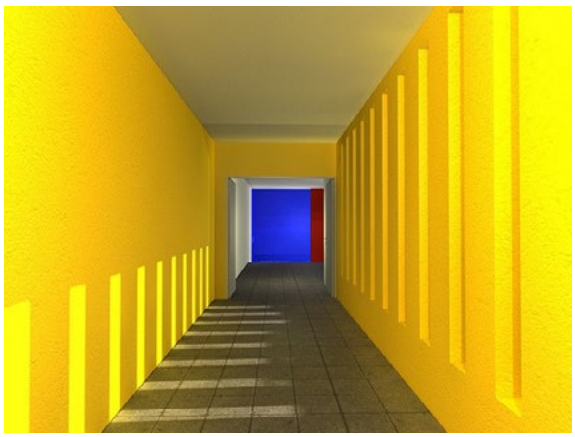


Figure 6: Emotions in spaces [7].

Figure 7: Emotions in spaces (happiness vs. loneliness), Emotional Architecture [7].

The third advantage is to produce a more sustainable, ecological, adaptive and resilient design and design process. Augustine Wing in "Automated Ecologies" [10] compares sustainability in architecture and urbanism with the micro-ecology of Amazon's automated warehouses. The document states that contemporary Architecture and Urban designs created by computers automatized machine intelligence have not engaged with social and physical environments. According to Wing's analysis, which gives an ecological view about the material and immaterial of machines' intelligence working in Amazon warehouses, this proposed new system will be considered eco-friendly. The term 'ecological` is based on the intersection between the digital and the physical world, as Wing states [10]. This system will give the same importance to the two physical and digital areas to merge them for an efficient result.

Finally, the fourth advantage is to have a pure and natural architectural design. The project will contain not only a physical and structured part but will also have a sensitive side. Our brain's image and experiences collection is organized hierarchically [5]. Just as in music, where we can recognize a song by its climax, our images and experiences are rated equally [9]. The most important memories in our mind would be those capable of awakening our emotions [7]. Therefore, the designed spaces will contain the most relevant information of our brain.

Conclusion

Concerning Wing's analysis in "Automated Ecologies" [10], the essential intersection is the relationship between space and time. The proposed new system will save time in the space design process and the required staff to achieve it. In addition, the design will be more ecological, natural and direct; this is cleaner and purer. However, human being intervention is always needed to refine the method. In Amazon warehouses today, the staff is needed to control and order the items in the factory. Similarly, for the new method, an architect is needed to define and order the different options of spaces that the system produced.

Technology will continue to advance over time. New technologies and operating systems will continue to try inventing machines to save time and personnel and improve processes. Regarding architecture, computer intelligence is increasing in the creation process. In this regard, Wing states: "In an age where space production is more intertwined to computation, negotiating complexity with a greater appreciation of the potential of intelligent machines will present unique opportunities not just for architectures "thinking, dreaming" but also its realization and habitation. What is certain is that intelligent machines are here to stay and will play a critical part in the evolution of the myriad ecologies of the post-digital condition" [10]. Further, human beings will always be part of technological advances.

Considering how technology advances, a system of this type could be built. This system could exist with some calculations, new technologies, applied theories, and studies. If this software can finally be made, the architectural designs will be promising. The only doubts we might have would be; can emotions from one space be transmitted to the people who inhabit it? Can anyone, regardless of profession, design architecture with this system? Can this system produce emotional patterns to design spaces by itself?

Bibliography

[1] M. Knight, "CNN México," 29 March 2011. [Online]. Available: http://edition.cnn.com/2011/TECH/innovation/03/29/music.brain.power.therapy/index.html. [Accessed 6 October 2014].

[2] R. LJ, "BBC News," 10 February 2014. [Online]. Available: http://www.bbc.co.uk/mundo/noticias/2014/02/140210_tecnologia_ondas_cerebrales_componer_musica_clasica_il. [Accessed 7 October 2014].

[3] E. Paz, "Eduardo Paz," 25 February 2014. [Online]. Available: http://eduardopaz.com/neurologia-musical-o-componer-musica-con-las-ondas-cerebrales/. [Accessed 4 October 2014].

[4] J. Lehrer, "Wired," 19 January 2011. [Online]. Available: https://www.wired.com/2011/01/the-neuroscience-of-music/. [Accessed 6 October 2014].

[5] Anne J. Blood, Robert J. Zatorre, "PNAS," 25 September 2001. [Online]. Available: https://www.pnas.org/content/98/20/11818. [Accessed 6 October 2014].

[6] Thomas Fritz, Sebastian Jentschke, Nathalie Gosselin, Daniela Sammler, Isabelle Peretz, Robert Turner, Angela D. Friederici, Stefan Koelsch, "Science Direct," 14 April 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0960982209008136. [Accessed 4 October 2014].

[7] C. Villanueva-Meyer, "Galenus," 15 January 2012. [Online]. Available: http://www.galenusrevista.com/La-arquitectura-emocional.html. [Accessed 4 October 2014].

[8] A. Rossi, 'An Analogical Architecture', Theorizing a New Agenda for Architecture: An Anthology of Architectural Theory 1965 – 1995, Princeton: Princeton Architectural Press, 1996.

[9] Y. Anwar, "Berkeley News," 22 September 2011. [Online]. Available: http://newscenter.berkeley.edu/2011/09/22/brain-movies/. [Accessed 6 October 2014].

[10] A. Wing, 'Automated Ecologies', Towards an Adaptive Ecology of Mind, Material and Intelligent Machines in Architecture?, International Kindle Paperwhite, 2014.

[11] Alejandra Sel, Beatriz Calvo-Merino, "neurologia.com," 1 March 2013. [Online]. Available: http://www.neurologia.com/pdf/Web/5605/bj050289.pdf. [Accessed 4 October 2014].

[12] M. Mina, "Univisión Noticias," 6 November 2011. [Online]. Available: https://www.univision.com/explora/la-musica-y-el-cerebro. [Accessed 7 October 2014].

Recibido: *10 de enero de 2022*

Aprobado: *31 de enero 2022*

Artículo de Investigación. Revista Killkana Técnica. Vol. 6, No. 1, pp. 31-42, enero-abril, 2022.
ISSN 2528-8024. ISSN Elect. 2588-0888. Universidad Católica de Cuenca

Aplicaciones web modernas con stack MEAN: Un caso de estudio

Modern web applications with MEAN stack: A case study

Jaime Sayago Heredia[1], Fernanda Revelo Bautista[1]

[1] Pontificia Universidad Católica del Ecuador. Sede Esmeraldas, Sede Esmeraldas, Espejo y subida a Santa Cruz Casilla 08-01-0065, 0984787662,

* jaime.sayago@pucese.edu.ec
DOI: https://doi.org/10.26871/killkanatecnica.v6i1.989

Resumen

En la actualidad, las tecnologías como JavaEE estan presentes en la materia de desarrollo basado en plataformas de la Pontificia Universidad Católica del Ecuador, Sede Esmeraldas – Escuela de Sistemas y Computación y Tecnologías de la Información. La parte más crucial en un proyecto de desarrollo web basado en servicios REST es la elección de las herramientas correctas para el front-end, back-end y entorno de base de datos. El objetivo principal de esta investigación es presentar la arquitectura de aplicaciones web modernas basadas en el stack MEAN junto con

sus componentes e integración con otras tecnologías web y su comparación con la implementación del del stack JavaEE. Hemos realizado un análisis comparativo de la implementación de conformada por MongoDB (base de datos), Node.js. (servidor web), Express (back-end) y Angular (front-end). El resultado de la comparativa y el respectivo análisis de las herramientas seleccionadas servirán a los desarrolladores de software a realizar una mejor elección de la tecnología y la arquitectura adecuadas, en función de los requisitos de la aplicación que están desarrollando.

Palabras clave: *Arquitectura software, Javascript, REST, Servicio Web, Java EE.*

Abstract

Nowadays, technologies such as JavaEE are present in the different platform-based development courses of the Pontificia Universidad Católica del Ecuador, Sede Es-meraldas - School of Systems and Computing and Information Technologies. The most crucial part in a web development project based on REST services is the choice of the right tools for the front-end, back-end and database environment. The main objective of this research is to present the architecture of modern web applications based on the MEAN stack along with its components and integration with other web technologies and its comparison with the implementation of the JavaEE stack. We have performed a comparative analysis of the implementation of the MEAN stack consisting of MongoDB (database), Node.js. (web server), Express (back-end) and Angular (front-end). The result of the comparison and the respective analysis of the selected tools will help software developers to make a better choice of the appropriate technology and architecture, depending on the requirements of the application they are developing.

Keywords: *Software architecture, Javascript, REST, Web Service, Java EE.*

1. Introducción

Nuestra motivación para esta investigación basada en el análisis de las nuevas tecnologías JavaScript, es mejorar la materia de la carrera Tecnologías de la Información en la materia de desarrollo basado en plataformas y encontrar arquitecturas de software alternativas para la implementación una aplicación web moderna. El problema radica que al momento de elegir la arquitectura apropiada de tecnologías para desarrollo, integración y ejecución de aplicaciones web. La elección no es fácil, muchos parámetros tienen que considerarse en la base de datos, en el lado del servidor o el lado del cliente, etc. Diversos autores presentan a la stack MEAN como una solución [1] [2] [3]. JavaScript [4]ha ganado una creciente popularidad en el de unos pocos años, lo cual es una hazaña en sí misma. El lenguaje JavaScript es compatible con la arquitectura de software Modelo-Vista-Controlador que mantiene un código legible y separa claramente las partes del código del programa. Angular como uno de los frameworks más populares de JavaScript se construyó para realizar un trabajo rápido y ágil trabajo en equipos de software [5]. Los autores realizaron un análisis exhaustivo de los frameworks existentes basados en JavaScript [6], y se puede concluir que Angular es uno de los frameworks más populares, utilizados y robustos [7] y es necesario que la materia de desarrollo basado en plataformas se encuentre a la vanguardia de las tecnologías para desarrollo web moderno. Además de conocer si MEAN es la solución más efectiva para el desarrollo de aplicaciones web modernas. Se realizó la implementación de una aplicación web para el manejo de la hoja de vida y gestión docente para el departamento de talento humano de la Pontificia Universidad Católica del Ecuador PUCE, Sede Esmeraldas – Ecuador, que permite almacenar, gestionar y analizar la información de los docentes y su gestión docente semestral. Como conclusión del caso de estudio es proponer la aplicación de estas tecnologías dentro de la materia desarrollo basado en plataformas en la universidad y recomendar su uso en el desarrollo de aplicaciones web modernas.

2. Metodología

La metodología de esta investigación incluyó las siguientes fases:

- Análisis bibliográfico de las arquitecturas y tecnologías Javascript para desarrollo web moderno: MongoDb, Express, Angular, NodeJS.
- Modelado de la aplicación en web basada en las tecnologías del estudior: MEAN
- Aplicación de un modelo dentro de la materia desarrollo basada en plataformas junto con las tecnologías JavaEE estudiadas.
- Los pros y los contras del análisis basado en la literatura abierta, los documentos y los modelos de aplicación web realizados.

2.1 Arquitectura

Cada sistema informático, grande o pequeño, está formado por piezas que están unidas entre sí. Puede haber un pequeño número de estas piezas, o tal vez solo una, o puede haber docenas o cientos; y este vínculo puede ser trivial, o muy complicado, o en algún punto intermedio, es decir cada sistema tiene una arquitectura [8]. Al tratar de definir el concepto de Arquitectura de Software existen varias definiciones alternativas o contrapuestas. Pero hay algunas que son reconocidas, a continuación, las citamos. Se puede definir la arquitectura de software como la descomposición de un sistema de nivel superior en cada uno de sus componentes principales, las interfaces y su comunicación [9]. La

IEEE la define de la siguiente manera: Es la organización fundamental de un sistema encarnada en sus componentes, las relaciones entre ellos y el ambiente y los principios que orientan su diseño y evolución [10]. Dentro de las ventajas de la arquitectura de software, podemos mencionar que: simplifica la capacidad de comprender sistemas complejos planteando limitaciones en el diseño, reutiliza componentes en múltiples niveles, separa elementos, lo que permite mayor facilidad en el cambio y mantenimiento del desarrollo, aplica utilización de patrones [11]. El uso de arquitectura de software puede realizarse de una manera eficiente en función del tiempo y ser rentable ya que permite la reutilización de los componentes y patrones de diseño en los proyectos [12]. Al implementar una arquitectura de software es fundamental el uso de los patrones arquitectónicos que brindan un principio general de estructura. Un patrón arquitectónico expresa un esquema de organización estructural fundamental para los sistemas de software. Proporciona un conjunto de subsistemas predefinidos, especifica sus responsabilidades e incluye reglas y pautas para organizar las relaciones entre ellos [13].

2.2 Arquitectura REST

REpresentational State Transfer (REST) es un estilo arquitectónico propuesto por Fielding [14]. REST es para sistemas hipermedias distribuidos a gran escala y que logra que la World Wide Web (WWW) sea escalable. Fielding argumenta que en REST es la existencia de recursos (elementos de información), que pueden ser accedidos utilizando un identificador global (un Identificador Uniforme de Recurso). Para manipular estos recursos, los componentes de la red (clientes y servidores) se comunican a través de una interfaz estándar (HTTP) e intercambian representaciones de estos recursos (los ficheros que se descargan y se envían). El cliente puede navegar esencialmente a través de una amplia gama de recursos existentes, siguiendo los enlaces de un recurso a recurso [15]. Un principio clave de REST es la interacción sin estado entre los participantes en una conversación. Un estado en este caso significa el estado de la aplicación/sesión. El estado se mantiene como parte del contenido transferido del cliente al servidor/servicio y viceversa [16]. Más concretamente, en el caso de los servicios, los clientes que desean utilizar un servicio acceden a una representación particular de los recursos que representan el servicio mediante la transferencia de contenido de la aplicación utilizando un conjunto pequeño y definido globalmente de métodos remotos [16]. Estos métodos describen la acción a realizar sobre los recursos. Los métodos HTTP para crear, leer, actualizar y borrar recursos, cada uno identificado por un URI, son (PUT, POST, GET, y DELETE en HTTP 1.0, mientras que HTTP 1.1 permite extensiones) [17]. En REST, cada solicitud enviada a un objeto resulta en la transferencia de una representación de este objeto por ejemplo, texto, XML, JSON, etc. [15]. REST se ha convertido en la implementación más utilizada en la actualidad [18].

3. MEAN

La stack MEAN es una solución potente y completa. Utiliza el lenguaje de programación JavaScript [19]. Comprende cuatro bloques principales: MongoDB como base de datos, Express como marco de trabajo del servidor web, AngularJS como marco de trabajo del cliente web y Node.js como plataforma del servidor. Estos componentes están desarrollados por diferentes equipos e involucran a una comunidad fuerte de desarrolladores y defensores impulsando el desarrollo y documentación de cada componente. Sin embargo, un

problema que podría afectar dramáticamente su proceso de desarrollo y presentar problemas de escalamiento y arquitectura es la conexión de estas herramientas [20]. La principal fortaleza de MEAN radica en su centralización de JavaScript como el principal lenguaje de programación, ya que cada componente está escrito en JavaScript, incluso la base de datos almacena los datos en formato JavaScript Object Notation (JSON) que es el único script que JavaScript entiende completamente [21]. Por lo tanto, JavaScript no sólo se utiliza como lenguaje de scripting del lado del cliente, sino que también se utiliza a lo largo de la aplicación, es decir, en el lado del cliente, del servidor y de la base de datos [1]. El uso de JavaScript como lenguaje principal de programación tanto en el lado del cliente como en el lado del servidor hace que la pila MEAN sea más potente y reduce el tiempo en la construcción de la aplicación [2]. El uso de todo el JavaScript permite dividir la funcionalidad y las tecnologías utilizadas de la siguiente manera [21]:

- Base de datos objetos JSON utiliza MongoDB.
- Servidor web utiliza Node.js.
- Framework web (back-end) utiliza Express.
- Cliente (front-end) utiliza Angular.

3.1 MongoDB

MongoDB es un modelo de almacenamiento de documentos NoSQL potente, adaptable y escalable [22]. En MongoDB, los datos se almacenan en la base de datos en un formato JSON llamado BJSON, que significa JSON binario, en lugar de filas y columnas como en la base de datos relacional. MongoDB tiene una capacidad para escalar con varias características que la base de datos relacional proporciona como índices secundarios, clasificación y consultas [23], que proporciona alto rendimiento, alta disponibilidad y escalabilidad [20].

3.2 Express

Express es un framework web maduro y flexible para construir aplicaciones web sobre el ecosistema Node. Por defecto, el framework Express utiliza el motor Pug para soportar plantillas [24]. Express es un framework relativamente pequeño que se encuentra en la parte superior de la funcionalidad del servidor web de Node para simplificar sus APIs y añadir nuevas funciones útiles. Facilita la organización de la funcionalidad de su aplicación con middleware y enrutamiento; agrega utilidades útiles a los objetos HTTP de Node y el renderizado de vistas HTML dinámicas; define un estándar de extensibilidad fácilmente implementado [25] . Express es fácil de configurar, implementar, controlar y proporcionar varios componentes clave para manejar las solicitudes web. Express ayuda en la creación de aplicaciones web y servidores HTTP simples ya que es un framework mínimo y flexible [25]. En MEAN, Express funciona como un medio para transferir las solicitudes de un cliente a una base de datos y envía las respuestas de la base de datos al cliente [21].

3.3 AngularJS

AngularJS es una librería escrita en JavaScript para el desarrollo de aplicaciones web, mantenida por Google, es un framework JavaScript de código abierto y aborda los retos de las single-page aplications (SPAs) [26]. Una aplicación web AngularJS sigue el patrón de diseño MVC, que resulta en el desarrollo de aplicaciones web ampliables, mantenibles, comprobables y estandarizadas [26]. La unión de datos AngularJS y la inyección de dependencias lo convierten en un socio ideal para cualquier tecnología de servidor, ya que elimina gran parte del código que de otro modo tendrías que escribir, y todo sucede dentro del navegador [21].

3.4 NodeJS

NodeJS es un framework de desarrollo desarrollado originalmente en 2009 por Ryan Dahl, basado en el motor JavaScript V8 de Google [27]. Node es una plataforma basada en el tiempo de ejecución JavaScript de Chrome para crear aplicaciones en red rápidas y escalables [20]. Node utiliza un modelo controlado por eventos y de no bloqueo de E/S que lo hace ligero y eficiente, perfecto para aplicaciones que requieren grandes cantidades de datos y que se ejecutan en dispositivos distribuidos [21]. Node es un lenguaje de scripting del lado del servidor que puede ser usado en el lado del servidor, lado del cliente, e incluso puede ser un servidor web. Antes de que existiera el Node, JavaScript se usaba simplemente para la interacción del usuario como script del lado del cliente [28].

3.5 Arquitectura MEAN

Al desarrollar una aplicación web la elección de la mejor arquitectura y que para el usuario sea una experiencia fácil, agradable y funcional es trascendental. MEAN trabaja con una arquitectura MVC model-view-controller, que comprende tres capas esenciales: datos, lógica y vista. Una arquitectura MVC funciona así [21]:

- Una solicitud entra en la aplicación.
- La petición se enruta a un controlador.
- Si es necesario, el regulador realiza una petición al modelo.
- El modelo responde al controlador.
- El controlador envía una respuesta a una vista.
- La vista envía una respuesta al solicitante original.

En la arquitectura MVC, la lógica, los datos y la presentación se separan tres tipos de objetos, cada uno se encarga de sus propias tareas. La vista maneja la parte visual, que trata de la interacción con el cliente. El controlador responde a las peticiones del sistema y del cliente, haciendo que el modelo y la vista cambien apropiadamente. El modelo maneja la información, respondiendo a las demandas de datos o cambiando su estado de acuerdo a las instrucciones enviadas desde el controlador [20].

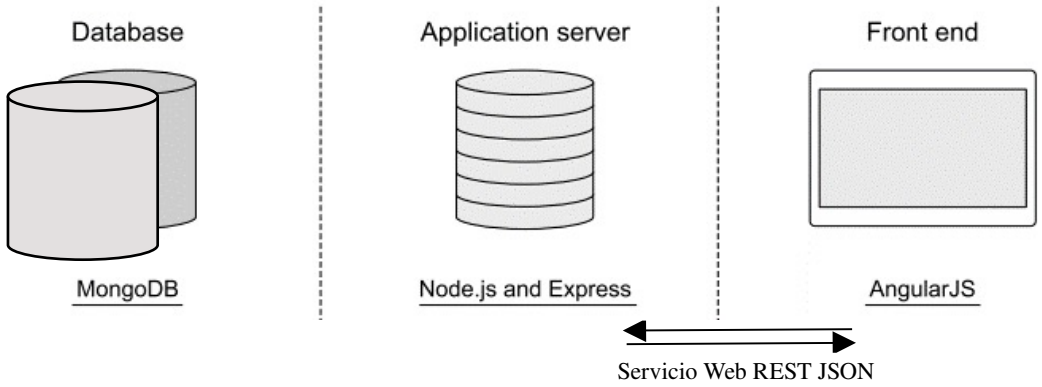


Figura 1. Arquitectura MEAN [21].

La figura 1 muestra la arquitectura de aplicación típica de una pila MEAN. AngularJS como Front-End con un MVC, que se comunica con el servidor Node a través de Express. Por cada solicitud de datos del Back-End, Node envía la solicitud a través del controlador nativo MongoDB o Mongoose. La

respuesta del servidor es enviada al cliente a desde Express. El modelo de datos que se utilizado es JSON y siendo RESTful la estructura de servicio para conectar las rutas desde Express, permitiendo la transferencia de petición y respuesta de ida y vuelta entre el cliente y el servidor [20] .

3.6 MEAN: Principales características

MEAN gana popularidad debido a las características de sus componentes: NodeJS, MongoDB, AngularJS, junto con Express y todo utilizando JavaScript que es una de sus mayores ventajas. Aunque podemos afirmar que MEAN no se recomienda en sistemas pesados de procesamiento computacional, debido a que el componente NodeJS es un entorno de un solo hilo y esto sería un inconveniente fuerte de esta tecnología. En una aplicación de una página (SPA), que requiere una alta interacción con el usuario, visualización y alta escalabilidad, MEAN es la mejor opción. La elección de la herramienta depende principalmente de algunas características que se detalla en la siguiente tabla [6]:

Característica	MEAN
Capa de servidor simplificada	Construcción de servidor localmente
Código isomórfico	Código puede ser ejecutado en el front-end como el back-end
Escalabilidad	La aplicación puede expandirse los eventos se ejecutan libremente de manera asíncrona
Arquitectura sin bloqueo	Maneja el uso de bucles de eventos sin bloqueo en un solo hilo.
Tiempo de desarrollo	Al utilizar el mismo lenguaje JavaScript se reduce el esfuerzo y tiempo de desarrollo
Transformación de datos y extensibilidad	Los datos manejados para el intercambio de información es JSON.

Tabla 1. Resumen de características de las stacks.

4 Caso de Estudio: App web desarrollada

En esta sección se procederá se desarrolló la aplicación de la hoja de vida y gestión de docente para el departamento de talento humano de la Pontificia Universidad Católica del Ecuador, Sede Esmeraldas, que fue construido utilizando la tecnología MEAN. La aplicación que se desarrolló es un CRUD, con varios datos del docente para llenar su hoja de vida por ejemplo datos personales, títulos, experiencia docente, experiencia no docente, capacitaciones, investigaciones, artículos, congresos, libros, etc. Junto con un informe de actividades de fin de cada semestre con la información de alumnos tutorados, cursos, seminarios, congresos y proyectos de vinculación realizados. El desarrollo de esta aplicación es constatar la facilidad o dificultad de construir software web con esta tecnología. En la Figura 2, se puede observar el front-end de la aplicación

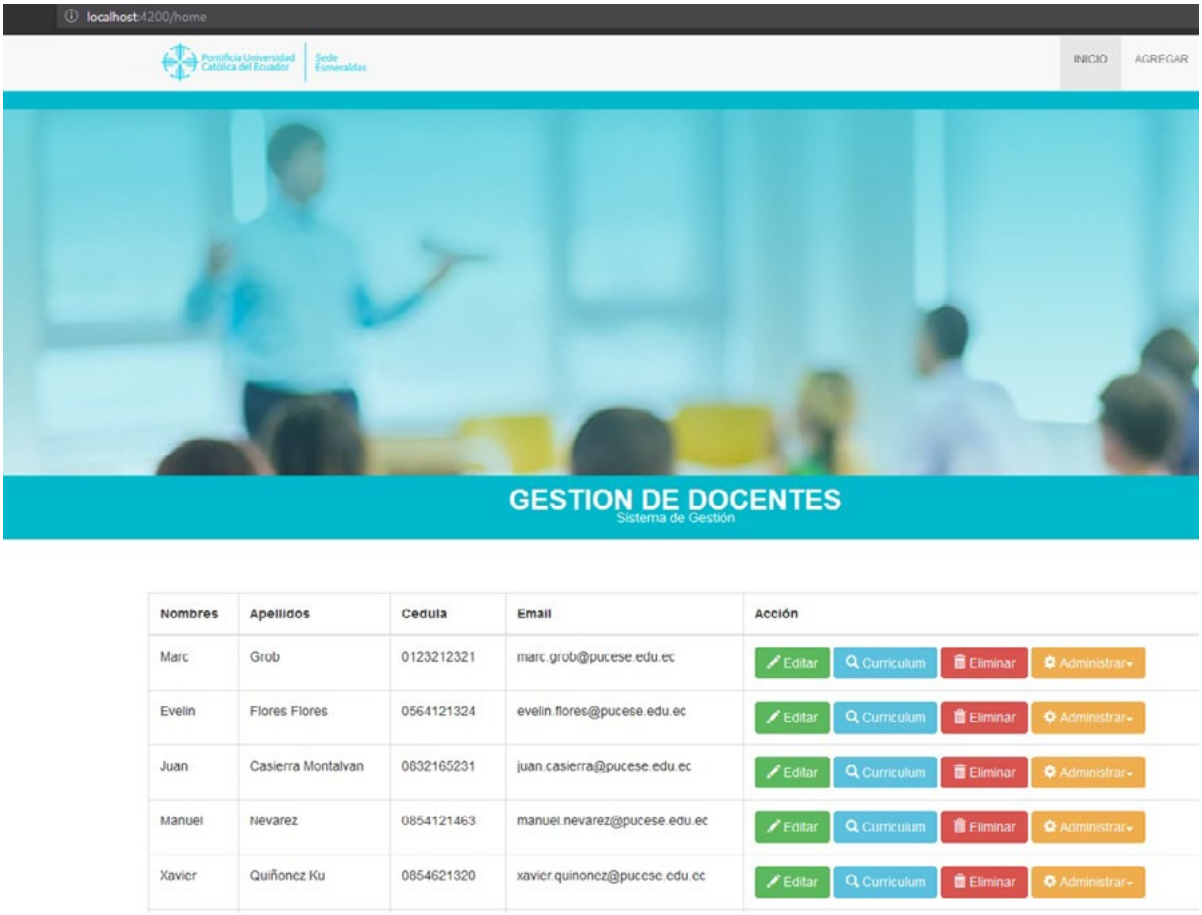


Figura 2. Captura de pantalla de sistema stack MEAN.

La tecnología utilizada para su implementación proporciona una rápida y necesaria flexibilidad y velocidad de las interacciones. También permitió incluir más características o funciones en la aplicación web y lo hizo más interactivo e intuitive. Esto ha sido posible gracias a la tecnología MEAN utilizada.

4.1 Resultados de la base de datos

La plataforma DbSchema permite exportar el modelo de las bases de datos MongoDB. La característica principal es obtener los resultados de la base de datos y presentarlos de forma agradable en un formato legible para el ser humano. El resultado de las distintas colecciones de la aplicación web en la Figura 3, muestra que los datos se almacenan utilizando bloques de JSON y BSON como formato de intercambio de JavaScript. A diferencia de las bases de datos relacionales, las tablas se llaman colecciones mientras que las filas se llaman documentos u objetos. Cada documento comienza con un _id y presenta los datos en forma de “nombre”: “valor”. Los valores en sí mismos pueden ser matrices de otros objetos anidados. MongoDB no obliga a actualizar el esquema como en RDBMS, lo que a veces puede resultar difícil. El resultado muestra que MongoDB nos permite almacenar objetos de una manera muy rica y dinámica. Esto hace que la presentación y la comprensión de las consultas a la base de datos sea muy fácil y la información requerida por el usuario.

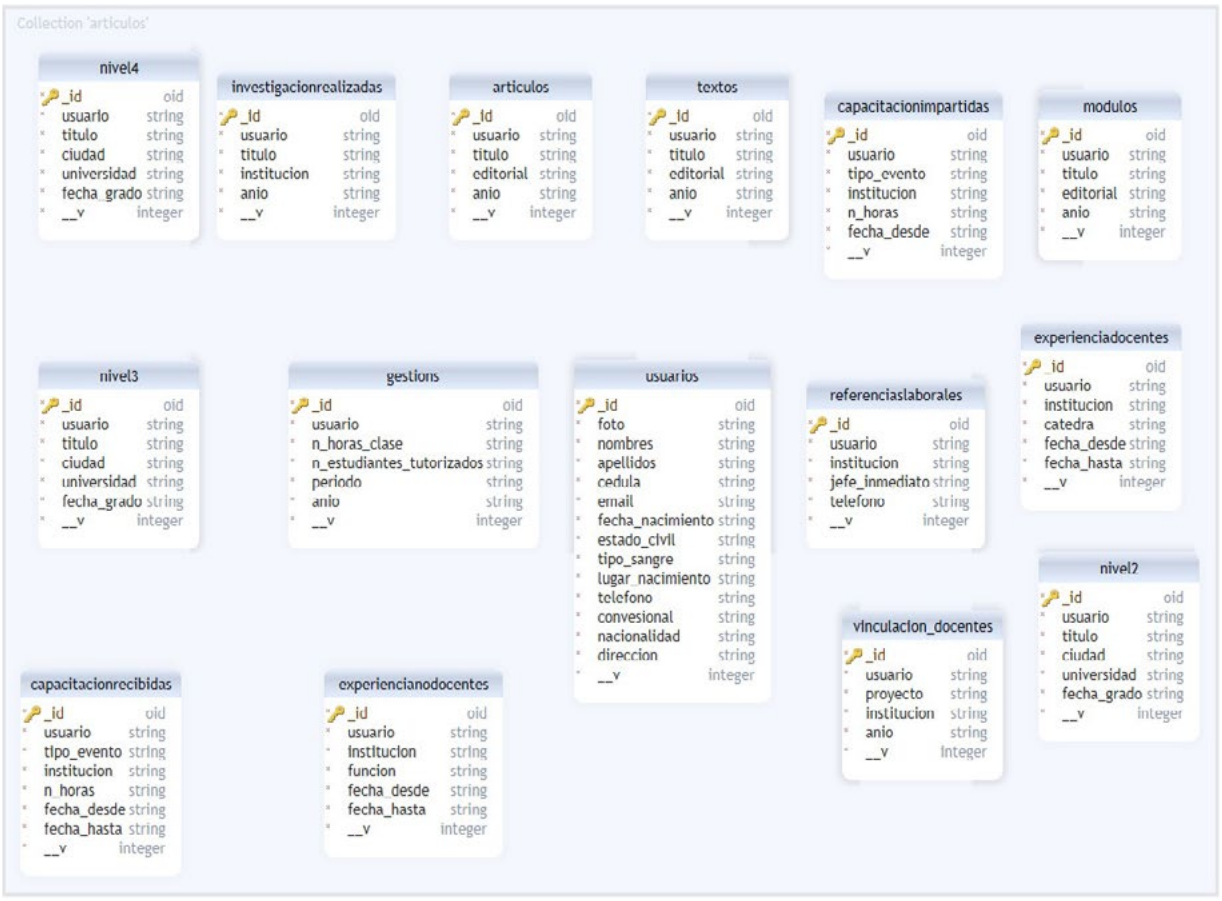


Figura 3. Colecciones de la base de datos MongoDB

4.2 Resultados de la materia desarrollo basado en plataformas

Los estudiantes de la materia desarrollo basado en plataformas tuvieron una impresión positiva hacia la tecnología MEAN, misma que se está impartiendo en la Pontificia Universidad Católica del Ecuador, Sede Esmeraldas, en su carrera de Ingeniería de Tecnologías de la Información. Además, los alumnos han tenido la oportunidad de construir un proyecto piloto e implementarlo en JavaEE y en MEAN. Los resultados de la introducción MEAN mostraron que, a pesar de tener menos bibliografía y lecciones aprendidas, construyeron el proyecto más rápido y con mejor interfaz en una moderna tecnología como es MEAN, en comparación con la pila de la tecnología JavaEE.

5. Conclusiones

En el estado del arte se hizo una descripción de las tecnologías para arquitecturas y servicios web, se describió y analizó las tecnologías para el desarrollo de aplicaciones web. MEAN es un paquete de software que combina MongoDB como la base de datos NoSQL, Express como un framework de NodeJS para el scripting para el desarrollo del back-end, Angular como plataforma MVC para la construcción del front-end, construido con código JavaScript. La creciente popularidad del uso de JavaScript como secuencias de comandos del front-end y del back-end ha hecho que MEAN sea una las combinaciones de tecnologías más utilizadas para desarrollo aplicaciones web. MEAN está construida exclusivamente en JavaScript, por lo

que es un lenguaje para gestionar el lado del cliente, servidor y base de datos. Todos los componentes utilizados en la stack MEAN son completamente de código abierto y actualmente son soportados por desarrolladores corporativos como MongoDB y Google. Todos los componentes de MEAN son relativamente ligeros. La stack MEAN es flexible y escalable. Angular es una muy buena opción para el desarrollo de una SPA y es responsiva. La buena impresión que ha dejado MEAN, se está impartiendo en la Pontificia Universidad Católica del Ecuador, Sede Esmeraldas, en su carrera de Ingeniería de Tecnologías de la Información. El análisis ha demostrado que MEAN es hoy la mejor combinación para unir el back-end de la aplicación con respecto al front-end realizado en tecnología Angular, teniendo en cuenta el rendimiento y la velocidad de la aplicación, la comunicación entre el cliente y el servidor. Un análisis de las deficiencias de MEAN nos proporcionaría con una mejor comprensión y su aplicabilidad. Sin embargo, este documento demostró como MEAN es óptima para el desarrollo de aplicaciones web modernas, hay limitaciones en nuestro estudio de caso. Por ejemplo, nuestro estudio de caso no muestra cómo MEAN reacciona con las aplicaciones intensivas y de gran procesamiento en CPU y memoria RAM. Por lo tanto, este documento podría beneficiarse de la introducción de un estudio de caso que se ocupe del uso intensivo y gran procesamiento de la CPU y memoria RAM.

References

[1] M. Stajcer and D. Orescanin, "Using MEAN stack for development of GUI in real-time big data architecture," *2016 39th Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2016 - Proc.*, pp. 524–529, 2016.

[2] A. J. Poulter, S. J. Johnston, and S. J. Cox, "Using the MEAN stack to implement a RESTful service for an Internet of Things application," *IEEE World Forum Internet Things,* WF-IoT 2015 - Proc., pp. 280–285, 2015.

[3] R. Salunkhe, S. Telang, P. Shrigondekar, and A. Tanpure, *Review of REST Ful Service Using MEAN Stack for Real Time Big Data Architecture*, vol. 3297, no. 11. Birmingham: Packt Publ, 2007.

[4] M. J. Collins, *Pro HTML5 with CSS, JavaScript, and Multimedia*. 2017.

[5] S. Holmes, "Introducing full-stack development," *Get. MEAN*, pp. 3–23, 2015.

[6] A. Mardan, Full stack javascript: *Learn Backbone.js, Node.js, and MongoDB*. 2018.

[7] M. Hajian and N. Oslo, "Progressive Web Apps with Angular Create Responsive, Fast and Reliable PWAs Using Angular-Majid Hajian," pp. 1–380, 2019.

[8] N. Rozanski and E. Woods, Software Systems Architecture: *Working with Stakeholders Using Viewpoints and Perspectives*. Addison-Wesley, 2005.

[9] D. Garlan and M. Shaw, "An Introduction to Software Architecture," *Knowl. Creat. Diffus. Util.*, vol. 1, no. January, pp. 1–40, 1994.

[10] S. Engineering and S. Committee, "IEEE Recommended Practice for Architectural Description of Software-Intensive Systems," 2000.

[11] D. Garlan and D. Garlan, "Software Architecture : a Roadmap Software Architecture : a Roadmap," 2000.

[12] L. Bass, P. Clements, and R. Kazman, *Software Architecture in Practice*, Second Edi. Addison Wesley, 2003.

[13] F. Buschmann, R. Meunier, H. Rohnert, P. Sommerlad, and M. Stal, *Pattern-Oriented Software Architecture - Volume 1: A System of Patterns*. Wiley Publishing, 1996.

[14] R. T. Fielding, "Architectural Styles and the Design of Network-based Software Architectures," *Building*, vol. 54, p. 162, 2000.

[15] M. Zur Muehlen, J. Nickerson, and K. Swenson, "Developing web services choreography standards - The case of REST vs. SOAP," *Decis. Support Syst.*, vol. 40, no. 1 SPEC. ISS., pp. 9–29, 2005.

[16] D. Fensel, F. M. Facca, E. Simperl, and I. Toma, *Semantic Web Services*, 1st ed. Springer Publishing Company, Incorporated, 2011.

[17] C. Pautasso, O. Zimmermann, and F. Leymann, "Restful web services vs. 'big'web services: making the right architectural decision," *Proceeding 17th Int. Conf. World Wide Web*, pp. 805–814, 2008.

[18] S. Patni, *Pro RESTful APIs*. 2017.

[19] D. Flanagan, *JavaScript - The Definitive Guide*. 2011.

[20] A. Q. Haviv, *MEAN Web Development*, vol. 1. 2014.

[21] S. Holmes, *Getting MEAN with Mongo, Express, Angular, and Node*, 1st ed. Greenwich, CT, USA: Manning Publications Co., 2015.

[22] K. Chodorow, *Mongo DB: The Definitive Guide*. 2013.

[23] R. O. Obe and L. S. Hsu, *MongoDB in Action*. 2011.

[24] E. Brown, *Web Development with Node and Express: Leveraging the JavaScript Stack*. O'Reilly Media, 2014.

[25] E. Hahn, Express in Action: *Node Applications with Express and Its Companion Tools*, 1st ed. Greenwich, CT, USA: Manning Publications Co., 2015.

[26] R. K. Soni, *Full Stack AngularJS for Java Developers*. 2017.

[27] S. Davis, "Mastering MEAN: Introducing the MEAN stack," *IBM.com,* pp. 1–20, 2014.

[28] M. Cantelon, M. Harter, T. J. Holowaychuk, and N. Rajlich, *Node.Js in Action*, 1st ed. Greenwich, CT, USA: Manning Publications Co., 2013.

Recibido: *10 de enero de 2022*
Aprobado: *31 de enero 2022*

Artículo de Investigación. Revista Killkana Técnica. Vol. 6, No. 1, pp. 43-68, enero-abril, 2022.
ISSN 2528-8024. ISSN Elect. 2588-0888. Universidad Católica de Cuenca

Metodología breve para la ejecución de pruebas de intrusión. Caso de estudio

Quick methodology for intrusion testing. A case study

Martin Gonzalez Palomeque[1]

[1] Universidad de Cuenca

* martin.gonzalez@ucuenca.edu.ec
DOI: https://doi.org/ 10.26871/killkanatecnica.v6i1.949

Resumen

En la presente investigación se desarrolla una metodología para la ejecución de pruebas de intrusión que sea fácil y rápida de implementar para todo tipo de empresas, especialmente para empresas pequeñas que no cuentan con personal de TI o disponen de personal limitado en esta área. Para ello, la metodología desarrollada se basa en la ejecución de herramientas automatizadas, a la vez que suministra las técnicas y procesos necesarios para su correcta implementación. La aplicación del caso de estudio permitió comprobar que la metodología desarrolla-

da es efectiva, rápida y optimiza el uso de recursos. Los resultados demuestran la falta de conciencia por parte de las empresas en temas de ciberseguridad y dejan en evidencia el poco o nulo conocimiento de los profesionales de TI en esta área.

Palabras clave: *ciberseguridad, seguridad de la información, pruebas de intrusión, metodología.*

Abstract:

This research develops a methodology for executing intrusion tests of easy and fast implementation in all types of companies, especially in small companies that lack or have limited personnel in the IT area. In order to achieve this, the methodology uses of automated tools while providing the necessary techniques and processes for its appropriate implementation. The application of the case study proved that the methodology developed is effective, fast and optimizes resources. The results demonstrate the lack of awareness on the companies' part regarding cybersecurity issues and evidencing the lack of knowledge of IT professionals in this area.

Keywords: *cybersecurity; information security; intrusion testing; methodology.*

1. Introducción

La adopción de las tecnologías de la información en los procesos críticos de las empresas trae consigo beneficios que no se podrían obtener de otra forma [1]. Debido a esto, el uso de las TIC's se ha masificado en los últimos años y no solo en el campo empresarial e industrial, sino en el personal, educativo, de salud y demás ámbitos de la sociedad. Sin embargo, esta hiperconectividad no solo aporta beneficios, también supone riesgos latentes, que, de no gestionarse de manera adecuada, exponen a las empresas y sus activos digitales a cualquier cantidad de amenazas [2].

Las amenazas tecnológicas han evolucionado de tal manera, que resulta difícil etiquetarlas o clasificarlas [3], el virus informático se ha convertido en un abanico de herramientas sofisticadas que actualmente invalida la utilidad de los sistemas de detección y control tradicionales [2].

Así mismo, el incremento en el número de ciberataques en los últimos años es alarmante [4]. El mapa en vivo de ataques cibernéticos de Kaspersky [5] nos demuestra que el ciber crimen no discrimina país, región, persona, empresa grande o pequeña. El bajo costo y riesgo en la perpetración de este tipo de ataques, considerando que solo se precisa de un computador y una conexión a internet, son un factor relevante para este aumento acelerado. Un dato importante es que, las empresas son el objetivo principal y a las que están dirigidos la gran mayoría de estos ataques [6].

El problema principal se debe a la falta de implementación u omisión de controles de seguridad [2] muchas veces básicos dentro de las empresas, esto a su vez, según [4], es consecuencia del desconocimiento y falta de preparación de las empresas y profesionales de TI, y del presupuesto que asignan las empresas a asegurar sus activos digitales [7].

Continuando con [4], el problema va mucho más allá. En América Latina y el Caribe son pocos los países que han creado organismos dedicados a la gestión de temas de ciberseguridad. De los 32 países analizados, un tercio no cuenta con un marco legal sobre delitos informáticos, 12 han aprobado una estrategia nacional de ciberseguridad y tan solo 5 están adheridos a la convención de Budapest que facilita la cooperación internacional en la lucha contra el cibercrimen. Como si fuera poco, la brecha de 600 mil profesionales en el área de ciberseguridad, ha ocasionado que la lucha contra el cibercrimen en la región tenga un avance muy conservador.

En este punto, se vuelve evidente la necesidad de implementar políticas y controles a fin de proteger los activos digitales [8], dentro y fuera de las empresas. Las nuevas modalidades de trabajo remoto y teletrabajo, que vieron su popularidad gracias a la emergencia sanitaria global del virus COVID-19, representan nuevos retos para las empresas y profesionales de TI, ya que los equipos personales y las redes domésticas carecen de las seguridades que posee una infraestructura empresarial, por lo que es necesario personalizar las políticas con el fin de salvaguardar el bienestar de los dispositivos personales y la información contenida dentro de estos [9].

Como mencionamos anteriormente, las herramientas de detección y prevención actuales no son útiles frente a las nuevas amenazas cibernéticas, y la materialización de éstas, representan pérdidas de 50 mil millones por año, solo para América Latina [10]. Tal es así, que se ha visto una creciente popularidad del CaaS (Crimen como servicio), en el que un usuario novel y malicioso, puede adquirir en foros abiertos (anteriormente solo disponible en sitios clandestinos de la dark web), cualquier tipo de herramientas de hacking, para perpetrar ciberataques [11].

Sin duda alguna resulta abrumador considerar el escenario, es por esto que proteger los activos tecnológicos requiere de soluciones con un enfoque holístico, a decir de [12], la ciberseguridad involucra personas, procesos, tecnología e información. De la misma forma, [13] establece que la seguridad de la información se encarga de establecer las pautas, políticas o normas a seguir con el fin de proteger los activos digitales, y las cuales se expanden a toda una organización (infraestructura física, personas, procesos, etc), y la diferencia de la Seguridad Informática, la cual se limita a la parte operacional de una infraestructura tecnológica, dejando de lado lo que [14] considera como el eslabón más débil en la cadena de la ciberseguridad; el factor humano.

En este sentido, existen varios tipos de soluciones que una empresa puede tomar como contramedida a los ataques informáticos, como soluciones basadas en hardware, software, políticas, etc., sin embargo, resalta una que toma la óptica de un atacante y expone las vulnerabilidades de una infraestructura tecnológica con el fin de subsanarlas antes de que puedan ser aprovechadas por un atacante real, se trata de la prueba de intrusión o pentest.

Una prueba de intrusión o pentest es un ataque simulado y autorizado a una infraestructura en búsqueda de vulnerabilidades, con el fin de explotarlas de la misma forma en que lo haría un atacante real, y de esta manera proponer acciones correctivas [15]. No obstante, la ejecución de pruebas de intrusión no es una tarea sencilla. Esta actividad requiere conocimiento profundo de los tipos de ataques, las herramientas, métodos y técnicas [16], por lo que está de más decir, que la mayoría de empresas no cuentan con personal calificado, ni con los recursos económicos para contratar este tipo de servicios [17].

Para facilitar esta tarea, existen varias metodologías en el mercado, algunas de gran relevancia y reconocimiento como The Penetration Testing Execution Standard [18], el OSSTMM [19] y la NIST SP 800-115 [20], entre otras. La mayoría de las cuales siguen el mismo modus operandi; acercarse al objetivo, interactuar con el objetivo en busca de vulnerabilidades, explotar las vulnerabilidades encontradas y generar un reporte [21].

Por otro lado, [22] afirma que el uso de metodologías para la ejecución de pruebas de intrusión, no aporta mejoría alguna, ni en la ejecución, ni al resultado final de la misma. [21] expone que toda implementación es distinta, y que se debe considerar el uso de las metodologías, en base a los requerimientos de cada empresa. Finalmente, [22] concluye en su estudio, que las empresas que prestan servicios de seguridad, implementan parcialmente estas metodologías dependiendo el caso, o simplemente deciden no hacerlo, esto debido a la complejidad requerida para su implementación.

Dentro de este marco, se busca con el desarrollo del presente trabajo, contrarrestar algunas de las problemáticas expuestas en párrafos anteriores, al elaborar una metodología para la ejecución de pruebas de intrusión orientada a empresas pequeñas, tomando la clasificación de [23], y con un enfoque práctico, que sea relativamente fácil de ejecutar, que, utilizando un mínimo de recursos nos permita conocer el estado actual de una empresa en materia de seguridad, y que sea adaptable y repetible. De la misma forma, se espera con el uso de la herramienta, generar una cultura de seguridad en las empresas.

Es importante mencionar que la metodología propuesta no se limita a su uso en infraestructuras pequeñas, no obstante, en una escala macro, existen varias otras consideraciones que requieren de soluciones a la medida y que ofrecen altos niveles de fiabilidad en sus resultados.

2. Metodología

Empezaremos analizando a breves rasgos algunas metodologías existentes [18] [19] [24] consideradas de gran relevancia dentro de la industria a fin de obtener una visión genérica de una prueba o test de intrusión, a la vez que podemos encontrar técnicas o ciertos planteamientos que puedan servir de base para la metodología propuesta.

2.1 Análisis de metodologías existentes

2.1.1 PTES (Penetration Testing Excecution Standard)

Metodología desarrollada en el año 2009 por un grupo de profesionales de todas las áreas. Se enfoca en identificar el "valor de negocio" de los riesgos asociados a los activos tecnológicos. Considerada muy completa, ya que se estructura de 7 fases que cubren todos los aspectos relacionados a la ejecución de pruebas de intrusión, incluyendo los aspectos no técnicos [18]. La guía técnica de implementación provee los procedimientos y la estructura básica para implementar un test de intrusión [25].

Fases:

1. Interacciones Previas: Actividades previas a la ejecución del test necesarias para elaborar una adecuada planificación en la que se definen el alcance, tiempos, fechas, horarios, costos, y demás reglas de ejecución, con el fin de ser lo más claro y transparente en cuanto a requerimientos y evitar futuras controversias.

2. Recolección de información: Consiste en recolectar la mayor cantidad de información sobre el objetivo a través de técnicas OSINT, con el fin de aumentar los posibles vectores de ataque para fases posteriores. El PTES provee una extensa colección de fuentes y métodos en su sitio web para facilitar esta actividad.

3. Modelado de amenazas: Consiste en anticipar cualquier tipo de amenaza considerando el valor de los activos para los atacantes, cuanto les costaría llegar a comprometerlos, bajo qué circunstancias podrían hacerlo y el impacto que tendría la perdida de esos activos.

4. Análisis de vulnerabilidades: Consiste en la búsqueda de vulnerabilidades presentes en el objetivo utilizando varias técnicas automáticas y manuales. A través de correlación específica y categórica, se procede a realizar una validación de las vulnerabilidades encontradas. Finalmente se realiza una investigación a fondo de las vulnerabilidades encontradas, su forma y posibilidad de explotación, daño potencial, etc.

5. Explotación: Se enfoca en establecer un acceso no autorizado a un sistema o recurso de una infraestructura a través del uso de exploits y pasando por alto la seguridad implementada.

6. Post explotación: Consiste en la valoración del equipo comprometido, la relevancia de la información contenida dentro de este y la utilidad del mismo para comprometer otros activos de la red. En esta fase, las Reglas de Compromiso están diseñadas para proteger los intereses tanto de cliente como de auditor, al asegurarse que los activos no están sujetos a riesgos innecesarios.

7. Reporte: El PTES considera 2 reportes finales, el Resumen ejecutivo, que está enfocado en proveer un valor de negocio a la ejecución y a los resultados del test, por lo que está dirigido a quienes están a cargo de la direc-

ción y estrategia de la empresa. El reporte técnico contiene los detalles técnicos del test en cada una de sus fases, las recomendaciones para subsanar los errores técnicos, califica la exposición y riesgo de la organización y provee una conclusión.

2.1.2 CEH (Certified Ethical Hacker)

Es un programa de certificación que valida los conocimientos de los profesionales en temas de seguridad y ethical hacking. Se diferencia de otras metodologías al tomar un enfoque externo, ya que provee las técnicas y herramientas utilizadas por hackers maliciosos para la ejecución de pruebas de penetración [24], sin embargo busca distanciarse de la imagen de estos últimos, al proveer un código de ética a sus profesionales, que de no ser sostenido, significa el retiro y la invalidación de su certificación [26]. Esta metodología está orientada a la práctica y consta de 5 fases.

Fases:

1. Reconocimiento (footprinting): Consiste en recolectar la mayor cantidad de información del objetivo haciendo uso de técnicas de reconocimiento activo y pasivo, siguiendo el método provisto por el CEH. Es el punto de partida que permite planificar las fases posteriores.

2. Escaneo de redes: Utiliza técnicas de escaneo de red, puertos y vulnerabilidades, a fin de obtener una visión general de la infraestructura del objetivo.

3. Enumeración: A través de consultas directas se busca obtener más información acerca de los servicios que se están ejecutando, el estado de los puertos, etc., a fin de encontrar posibles métodos de entrada a la infraestructura del objetivo.

4. Análisis de vulnerabilidades: Consiste en la búsqueda de debilidades en un activo de red, ya sea errores de configuración, vulnerabilidades conocidas, ausencia de parches, etc., para luego proceder a clasificar estas vulnerabilidades según su severidad. Por último, a través de un informe recomendar las acciones a seguir para remedias las vulnerabilidades encontradas.

5. System Hacking (Hackeo del sistema): Con toda la información recolectada en las fases previas, el auditor intenta vulnerar el sistema comprometiendo su seguridad. La metodología en esta fase sigue de esta forma; obtener acceso, escalar privilegios, mantener acceso y eliminar rastros.

2.1.3 OSSTMM (The Open Source Security Testing Methodology Manual)

Creada por el ISECOM con la colaboración de más de 150 profesionales de todas las áreas, está orientada a la medición de la seguridad en un nivel operacional [19]. Para esto se enfoca en el análisis de las superficies de ataque de una organización, en los controles de seguridad implementados, en la eficacia de los mismos, y realiza un análisis de brecha entre la situación actual y la deseada. Establece varios tipos de test genéricos para poner a prueba los llamados canales operacionales, obtener las métricas derivadas y finalmente elaborar un informe. Es considerada todavía una metodología de mucha relevancia ya que considera la totalidad de los canales de operación empresarial (físico, humano, telecomunicaciones y redes de datos) [27]. Consta de 4 fases.

Fases:

1. Inducción: Se basa en el análisis de la organización y su entorno. Consiste en la revisión de la cultura, normativa, políticas, etc., para

obtener una idea del alcance, el tipo de test requerido y sus restricciones.

2. Interacción: Consiste en interactuar con el objetivo y sus activos digitales a través de actividades de verificación y auditoria, con el fin de obtener respuestas y analizarlas.
3. Investigación: Consiste en identificar las respuestas o emanaciones que produce el objetivo en la fase de interacción, esto nos revela los procesos y activos de valor, y sus seguridades.
4. Intervención: Consiste en intervenir en los recursos que consume el objetivo con el fin de provocar cambios en su comportamiento.

2.2 Estudio comparativo entre metodologías existentes

Para este pase, se ha hecho uso del Método de Estudio de Similitud entre Modelos y Estándares MSSS [28] el cual parte considerando 3 aspectos:

- Alcance o enfoque de la aplicación del modelo o estándar.
- Filosofía o principios básicos y parámetros del modelo o estándar.
- Estructura de los pasos o fases que componen el modelo o estándar.

Aplicándolo a nuestro estudio, obtenemos una vista general de las metodologías analizadas, como se ve en la tabla 1.

Tabla 1. Datos comparativos de las Metodologías seleccionadas.

Metodología	Alcance	Filosofía	Estructura
PTES	Para proveedores de servicio y empresas que requieren contratar este tipo de servicios. Cubre aspectos técnicos y no técnicos relacionados a la ejecución de pruebas de penetración.	Se centra en proporcionar un valor de negocio a los riesgos y vulnerabilidades asociados a los activos digitales de una organización.	1. Interacciones previas al compromiso 2. Recolección de información 3. Modelado de amenazas 4. Análisis de vulnerabilidades 5. Explotación 6. Post explotación 7. Reportes
CEH	Enfoque práctico y orientado al profesional.	Se orienta en proveer el conocimiento, las herramientas, la práctica y la experiencia para la ejecución de pruebas de penetración, con una óptica externa o de un atacante.	1. Footprinting 2. Escaneo 3. Enumeración 4. Análisis de vulnerabilidades 5. System Hacking

OSSTMM	Se enfoca en analizar las superficies de ataque de una organización, los controles implementados, la eficacia de los controles, y realiza un análisis de brecha entre la situación actual y la deseada.	Está orientada a la medición de la seguridad en un nivel operacional, y está diseñada para ser repetible y adaptable a cualquier tipo de auditoría.	1. Inducción 2. Interacción 3. Investigación 4. Intervención

Seguidamente, consideramos relevante comparar las metodologías, en base a algunas características relevantes en orden con nuestra orientación, para lo que elaboramos una lista de verificación, la cual se demuestra en la tabla 2.

Tabla 2. Lista de verificación de características relevantes

Metodología	PTES	CEH	OSSTMM
Provee una guía técnica de aplicación		X	
Provee las herramientas para su aplicación	X	X	
Enfoque específico en la práctica		X	
Contempla los pasos del proceso genérico de pentest	X	X	
Cubre aspectos no técnicos relacionados al test	X		X

Por último, considerando el enfoque requerido para nuestra metodología, analizamos los objetivos y carencias de cada metodología estudiada, en relación a la orientación práctica. Los resultados se observan en la tabla 3.

Tabla 3. Objetivos de las metodologías en relación con el enfoque práctico.

Metodología	Enfoque	Objetivos	Relación con la ejecución practica
PTES	Metodología de pruebas de penetración	Cubrir todos los aspectos relacionados a la ejecución de pruebas de penetración (técnicos y no técnicos), analizar los riesgos y traducirlos a un lenguaje de negocio	Contiene una guía técnica y las herramientas para su ejecución. Su implementación va más allá de la práctica por lo que le incrementa complejidad. Contempla todas las fases del proceso genérico de ethical hacking. No provee lineamientos técnicos de como ejecutar pruebas de penetración

CEH	Metodología de ethical hacking	La formación y acreditación de profesionales y especialistas en seguridad informática y ethical hacking, en la aplicación de las mismas técnicas y herramientas de un atacante	Es una metodología 100% practica, provee las herramientas y métodos para la implementación de pruebas de penetración y contempla todas las fases del proceso genérico de ethical hacking. No contempla aspectos no técnicos relacionados con pruebas de penetración
OSSTMM	Metodología de auditorías de seguridad	Proveer una metodología científica que permita verificar y medir los controles de seguridad de una organización, y presentar métricas en base a hechos derivados de la ejecución de las pruebas	Provee varios tipos de test para la ejecución de las pruebas o auditorias de seguridad, también provee técnicas para la ejecución de los test en cada uno de los canales. No provee las herramientas para la ejecución de las pruebas y no contempla las fases del proceso genérico de ethical hacking

La implementación del método MSSS nos permitió observar que la metodología CEH es la que más se alinea a lo requerido por nuestra metodología por lo que la consideraremos como base principal para el desarrollo de nuestra herramienta.

2.3 Desarrollo de la metodología propuesta

Gracias a la revisión y análisis comparativo de las diferentes metodologías estudiadas, tenemos una visión genérica del proceso de ejecución de pruebas de intrusión, por lo que estamos en la condición de sintetizar lo aprendido y adaptarlo en base a los requerimientos de nuestra metodología.

De esta manera, hemos estructurado nuestro modelo con la siguiente disposición:

Fase 1: Definición del alcance

Fase 2: Escaneo

Fase 3: Análisis de vulnerabilidades

Fase 4: Explotación

Fase 5: Reporte

De manera general, la tabla 4 presenta las características más relevantes de la metodología propuesta, a la vez que justifica las decisiones de diseño con el fin de proveerle sentido.

Tabla 4. Características generales de la metodología propuesta.

Fases	Objetivo	Actividades	Metodología Base	Justificación
1. Definición del alcance	Recolectar la información necesaria para planificar las fases posteriores y organizar los recursos disponibles, con el fin de garantizar fluidez en la ejecución del test y prevenir inconvenientes	A través de reuniones con el beneficiario o su representante se debe definir: Rangos de IP, dominios, puertos, Fechas de inicio, fin, horarios de ejecución y honorarios de ser el caso.	Se basa en la fase de "Interacciones previas al compromiso" del PTES	Aunque el método propuesto está orientado a la ejecución práctica, se ha integrado esta fase por considerarse de gran valor, al proporcionar cierto grado de seguridad tanto para el beneficiario como para el equipo auditor, estableciendo reglas claras y límites para la ejecución de las fases posteriores. Esta fase, aunque corta, previene posibles futuras controversias como desbordamiento del alcance, insatisfacción del cliente o beneficiario, etc.
2. Escaneo	La búsqueda de vulnerabilidades y vías de acceso a la infraestructura tecnológica del objetivo a través de la interacción con herramientas automatizadas	Escaneo de red Escaneo de puertos Escaneo de vulnerabilidades Elaborar un diagrama de red	Se basa en las fases de "Escaneo de redes" y "Enumeración" de la metodología CEH	Ya que el método propuesto se basa en un test de caja blanca (o un test doble caja gris según el OSSTMM), el equipo auditor cuenta con toda la información sobre la infraestructura de la organización, siendo necesario únicamente realizar un escaneo automatizado de la misma. Se ha combinado la fase de Enumeración junto con la fase de escaneo de redes del CEH, ya que la orientación, el alcance de cierta forma genérico del test, y las herramientas utilizadas, permiten realizar la enumeración de manera simultánea al escaneo.

3. Análisis de Vulnerabilidades	Aumentar la probabilidad de una explotación exitosa al analizar las vulnerabilidades encontradas, priorizarlas por nivel de severidad y posibilidad de explotación. Buscar y analizar los métodos de explotación.	Correlación específica y correlación categórica de vulnerabilidades	Se basa en la fase de "Análisis de vulnerabilidades" de la metodología PTES	Las herramientas utilizadas para el escaneo de vulnerabilidades, devuelven en la mayoría de los casos, vulnerabilidades conocidas, por lo que, el proceso de validación (de la fase Análisis de Vulnerabilidades del PTES), a través de correlación especifica (y categórica en ciertos casos), resulta más que suficiente para encontrar métodos de explotación.
4. Explotación	Obtener evidencia de una explotación exitosa de un host, dentro de la infraestructura del objetivo.	Búsqueda, selección y ejecución de payloads y exploits en un host vulnerable	Se basa en la fase de "System hacking" de la metodología CEH	La consecución de una explotación exitosa a un host dentro de la infraestructura del objetivo, resulta de suma importancia, ya que provee evidencia "tangible" de que una organización es vulnerable, y ayuda al beneficiario a interiorizar el peligro y los riesgos de un ataque real
5. Reporte	Presentar los resultados del test de una manera entendible y cuantificable	Generar reportes de herramientas utilizadas, Elaborar reporte final	Se basa en la fase "Reporte" de la metodología PTES	Es necesario un entregable con información relevante y entendible, que provea una visión holística de la situación en temas de seguridad de la información, y que sirva de soporte para la elaboración de hojas de ruta y planes de acción para subsanar las vulnerabilidades encontradas. Podría considerarse la fase más importante del método, ya que, sin este documento, el beneficiario no tendría conocimiento del estado de su infraestructura, por lo que, la ejecución del test habría sido en vano.

A continuación, desarrollaremos el planteamiento de cada fase y facilitaremos el conocimiento para su correcta aplicación.

2.3.1 Fase 1: Definición del alcance

A pesar de tener enfoque práctico, se ha considerado importante incluir una fase previa a la ejecución en la que se establezcan acuerdos y compromisos necesarios para garantizar una adecuada logística que resulte beneficiosa tanto para el cliente como para el auditor. En esta fase se realiza la planificación del test y se definen aspectos como:

- Rangos de IP
- Dominios
- Puertos
- Horarios para la ejecución del test
- Fechas de inicio y fin
- Entregables
- Honorarios
- Restricciones y exclusiones
- Acuerdos de confidencialidad, entre otros.

Luego de definir estos y otros aspectos no contemplados anteriormente, se generan los documentos que autorizan legalmente al auditor a iniciar la ejecución del test.

En esta fase pueden ser útiles los siguientes documentos:

- Contratos de trabajo
- Formularios de autorización
- Acuerdos de confidencialidad, etc.

2.3.2 Fase 2: Escaneo

Se ha omitido la fase de reconocimiento ya que la misma se encuentra implícita en la fase anterior, por lo que podríamos decir, que nuestra metodología está basada en un test de caja blanca.

Esta fase es la combinación de las fases de escaneo y enumeración del CEH, ya que la naturaleza del método se basa en la ejecución de herramientas automatizadas, las que en la práctica, permiten realizar estas acciones al mismo tiempo. La fase consta de 2 actividades:

Escaneo de red y puertos: Con el uso de herramientas automatizadas, se procede a escanear la red con el objetivo de encontrar los hosts que se encuentran activos, los puertos que se encuentran abiertos y los servicios que ejecutan. También es importante elaborar un diagrama de red con el fin de obtener una visión general de la infraestructura del objetivo, a la vez que podemos anotar hallazgos importantes y consultarlos de forma visual.

Escaneo de vulnerabilidades: Consiste en obtener un listado de las vulnerabilidades presentes en la infraestructura del objetivo a través de escáneres automatizados, para proceder a analizarlas en la fase posterior.

Se recomienda a partir de esta fase, documentar todo lo relacionado a la ejecución del test con el fin de respaldar el trabajo realizado, los hallazgos encontrados y facilitar la elaboración del reporte final. Herramientas útiles para esta fase son, nmap, nessus, draw.io para la elaboración de diagramas y keepnote o cherry tree para realizar anotaciones.

2.3.3 Fase 3: Análisis de vulnerabilidades

Consiste en el análisis de las vulnerabilidades encontradas a través del método de correlación específica, del proceso de validación de la fase de análisis de vulnerabilidades del PTES. El cual consiste en cotejar las vulnerabilidades encontradas, en bases de datos de vulnerabilidades utilizando su id de CVE (Common Vulnerabilities and Exposures).

Para ello es necesario, antes que nada, clasificar u ordenar las vulnerabilidades encontradas, de

acuerdo a su daño potencial o criticidad. Aquellas de criticidad alta tendrán más probabilidades de una explotación exitosa, por lo que se recomienda empezar por ellas.

Seguidamente, se procede a la búsqueda de un exploit adecuado haciendo uso de bases de datos de vulnerabilidades como cve.mitre, exploit-db, rapid7 o vuldb. Estas bases de datos generalmente contienen los métodos de explotación, exploit, payloads, el código fuente y las indicaciones necesarias para la explotación.

La correlación especifica no siempre es exitosa, por lo que también será necesario realizar una búsqueda manual en base a los puertos, servicios y versiones encontrados en la fase anterior. En este paso son útiles herramientas como searchsploit o metasploit framework. Es sumamente importante recalcar que los exploits encontrados están desarrollados para el sistema, servicio y versión que se ejecuta en el host objetivo, ya que, de no hacerlo, podríamos perjudicar de forma permanente el sistema.

Debe señalarse, que lo que busca la metodología es poner a prueba la seguridad de una infraestructura, y bajo ningún motivo perjudicar los sistemas y activos digitales dentro de ésta, por lo que la búsqueda de exploits y payloads estará orientada a la obtención de un shell remoto únicamente, y no a alterar la operación normal de los equipos, como por ejemplo, el uso de ataques DOS.

Una vez encontrado el exploit adecuado, procedemos a la fase de explotación.

2.3.4 Fase 4: Explotación

Esta fase consiste en poner a prueba el exploit encontrado. Nuevamente se recomienda hacerlo desde un inicio con las vulnerabilidades de criticidad alta y en los hosts que tienen mayor relevancia para el beneficiario del test, a fin de proveer evidencia de los riesgos existentes y concientizar al cliente sobre el impacto de negocio que ocasionaría un host comprometido.

Para la ejecución de esta fase, es posible utilizar los exploits descargados de las bases de datos de vulnerabilidades utilizando las guías disponibles o los menús de ayuda que generalmente vienen contenidos dentro del mismo exploit. Otra herramienta muy útil para la explotación es Metasploit Framework, la cual contiene gran cantidad de auxiliares, exploits, payloads y otras utilidades que facilitan en gran manera la tarea de explotación.

[29] recomiendan de manera insistente, realizar pruebas de los exploits descargados de internet en ambientes controlados antes de utilizarlos en un ambiente real, esto con el fin de evitar daños a los sistemas y a la operación normal de la empresa. Los exploits podrían hacer más de lo que dicen hacer y podríamos estar perjudicando en lugar de proporcionando un servicio a la empresa.

Al obtener un Shell remoto en un host objetivo finaliza la fase de explotación, ya que es evidencia suficiente de haber vulnerado la infraestructura del cliente. Puesto que en la práctica no resulta tan sencillo, en el caso de haber fallado el exploit, es necesario repetir el proceso con la siguiente vulnerabilidad de criticidad alta encontrada en la fase anterior.

Si el exploit ha tenido éxito, no se recomienda dar seguimiento al resto de vulnerabilidades encontradas, sobre todo por cuestiones de tiempo y seguridad. En este punto se ha cumplido el objetivo del test al exponer los riesgos presentes en la infraestructura objetivo.

Como en las fases anteriores, se recomienda documentar todo el proceso, tomar capturas y guardar la ejecución de comandos en archivos de texto, ya que servirán de anexos para el reporte final, además de que sirven de evidencia del trabajo realizado.

2.3.5 Fase 5: Reporte

Consiste en la elaboración de un reporte final en base a lo realizado y los resultados obtenidos en cada una de las fases del test. El auditor debe ser capaz de sintetizar la información relevante y generar un resumen ejecutivo de fácil comprensión, considerar que no todas las personas a quienes va dirigido el reporte final poseen entendimiento en temas de tecnología ni manejan terminología técnica.

Seguido, se recomienda incorporar todo lo realizado a modo de narrativa, a fin de proveer una línea de tiempo que ayude a comprender de principio a fin el proceso ejecutado. Por último, se requiere el criterio del auditor sobre el estado general de la infraestructura y una breve recomendación. Los archivos de texto con la ejecución de los comandos, las capturas de pantalla y los reportes generados de la ejecución de las herramientas, serán parte del apéndice y servirán de soporte para el tratamiento de las vulnerabilidades encontradas a través de hojas de ruta y planes de acción y prevención de riesgos.

A manera de plantilla, se recomienda incluir por lo menos los siguientes puntos:

- Resumen ejecutivo
- Metodología Utilizada (por ejemplo, caja gris orientada al network assesment)
- Narrativa o cronología del test
- Conclusiones y recomendaciones
- Apéndice

2.3.6 Flujograma

Para ilustrar lo desarrollado en párrafos anteriores, se ha elaborado un flujograma (figura 1) de la metodología propuesta, con el objeto de ofrecer una herramienta visual y de fácil comprensión, al mismo tiempo que servirá de soporte para una correcta ejecución.

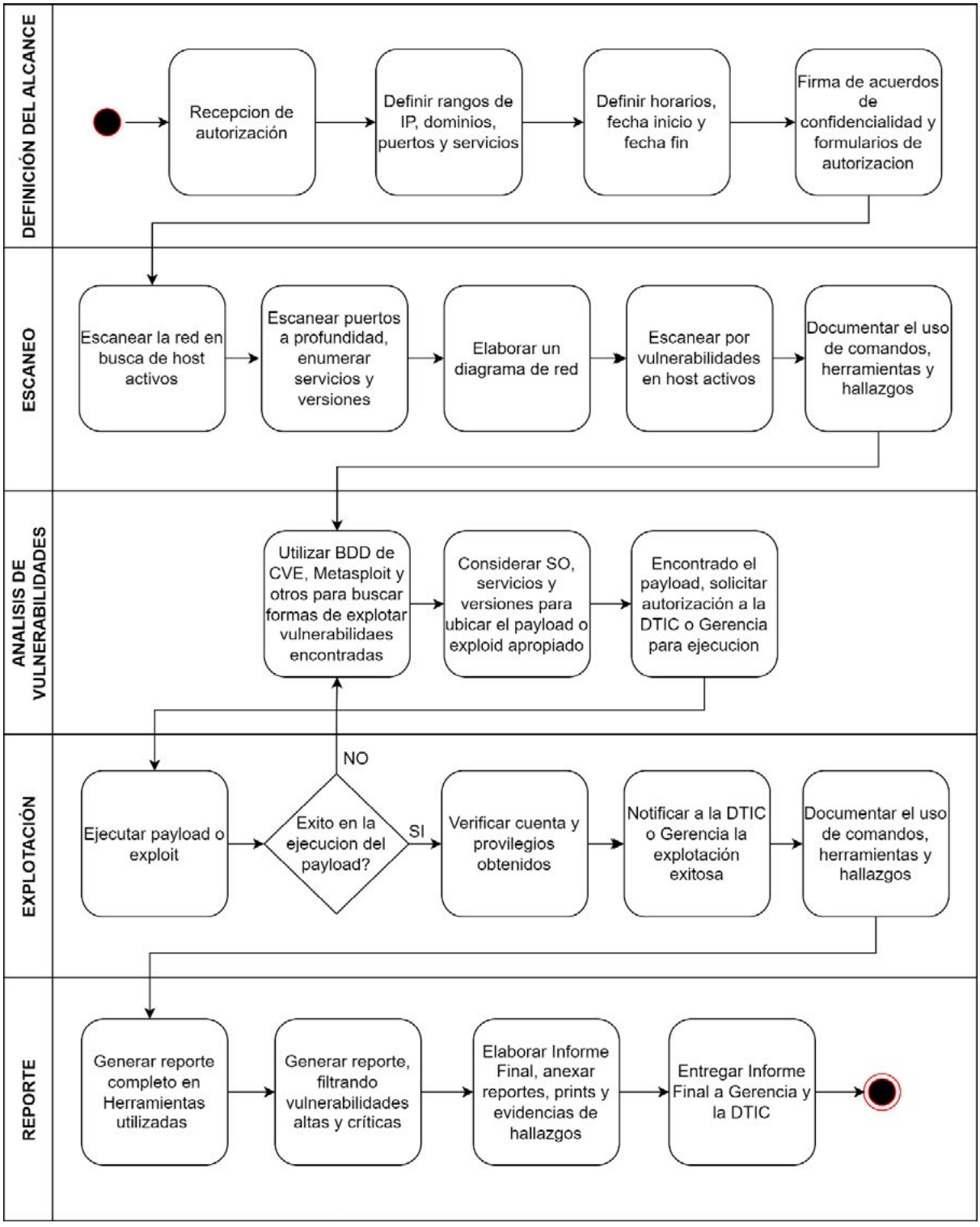


Figura 1. Diagrama de flujo metodología propuesta

2.4 Aplicación del caso de estudio

Luego de haber desarrollado la metodología, lo siguiente es evaluar la utilidad de la misma a través de un caso de estudio. En las siguientes líneas vamos a ir desglosando la metodología y aplicando los conocimientos aprendidos en cada una de sus fases.

La infraestructura seleccionada para el caso de estudio corresponde a una pequeña empresa ecuatoriana en la ciudad de Azogues que cuenta con 17 empleados, cada uno con un equipo de cómputo con conexión a internet. Luego de que se ha recibido la autorización para la aplicación de la metodología por parte del dueño de la empresa, procedemos con la primera fase.

Antes que nada, es importante mencionar que la información de carácter sensible y confidencial, obtenida por el resultado de la ejecución de comandos y herramientas ha sido enmascarada con el fin de preservar la anonimidad de la empresa, evitar poner en riesgo sus activos digitales y dar cumplimiento al acuerdo de confidencialidad.

2.4.1 Definición del alcance

En esta fase, hemos mantenido una reunión con la Gerencia de la empresa y con el área de TIC's con el objeto de definir lo establecido en el apartado anterior. Para ello y como resultado de la reunión, se han elaborado 2 documentos:

- Formulario de autorización de prueba de intrusión: en el que se definen los aspectos técnicos (rangos de ip, puertos, dominios, horarios de ejecución, etc) y se recibe la autorización expresa para ejecutar esta labor.
- Acuerdo de confidencialidad: Establece las condiciones para el uso de la información proporcionada por la información y resultado de la ejecución del test.

Existen en internet disponibles varias plantillas de los documentos enumerados anteriormente los cuales podemos modificar en beneficio del cliente y el auditor, y según los requerimientos del test.

En la gran mayoría de los casos, será necesario notarizar estos documentos a fin de contar con un respaldo legal en al caso de presentarse controversias futuras.

2.4.2 Escaneo

Empezamos conectando el equipo auditor (hack box) a la red de la empresa y verificando el segmento de red en el que nos encontramos (figura 2).

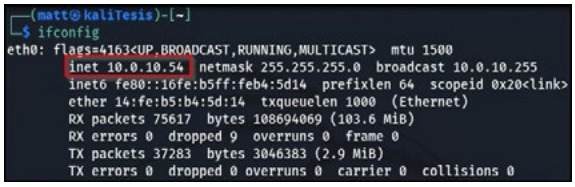


Figura 2. Verificación segmento de red

Pasamos al escaneo de red, en la misma terminal utilizando la herramienta nmap con el siguiente comando (figura 3):

nmap -Pn 10.0.10.0/24 -o /home/comando1.txt

- -Pn: evita el bloqueo de host Discovery
- -o: almacena el resultado de la ejecución del comando en un archivo de texto

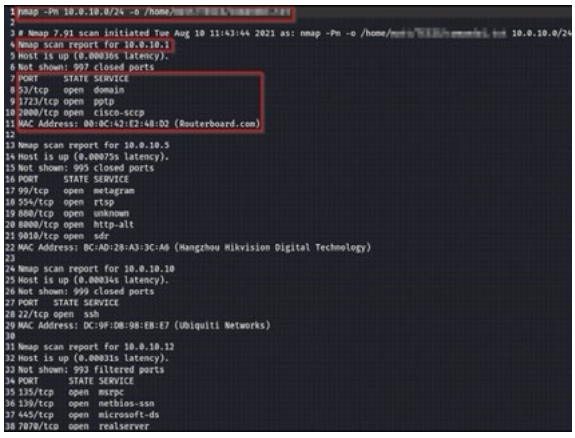


Figura 3. Escaneo de red con nmap

De esta forma obtenemos los hosts que se encuentran activos. También se obtiene información adicional como puertos, información de tarjetas de red, y algunos servicios que están en ejecución, sin embargo, en este caso solo nos interesan los hosts activos, con los que podemos ir elaborando un diagrama de red y con los que realizaremos el escaneo de puertos más profundo, para ello utilizamos el siguiente comando:

nmap -T4 -p- 10.0.10.1

- -T4: utiliza una plantilla predeterminada (0: sigiloso y lento, 5: ruidoso y rápido)
- -p-: selecciona todos los puertos (65535) para el análisis

La salida del comando la podemos ver en la figura 4.

```
└─$ nmap -T4 -p- 10.0.10.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-10 11:58 -05
Nmap scan report for 10.0.10.1
Host is up (0.0049s latency).
Not shown: 65530 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
1723/tcp open  pptp
2000/tcp open  cisco-sccp
4365/tcp open  unknown
4532/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 14.43 seconds
```

Figura 4. Escaneo de puertos con nmap

El comando devolvió información adicional en comparación con el anterior, ahora procedemos a enumerar cada puerto disponible. Ya que el ejemplo anterior corresponde al escaneo de puertos en un router, procederemos de ahora en adelante, por fines académicos, a demostrar la ejecución de comandos en un host de la red. El comando para enumerar los puertos es el siguiente:

nmap -A -T4 -p80,135,139,443,445,3306,3389,5357,5800,5900,7070,49152,49154,49180,49206,49207,49318 10.0.10.16

- -A: combina detección de sistema operativo, versiones, ejecución de scripts y otros más.
- -p: especifica el puerto, puertos o rango de puertos dentro del análisis

La salida del comando la podemos ver en la figura 5.

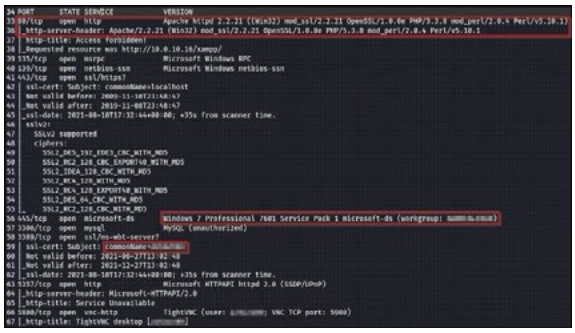


Figura 5. Enumeración de puertos con nmap

La ejecución del comando nos devuelve información valiosa como el sistema operativo, su versión, el nombre de host y grupo de trabajo, también nos presenta información importante en cuanto a puertos y servicios en ejecución y sus versiones respectivas. Esta información será de gran utilidad para la fase de análisis de vulnerabilidades.

En este punto podemos ir actualizando nuestro diagrama de red, por considerarse una herramienta de consulta rápida y útil como nos demuestra la figura 6. Para ello se ha utilizado la herramienta draw.io y se recomienda incluir sistemas (Windows 7 para todos los hosts en este caso), números de puertos y servicios activos.

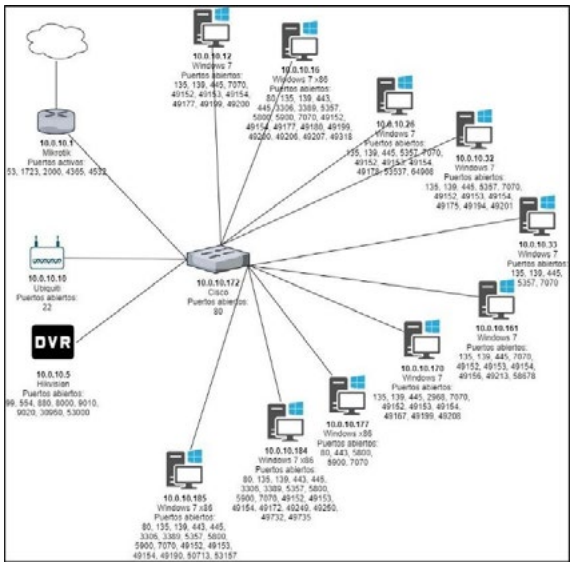


Figura 6. Diagrama de red

Posteriormente, pasamos al escaneo de vulnerabilidades. Ya que hemos encontrado únicamente 10 hosts disponibles en la red, utilizaremos la herramienta Nessus que en su versión gratuita nos permite escanear hasta 16 hosts al mismo tiempo. Para redes que contengan más de 16 hosts disponibles se recomienda considerar el uso de la herramienta OPENVAS que es igual de potente que Nessus, pero de libre uso.

Iniciamos la herramienta y seleccionamos la opción Basic Network Scan, dentro de la sección New Scan. Le damos un nombre y una descripción a nuestro escáner e ingresamos las direcciones IP de los hosts activos descubiertos en los pasos anteriores, como se ve en la figura 7.

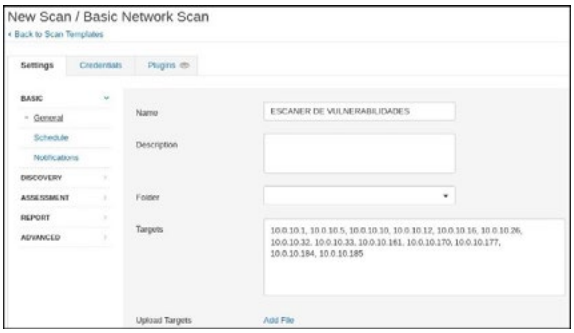


Figura 7. Configuración básica Nessus 1

De las configuraciones por defecto, partimos a modificar únicamente la opción Scan Type a todos los puertos como se ve en la figura 8.

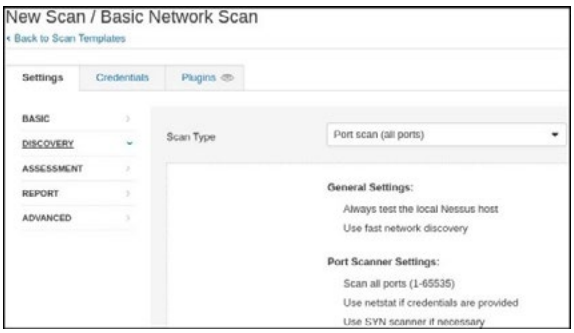


Figura 8. Configuración básica Nessus 2

Acto seguido, guardamos el test y procedemos a ejecutarlo desde la sección My Scans. Una vez concluido el escaneo, ingresamos a los resultados para continuar con la siguiente fase.

2.4.3 Análisis de vulnerabilidades

Como nos muestra la figura 9, la interfaz de la herramienta Nessus nos permite verificar el número total de vulnerabilidades encontradas, a la vez que las clasifica por host y sub clasifica de forma visual, por severidad.

Figura 9. Resultado Nessus - Escaneo

Si seleccionamos un host, Nessus nos muestra las vulnerabilidades presentes dentro de ese host clasificándolas por grupo de amenaza. Para continuar con el flujo propuesto, deshabilitamos la clasificación de amenazas y ordenamos los resultados por severidad, empezando por las de carácter crítico y accedemos a la primera vulnerabilidad listada, tal como se muestra en la figura 10.

La herramienta despliega múltiples vulnerabili-

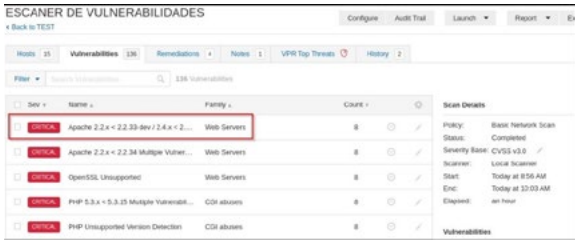


Figura 10. Resultados Nessus – ordenados por severidad

dades encontradas y la información relacionada a cada una. Al final, como demuestra la figura 11, se encuentra la id de la CVE que podemos consultar en las bases de datos de vulnerabilidades por sus respectivos exploits, o podemos usar herramientas como searchsploit o metasploit framework para validad su aplicabilidad en este caso, tomando en cuenta siempre, los sistemas, servicios y versiones en ejecución en el sistema objetivo.

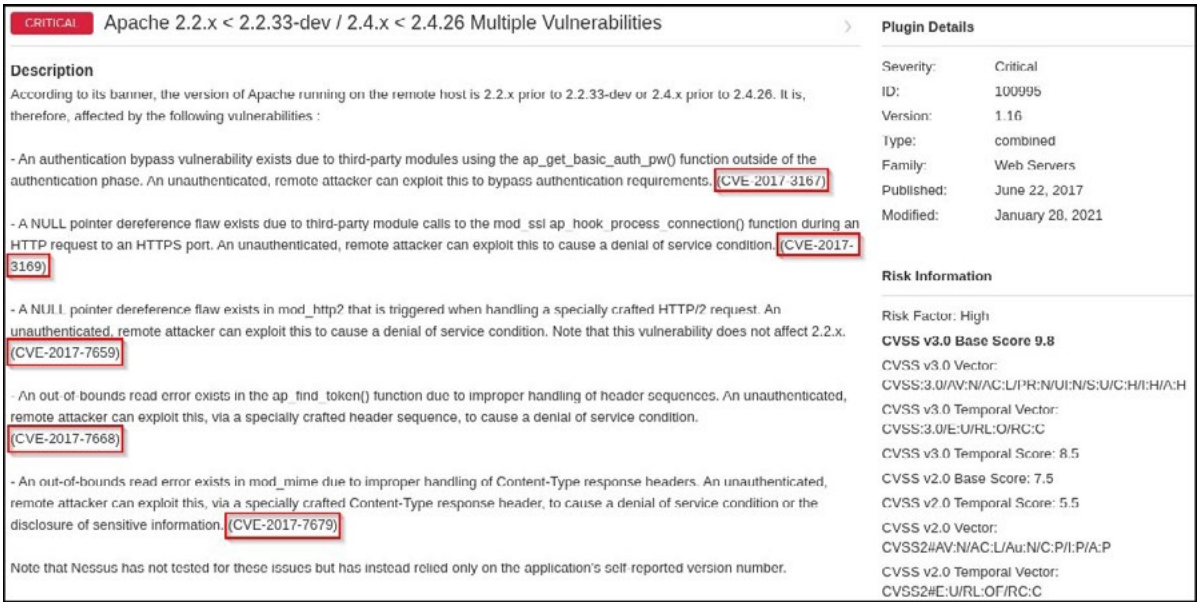


Figura 11. Información Nessus - vulnerabilidad Apache

Luego de realizar una búsqueda exhaustiva en searchsploit y metasploit sin encontrar un exploit adecuado para nuestro caso, procedemos a utilizar una base de datos de vulnerabilidades. Al igual que con las otras herramientas, no tenemos éxito en la búsqueda de un exploit apropiado. Como podemos ver en la figura 12, existen varios exploits disponibles, pero ninguno para sistemas Windows 7.

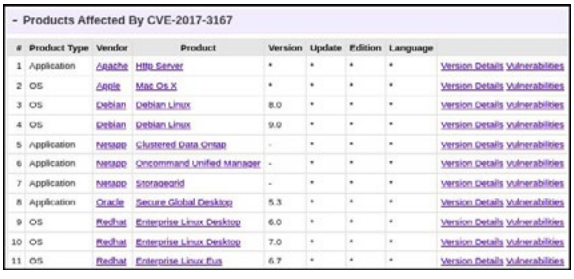


Figura 12. Resultados CVE – productos afectados

Ya que no hemos tenido éxito en la búsqueda de exploits para esta vulnerabilidad, continuamos con el flujo y seleccionamos la siguiente vulnerabilidad en la lista. Como podemos ver en la figura 13, hemos encontrado la vulnerabilidad MS17-010 del protocolo smb.

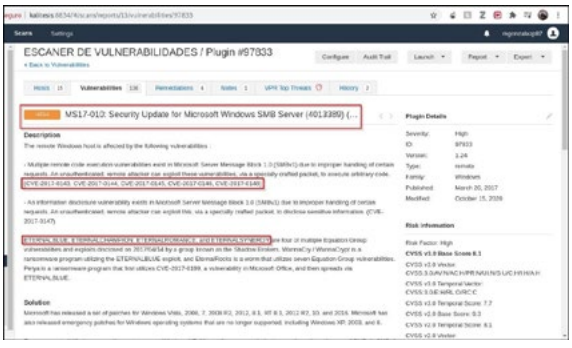


Figura 13. Información Nessus - vulnerabilidad MS17-010

Haciendo una búsqueda rápida en Google, encontramos que la vulnerabilidad MS17-010 o más conocida como Eternal Blue [30], es una vulnerabilidad muy destacada, es explotable en sistemas Windows y permite la ejecución de código remoto que es lo que buscamos. Dando seguimiento al hallazgo, realizamos una búsqueda en Metasploit Framework y encontramos el exploit ms17_010_eternalblue (figura 14), por lo que procedemos a la siguiente fase.

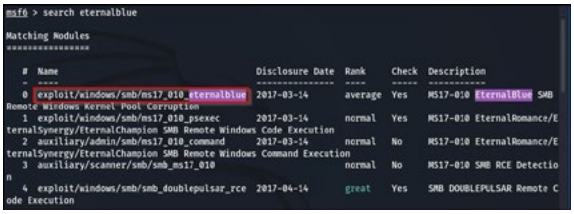


Figura 14. Resultados Metasploit Framework – Búsqueda eternalblue

2.4.4 Explotación

La explotación es la fase más sencilla, si hemos realizado bien las fases anteriores. En este caso hemos encontrado el exploit eternalblue en la herramienta Metasploit Framework, por lo que procedemos a seleccionarlo para su uso con el comando use, tal como se observa en la figura 15. En la misma podemos observar también, el payload cargado por defecto. Si no tenemos problema con el payload seleccionado, procedemos a configurar el parámetro rhosts con la dirección IP del objetivo, y finalmente utilizamos el comando run para ejecutar el payload. Si todo se ejecuta de manera adecuada, veremos la palabra WIN (o FAIL en el caso de que el exploit ha fallado) y en la última línea de la terminal de comandos, el prompt de nuestro Shell remoto.

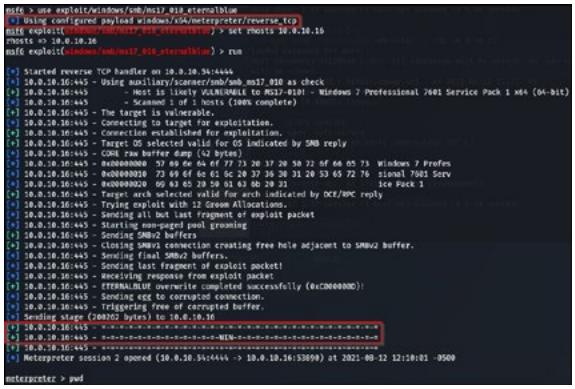


Figura 15. Resultados Metasploit Framework – Selección y ejecución de exploit

En este caso, el payload seleccionado ha funcionado en el primer intento. Dependiendo de varios factores, puede ser necesario ejecutar el exploit un par de veces para que funcione, o en otros casos será necesario cambiar el tipo de payload (modular o no modular, reverse o bind) hasta encontrar uno q funcione.

En este punto, el auditor puede ejecutar comandos para comprobar el nivel de privilegios (ver figura 16), revisar configuraciones, o realizar acciones de post explotación como escalar privilegios. Para nuestra metodología, hemos cumplido en demostrar una explotación exitosa por lo que documentamos todo el proceso, notificamos a la Gerencia o Dirección de Tecnología, y pasamos a la siguiente fase.

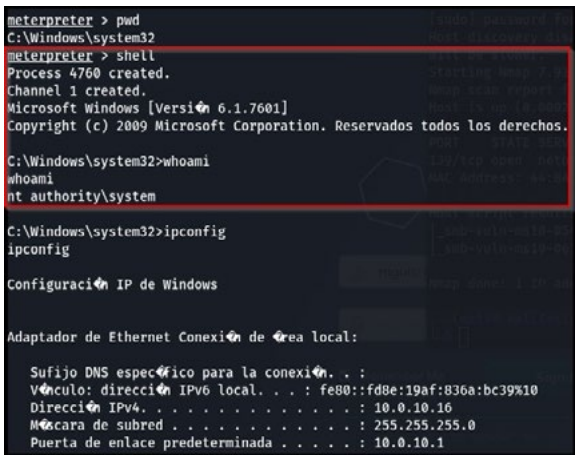


Figura 16. Metasploit Framework – Sesión de Meterpreter

2.4.5 Reporte

El reporte final elaborado para este caso es extenso y contiene información sensible que de ser publicada podría llegar a comprometer la seguridad de la empresa, por lo que el mismo fue entregado directamente a la gerencia para su gestión interna. Las indicaciones para la elaboración del reporte se encuentran en el apartado 2.3.5.

3. Resultados y Discusión

La figura 17 nos muestra un numero alarmante de vulnerabilidades encontradas, sobre todo si consideramos el tamaño de la infraestructura. Las amenazas de severidad critica señalan una infraestructura altamente vulnerable que fácilmente podría ser comprometida y pondría en riesgo los activos digitales de la empresa.

Figura 17. Nessus – Resultados generales

Las herramientas utilizadas para hacerlo además de un computador y un navegador de internet fueron, Kali Linux, Nmap, y Nessus, las cuales son herramientas gratuitas (Nessus permite escanear hasta 16 hosts en su versión gratuita) coincidiendo con el Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe (2020) en el bajo costo que requiere un ataque informático. Así mismo, la implementación de la metodología en el caso de estudio ha tomado alrededor de 20 horas de trabajo, dando un promedio de 4 horas por fase, el cual podrá variar en cada caso, dependiendo del alcance del test y la experiencia del auditor.

Cabe destacar, que la explotación fue relativamente fácil, seguramente debido al alto número de vulnerabilidades presentes en la infraestructura. También se verificó que la empresa continúa utilizando software desatendido como es el caso del sistema operativo Windows 7. Esto quiere decir que el sistema utilizado ya no recibe actualizaciones de seguridad y por lo tanto es vulnerable.

Resulta evidente pensar que en la empresa, la seguridad de la información no es un tema prioritario, probablemente por desconocimiento del riesgo al que están expuestos, ya sea por parte de la gerencia o por el área de TI. Dado que no podemos generalizar los resultados, esperamos que el caso sea aislado.

Cabe destacar la importancia de una fase previa a la ejecución de una prueba de intrusión, como lo es en este caso la Definición del Alcance. Si bien en la metodología propuesta, es una fase muy pequeña, nos permite obtener información relevante y los documentos necesarios para elaborar una adecuada planificación que garantice la ejecución del test en un ambiente seguro tanto para el cliente como para el auditor.

4. Conclusiones y recomendaciones

Los resultados del caso de estudio nos proveen una clara idea de cómo se gestiona la seguridad en las empresas pequeñas. A experiencia del autor, el escenario es genérico y se repite en la mayoría de los casos. La implementación de soluciones basadas en hardware y software como firewalls y antivirus proporcionan un falso sentido de seguridad, en la que los profesionales de TI entran en una zona de confort básicamente a la espera de

ataques informáticos y poniendo en riesgo los activos tecnológicos de las empresas. En ese sentido, es necesario considerar a la seguridad de la información desde un enfoque holístico, como una solución integral que considere los aspectos tanto técnicos como no técnicos de una empresa, como infraestructura, personal, políticas, etc., y no como la suma de herramientas que trabajan de forma aislada.

Al igual que las otras metodologías analizadas, la metodología propuesta contempla todos los pasos de un proceso genérico de pentest, sin embargo, al tener una orientación al análisis de red, permite ser mas especifica en sus requerimientos. Esto minimiza la ambigüedad en la comprensión de criterios, que, en comparación con las otras metodologías, complican su implementación

En este aspecto, la metodología presentada ha cumplido con los objetivos propuestos al ofrecer una herramienta útil, completa y sencilla en su ejecución. La aplicación del caso de estudio nos permitió comprobar su efectividad al analizar una infraestructura tecnológica, encontrar sus vulnerabilidades y darles seguimiento hasta obtener una explotación exitosa. El reporte final nos da una idea de los riesgos a los que está expuesto la infraestructura, a la vez que compromete a la Dirección de Tecnologías a subsanar las mismas y a tomar acciones para prevenir riesgos futuros o mitigar su impacto.

La brecha de profesionales en el área de seguridad de la información se hace tangible cuando encontramos infraestructuras tan desatendidas que demuestran el poco conocimiento de los profesionales a cargo, y que se traduce en empresas susceptibles a todo tipo de ataques. La seguridad de la información debería ser un tema de interés para todo tipo de empresas, y la socialización de este tipo de temas a través de talleres y capacitaciones a su personal, generando una cultura de seguridad, una prioridad.

Se considera que el método propuesto puede ayudar a cubrir, de cierta forma, el déficit de profesionales de ciberseguridad, ya que es una herramienta simple, pero a la vez efectiva, requiere de pocos recursos (humanos, económicos y tiempo) y es relativamente fácil de ejecutar. Como en el caso de cualquier auditoria de seguridad, es muy importante implementarla de manera periódica, sea semestral o anual, de esta forma podemos llevar un control de la efectividad de las acciones tomadas y soluciones provistas para los riesgos encontrados. Lo más beneficioso de todo esto, es que se establece una cultura de seguridad en las empresas, sin importar su tamaño.

Bibliografía

[1] M. L. S. Limón y M. H. D. la G. Cárdenas, “Tecnologías de información y desempeño organizacional de las pymes del noreste de México”, *Rev. Venez. Gerenc.*, vol. 23, núm. 82, pp. 298–313, 2018.

[2] E. J. Santiago y J. Sánchez Allende, “Riesgos de ciberseguridad en las Empresas”, *Tecnol. Desarro.*, vol. 15, núm. 0, Art. núm. 0, dic. 2017, Consultado: el 9 de enero de 2022. [En línea]. Disponible en: https://revistas.uax.es/index.php/tec_des/article/view/1174

[3] K.-K. R. Choo, “The cyber threat landscape: Challenges and future research directions”, *Comput. Secur.*, vol. 30, núm. 8, pp. 719–731, nov. 2011, doi: 10.1016/j.cose.2011.08.004.

[4] “Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe”, Banco Interamericano de Desarrollo, 2020,

2020. Consultado: el 14 de agosto de 2020. [En línea]. Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

[5] "MAPA | Mapa en tiempo real de amenazas cibernéticas Kaspersky", *MAPA | Mapa en tiempo real de amenazas cibernéticas Kaspersky*. https://cybermap.kaspersky.com/es (consultado el 13 de enero de 2022).

[6] "The Top 6 Industries At Risk For Cyber Attacks - RedTeam Security". https://www.redteamsecure.com/blog/the-top-6-industries-at-risk-for-cyber-attacks (consultado el 29 de marzo de 2022).

[7] R. Vargas Borbúa, L. Recalde Herrera, y R. P. Reyes Ch., "Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa", *Cyber-defense and cybersecurity, beyond the virtual world: Ecuadorian model of cyber-defense governance*, jun. 2017, Consultado: el 14 de agosto de 2020. [En línea]. Disponible en: http://repositorio.flacsoandes.edu.ec/handle/10469/12199

[8] D. Santo Orcero, *Pentesting con Kali: aprende a dominar la herramienta Kali para hacer tests de penetración y auditorías activas de seguridad*. 2018.

[9] M. Ortiz Osorio, "Importancia de las buenas prácticas en ciberseguridad en el trabajo remoto de entidades públicas de Colombia en época de pandemia.", nov. 2021, Consultado: el 13 de enero de 2022. [En línea]. Disponible en: http://repository.unad.edu.co/handle/10596/44501

[10] R. Gonzalez, "Estiman en $87 mil 940 millones pérdidas anuales por ataques cibernéticos | La Prensa Panamá", *La Prensa*, el 20 de junio de 2019. Consultado: el 7 de agosto de 2020. [En línea]. Disponible en: https://www.prensa.com/economia/Estiman-millones-perdidas-anuales-ciberneticos_0_5331966763.html

[11] U. Akyazi, "Measuring Cybercrime as a Service (CaaS) Offerings in a Cybercrime Forum", p. 15, 2021.

[12] Á. M. Rea Guamán, "Madurez en la identificación y evaluación de riesgos en ciberseguridad", phd, E.T.S. de Ingenieros Informáticos (UPM), 2020. Consultado: el 9 de enero de 2022. [En línea]. Disponible en: https://doi.org/10.20868/UPM.thesis.65871

[13] J. A. Figueroa-Suárez, R. F. Rodríguez-Andrade, C. C. Bone-Obando, y J. A. Saltos-Gómez, "La seguridad informática y la seguridad de la información", *Polo Conoc.*, vol. 2, núm. 12, Art. núm. 12, mar. 2018, doi: 10.23857/pc.v2i12.420.

[14] V. Greavu Serban y O. Serban, "Social Engineering A General Approach", *Inform. Econ.*, vol. 18, núm. 2/2014, pp. 5–14, jun. 2014, doi: 10.12948/issn14531305/18.2.2014.01.

[15] J. L. Guillen Zafra, "Introducción al pentesting", Universitat de Barcelona, 2017. [En línea]. Disponible en: http://diposit.ub.edu/dspace/bitstream/2445/124085/2/memoria.pdf

[16] V. Casola, A. De Benedictis, M. Rak, y

U. Villano, “Towards Automated Penetration Testing for Cloud Applications”, en *2018 IEEE 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, jun. 2018, pp. 24–29. doi: 10.1109/WETICE.2018.00012.

[17] J. S. Ferrer Bustos, “Pruebas de penetración en las redes de datos en cualquier entidad pública o privada.”, mar. 2021, Consultado: el 10 de enero de 2022. [En línea]. Disponible en: http://repository.unad.edu.co/handle/10596/40111

[18] “The Penetration Testing Execution Standard”. http://www.pentest-standard.org/index.php/Main_Page (consultado el 6 de junio de 2020).

[19] ISECOM, “OSSTMM 3”. 2010. [En línea]. Disponible en: www.isecom.org/OSSTMM.3.pdf

[20] kaitlin.boeckl@nist.gov, “NIST SP 800-115”, NIST, el 12 de enero de 2020. https://www.nist.gov/privacy-framework/nist-sp-800-115 (consultado el 13 de enero de 2022).

[21] C. A. Castro Vasquez, “Pruebas de penetración e intrusión”, jul. 2019, Consultado: el 10 de enero de 2022. [En línea]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/6273

[22] N. J. van den Hout, “Standardised Penetration Testing? Examining the Usefulness of Current Penetration Testing Methodologies”, Royal Holloway, University of London, 2019. [En línea]. Disponible en: https://www.researchgate.net/publication/335652869_Standardised_Penetration_Testing_Examining_the_Usefulness_of_Current_Penetration_Testing_Methodologies

[23] G. Chávez Cruz, J. Campuzano Vásquez, y V. Betancourt Gonzaga, “Las micro, pequeñas y medianas empresas. Clasificación para su estudio en la carrera de Ingeniería en Contabilidad y Auditoría de la Universidad Técnica de Machala”, Conrado, vol. 14, pp. 247–255, dic. 2018.

[24] Ec Council, *CEH Ethical Hacking and Countermeasures* v11. 2020.

[25] D. Dalalana Bertoglio y A. F. Zorzo, “Overview and open issues on penetration test”, *J. Braz. Comput. Soc.*, vol. 23, núm. 1, p. 2, feb. 2017, doi: 10.1186/s13173-017-0051-1.

[26] R. Slayton, “Certifying ‘ethical hackers’”, *ACM SIGCAS Comput. Soc.*, vol. 47, núm. 4, pp. 145–150, jul. 2018, doi: 10.1145/3243141.3243156.

[27] O. Sierra, “ANALISIS Y PRUEBAS DE NIVELES DE SEGURIDAD DE LA INFORMACIÓN BASADOS EN LAS GUIAS DEL OSSTMM v3”, p. 11, nov. 2018.

[28] G. P. Gasca Hurtado, “Estudio de similitud del proceso de gestión de riesgos en proyectos de outsourcing de software: utilización de un método”, *Rev. Ing. Univ. Medellín*, vol. 9, núm. 17, pp. 119–130, jul. 2010.

[29] R. Martí y J. Lloret, “Desarrollo e implementación práctica de un PENTEST”, sep. 2016, Consultado: el 25 de agosto de 2020. [En línea]. Disponible

en: https://riunet.upv.es/handle/10251/70164

[30] Z. Liu, "Working mechanism of Eternalblue and its application in ransomworm", *ArXiv211214773 Cs*, dic. 2021, Consultado: el 17 de enero de 2022. [En línea]. Disponible en: http://arxiv.org/abs/2112.14773

ISSN IMPRESO: 2528-8008
ISSN ELECTRÓNICO: 2588-0888