



Facultad
de Informática
y Electrónica



REVISTA PERSPECTIVAS

REVISTA TÉCNICA CIENTÍFICA DE LA FIE



▀ ENERO - JUNIO 2024

e-ISSN: 2661-6688

VOL 6, N°1



epoch
**HACEMOS
HISTORIA**



REVISTA PERSPECTIVAS

REVISTA TÉCNICA CIENTÍFICA DE LA FIE

▀ **ENERO - JUNIO 2024**

e - ISSN: 2661 - 6688

VOL 6, N°1

RIOBAMBA - ECUADOR



epoch
**HACEMOS
HISTORIA**



epoch

Facultad de
Informática y
Electrónica

Instituto de
Investigaciones

Dirección de
Publicaciones



REVISTA PERSPECTIVAS

PRÓXIMA
CONVOCATORIA

JULIO - DICIEMBRE 2024

<http://perspectivas.esPOCH.edu.ec/>

CONVOCATORIA DE RECEPCIÓN DE MANUSCRITOS

PERIODICIDAD SEMESTRAL

1ERA. CONVOCATORIA:

Recepción abierta hasta Octubre

Publicación: Enero

2DA. CONVOCATORIA:

Recepción abierta hasta Abril

Publicación: Julio



esPOCH
**HACEMOS
HISTORIA**



esPOCH Facultad de
Informática y
Electrónica



COMITÉ EDITORIAL

• **DIRECTOR**

Omar S. Gómez, Ph.D.

Escuela Superior Politécnica de Chimborazo (Ecuador)

• **EDITOR EJECUTIVO**

Raúl H. Rosero, Ph.D.

Escuela Superior Politécnica de Chimborazo (Ecuador)

• **EDITORES ASOCIADOS**

Raúl Antonio Aguilar Vera, Ph.D.

Universidad Autónoma de Yucatán (México)

Jesús Pardo Calvache, Ph.D.

Universidad del Cauca (Colombia)

Rosa Sumactika Delgadillo Avila de Mauricio, Ph.D.

Universidad Nacional Mayor de San Marcos (Perú)

George Enrique Figueras Benítez, Ph.D.

Universidad Simón Bolívar (Venezuela)

Luis Antonio Rivera Escriba, Ph.D.

Universidade Estadual do Norte Fluminense (Brasil)

Talia Beatriz Tene Fernandez, Ph.D.

Universidad Técnica Particular de Loja (Ecuador)

• **SECRETARIO CIENTÍFICO**

Mayra A. Pacheco Cunduri, M.Sc.

Escuela Superior Politécnica de Chimborazo (Ecuador)

• **COORDINACIÓN PROCESO PUBLICACIÓN**

Diego Avila Pesántez, M.Sc.

Escuela Superior Politécnica de Chimborazo (Ecuador)

• **REVISORES DE IDIOMA INGLÉS**

Nelly Padilla Padilla, M.Sc.

Escuela Superior Politécnica de Chimborazo (Ecuador)

• **DISEÑO Y DIAGRAMACIÓN**

Rosa Ramos Jiménez, M.A.

Escuela Superior Politécnica de Chimborazo (Ecuador)

Lcdo. José Luis Heredia Hermida Mgtr.

Escuela Superior Politécnica de Chimborazo (Ecuador)



COMITÉ CIENTÍFICO

Lorena Molina Valdiviezo, Ph.D.
Universidad Nacional de Chimborazo (Ecuador)

Eliana Acurio Méndez, Ph.D.
Escuela Politécnica Nacional (Ecuador)

Miguel Delgado Prieto, Ph.D.
Universidad Politécnica de Cataluña (Ecuador)

Luis Miguel Procel Moya, Ph.D.
Universidad San Francisco de Quito (Ecuador)

Luis Tello Oquendo, Ph.D.
Universidad Nacional de Chimborazo (Ecuador)

Cristian Vacacela Gómez, Ph.D.
Universidad Yachay Tech (Ecuador)

Ciro Radicelli García, Ph.D.
Universidad Nacional de Chimborazo (Ecuador)

Lorena Guachi Guachi Núñez, Ph.D.
Universidad Yachay Tech (Ecuador)

Patricio Humanante Rámos, Ph.D.
Universidad Nacional de Chimborazo (Ecuador)

Edison Taco Lasso, Ph.D.
Universidad San Francisco de Quito (Ecuador)

Edison Espinosa, Ph.D.
Filiación: Universidad de las Fuerzas Armadas (Ecuador)

Maricela Jiménez Rodríguez, Ph.D.
Filiación: Universidad de Guadalajara (México)

Juan Carlos Estrada, Ph.D.
Filiación: Universidad de Guadalajara (México)



CONTENIDO

PRESENTACIÓN

- | | |
|----------------|---|
| 1 - 12 | Análisis comparativo de modelos de propagación para comunicaciones en entornos acústicos submarinos |
| 13 - 26 | Exploración integral de la seguridad en redes de proveedores de servicios de internet: una revisión sistemática de literatura |
| 27 - 40 | Cifrado de texto mediante atractores caóticos: cryptoguard |
| 41 - 58 | Pérdidas económicas y peligros que representan las malas conexiones eléctricas |
| 59 - 72 | Desarrollo de una aplicación web para la graficación de atractores caóticos utilizando la metodología scrum |
| 73 - 82 | Recursos educativos multimedia para el fomento del patrimonio cultural inmaterial: Identificación de personajes festivos populares chimboracenses |



PRESENTACIÓN

Apreciables lectores,

En este año que inicia, hacemos de su conocimiento la publicación del número 1 del volumen 6 de la revista Perspectivas. En este número se encuentran disponibles publicaciones afines a las áreas de informática, electrónica, telecomunicaciones y diseño. Sabemos que los contenidos ofrecidos en este número serán de interés para nuestra comunidad de lectores.

Reiteramos nuestro agradecimiento todos aquellos quienes han hecho posible mantener la continuidad de esta revista, a nuestros autores por sus contribuciones y por confiar en

este medio de divulgación técnico-científica, a nuestro equipo de revisores que dedican parte de su tiempo en el proceso de revisión con el fin de contar con publicaciones de mayor calidad. Agradecemos también al equipo editorial así como a nuestras autoridades institucionales.

Recordamos a nuestra comunidad que continua abierta la recepción de manuscritos, los cuales tras su correspondiente proceso de revisión y aceptación se publicarán en los números correspondientes de este año.

**Cordialmente,
EQUIPO EDITORIAL**

Saber para Ser !

ANÁLISIS COMPARATIVO DE MODELOS DE PROPAGACIÓN PARA COMUNICACIONES EN ENTORNOS ACÚSTICOS SUBMARINOS

Comparative analysis of propagation models for communications in underwater acoustic environments

Erika Viviana Ñaupá Shagñay ¹	erika.niaupa@esPOCH.edu.ec
Stalin Bolívar Molina Molina ²	stalin.molina@esPOCH.edu.ec

^{1,2} Telecomunicaciones, Escuela Superior Politécnica de Chimborazo (ESPOCH) Riobamba, Ecuador.

RESUMEN

Este documento presenta un análisis comparativo de los modos de propagación referente a la importancia de la forma del perfil de la velocidad del sonido, y para determinar la pérdida de transmisión del campo acústico generado por ondas acústicas que se propaga en el agua.

Estos son usados para obtener la representación gráfica de las pérdidas de transmisión dependiendo de la distancia y la profundidad. Se obtienen las respectivas graficas a raíz de su simulación según el modo propagado y la contribución lateral de la onda, de esa forma con los parámetros que se exponen se determina el modelo más eficiente en propagación acústica. La comparativa radica en ver los detalles de cada modelo y tener en cuenta a más de la eficiencia los errores que también pueden existir, además de ello en conjunto con minúsculos detalles suscritos, aprender varias teorías para llegar a un resultado propicio.

Palabras Clave: Modelos, distancia, pérdidas, profundidad, propagación, rayos.

to determine the transmission loss of the acoustic field generated by an acoustic wave propagating in water.

These modes are used to obtain the graphical representation of the transmission loss depending on distance and depth. The respective graphs are obtained as a result of their simulation taking into account the propagated mode and the lateral contribution of the wave, thus with the parameters that are exposed can determine the most efficient model when used in acoustic propagation. The comparative lies in seeing the details of each model and in such a way to observe, to be able to take into account in addition to the efficiency the errors that can also exist, in addition to it in conjunction with tiny details subscribed, to learn several theories to arrive at a propitious result.

Keywords: Models, distance, losses, depth, propagation, lightning.

ABSTRACT

This paper presents a comparative analysis of the propagation modes with respect to the importance of the shape of the sound velocity profile, and also

► I. Introducción

La comunicación acústica subacuática es un método para enviar y recibir mensajes bajo el agua [1]. Se ha utilizado en una variedad de tareas, incluida la vigilancia del medio ambiente, el control de vehículos submarinos, el análisis del fondo marino y la detección de objetos. La utilización de ondas acústicas es un patrón repetido en todas

ellas. Esto se debe a las características que tiene este tipo de medios, que lo hacen ideal para su uso en comparación con las ondas electromagnéticas. Aunque las ondas acústicas son mejores para las comunicaciones submarinas, también hay muchos desafíos que tener en cuenta. El océano y los mares son los principales medios subacuáticos [2].

Se puede considerar que este medio tiene efectos similares a los de la atmósfera, como atenuación y absorción, presencia de ruido y multicamino, la atenuación por absorción es uno de los principales efectos observados: una onda electromagnética experimenta una disminución en función de su frecuencia. La alta conductividad del agua del mar es la causa de esta pérdida de intensidad. Se observan múltiples caminos creados por el rebote de las ondas tanto en la superficie como en el fondo marino cuando es necesario establecer una comunicación a determinada distancia entre transmisor y receptor. Por lo tanto, es necesario desarrollar un modelo del medio subacuático para facilitar la comunicación.

En este artículo se describe la propagación de señales en entornos subacuáticos, mismas que cobran una importancia análoga a la radiofrecuencia en aire, la acústica subacuática que implica el desarrollo y el empleo de métodos acústicos para obtener imágenes de las características submarinas, para comunicar información a través del agua, guía de ondas, o para medir las propiedades oceánicas. Se aborda los parámetros fundamentales de los que depende la propagación acústica en el agua y los 3 modelos existentes que estudian dicha propagación.

En su sentido más fundamental, el modelado es un método para organizar el conocimiento acumulado a través de la observación o deducido de los principios subyacentes [3]. A continuación se menciona de manera rápida los resultados que proporciona el modelo de trazado de rayos, siendo el más utilizado, este modelo se basa en la consideración de que la energía de la onda se puede concentrar en caminos definidos, de manera que se puede pensar en rayos en lugar de ondas y esto viene a ser válido siempre que la amplitud de la onda y la velocidad del sonido no

sea tan variante en una longitud de onda, dicho esto, la condición se cumplirá mejor para altas frecuencias, puesto que la longitud de onda será más pequeña. El modelo de trazado de rayos lo que hace es calcular las ecuaciones que siguen los rayos, utilizando la herramienta de simulación Matlab para una comparación eficiente entre gráficos de los distintos campos a tratar dentro de cada modelo: un ejemplo es el campo de presiones que generan, del cual se puede obtener las pérdidas de transmisión, y el tiempo de propagación de dichos rayos.

► II. Canal acústico subacuático

Una estructura destinada a transmitir señales acústicas por largos períodos de tiempo a través del agua se conoce como línea de transmisión acústica subacuática [4]. Existen parámetros importantes como la velocidad del sonido y la pérdida de transmisión de cada elemento. A continuación, se analizarán los distintos parámetros que influyen en el modelado del canal submarino.

A. Velocidad del sonido

La velocidad de propagación de las ondas de sonido es un parámetro que describe cómo se desplazan en el medio [5]. Las ondas acústicas corresponden a un tipo especial de ondas: las ondas mecánicas. La peculiaridad de este tipo de ondas es que dependen de un medio elástico. Esto permite la propagación de perturbaciones a través de dicho medio [6].

Además, es la velocidad a la que una onda longitudinal recorre un medio determinado, creando un continuo de compresión y expansión, que el cerebro interpreta como sonido [7]. El "perfil de velocidad del sonido", muestra los cambios en la velocidad de propagación del sonido en función de la profundidad del océano mediante ilustraciones. La ubicación geográfica, la estación y las condiciones meteorológicas pueden ser factores que afectan esta representación [8]; viene determinado por la relación entre la velocidad del sonido y la profundidad, influirá en la forma en que se propague la irrupción acústica. La ecuación

de la velocidad del sonido se obtiene a partir de la misma ecuación de onda lineal:

$$C = \sqrt{\frac{\gamma B_T}{\rho_0}} \quad (1)$$

Donde, c es la velocidad del sonido en m/s, γ es el índice adiabático, ρ_0 es la densidad de equilibrio, B_T es el módulo de compresibilidad isotérmica.

A su vez, estas magnitudes dependen de otros parámetros, como la temperatura, la salinidad y la presión del agua. El valor típico de la velocidad de una onda acústica es de media 1500 m/s, aunque puede tomar valores entre 1450 y 1550 m/s [9]. Es crucial comprender cómo se producen las variaciones en la velocidad del sonido en función de los parámetros mencionados anteriormente. Es necesario investigar cómo estos parámetros cambian a su vez con respecto a la profundidad para lograrlo.

Tabla I.

VALORES DE DENSIDAD Y VELOCIDAD DEL SONIDO

Medio	Densidad [Kg/m ³]	Velocidad del sonido [m/s]
Aire	1,2	340
Agua	1030	1500
Aceites	900	1200-1700
Aluminio	2700	5000-6000
Resinas y plásticos	1000-1500	1000-2000

La temperatura del agua (mar, ríos grandes, etc.) disminuye hacia el fondo desde la superficie. En las capas menos profundas, la variación es más alta debido a una variedad de factores, como la combinación de corrientes de agua, el calor de la luz solar y las estaciones del año [10]. El valor promedio de la temperatura disminuye ligeramente con la profundidad a medida que aumenta la profundidad.

La presión hidrostática es la responsable directa de los cambios en la velocidad del sonido con respecto a la profundidad [11]. Cuando se trata de aguas marinas, también están formadas por una mezcla de agua pura y sales disueltas.

A lo largo de los años se han estudiado diferentes ecuaciones semi-empíricas para expresar la velocidad del sonido en ambientes marinos. Por

lo tanto, se realizan mediciones de los diversos parámetros involucrados, como la temperatura, la presión y la concentración de sal, de las cuales las dos ecuaciones más utilizables son las Del Grosso y Chen y Millero [12]. La ecuación de Grosso, Ec. 2 data de 1974. Los términos son función de la temperatura T , la presión P y la salinidad S .

$$c(S,T,P) = 1402,392 + \Delta C_S + \Delta C_T + \Delta C_P + \Delta C_{STP} \quad (2)$$

Por otro lado, existe la ecuación de Chen y Millero, Ec. 3 expuesta en 1977, de igual forma los términos son función de la temperatura T , presión P y salinidad S , además esta ecuación fue reconocida por la UNESCO como estándar para el cálculo de la velocidad de propagación en ambientes marinos [13].

$$c(S,T,P) = c_0 + c_1 P + c_2 P^2 + c_3 P^3 + AS + BS^{\frac{3}{2}} + CS^2 \quad (3)$$

1. Perfil de la velocidad del sonido

Con los perfiles de velocidad se puede determinar de qué forma se va a propagar una señal acústica por este tipo de medios existen zonas donde la velocidad del sonido es diferente, pues aparece una curvatura de las ondas acústicas cuando son transmitidas en zonas de velocidad baja.

Es posible generar gráficos de la velocidad del sonido en función de la profundidad, denominados perfiles de velocidad. En el caso de las latitudes medias, se representa un tipo de perfil dividido en diferentes capas, cada una con sus propias características, como se muestra en la Fig. 1.

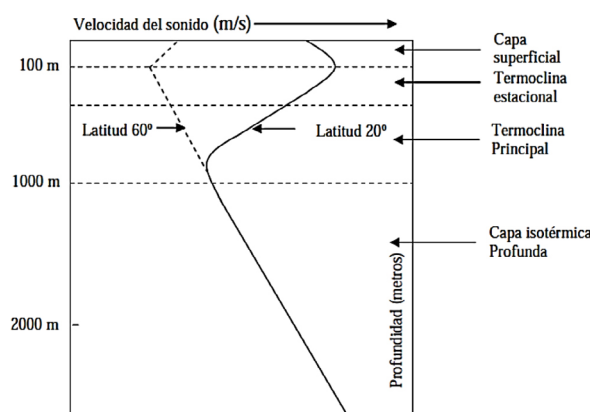


Fig. 1. Perfiles de velocidad del sonido.

Sin embargo, las diferentes capas se detallan a continuación:

- **Capa superficial:** comprendida entre la superficie y una profundidad que varía entre los primeros 50 m y los 100 m. Se ve afectada por el movimiento de las masas de agua (en este caso). A lo largo de esta capa, la velocidad permanece prácticamente constante [14].
- **Termoclina estacional:** se extiende aproximadamente entre 100 m y 200 m, dependiendo de la hora del día, las latitudes y la estación del año. Presenta una variación de temperatura prácticamente monótona, con un gradiente positivo.
- **Termoclina principal:** Se extiende desde los límites de la capa anterior hasta 1600 m o 2000 m de profundidad. Se produce un descenso aproximadamente lineal de la temperatura y, a su vez, una disminución de la velocidad.
- **Isoterma profunda:** temperatura constante. La velocidad aumenta linealmente con la profundidad (debido a la presión hidrostática), el perfil es aproximadamente lineal.

B. Modelo de trazado de rayos

En este modelo se menciona que la energía de una onda puede concentrarse en trayectorias claramente definidas, por lo que es posible considerar rayos en lugar de ondas. Esto es válido siempre que la amplitud de la onda y la velocidad del sonido no varíen considerablemente a lo largo de una longitud de onda [15]. Aquí se estudian básicamente los efectos de refracción de los rayos sonoros en medios donde la velocidad del sonido varía con la profundidad, pero con un comportamiento constante en diferentes capas horizontales a lo largo de toda la columna de agua. "Además, se considera que la reflexión es de tipo especular, por lo que la pérdida de energía es mínima" [16].

C. Pérdidas de transmisión

Hay dos factores tras los cuales la presión de irrupción pierde energía en el CAS, dando lugar a

TL (pérdidas de transmisión) [17].

1. Por un lado, están las pérdidas geométricas TL_g , que se deben a que la energía de la onda entrante se dispersa por una superficie mayor.

$$TL_g = 10klogd \quad (4)$$

Donde, d es la distancia de enlace en metros y k es el factor de propagación (1 para propagación cilíndrica, 2 para propagación esférica, 1,5 para propagación intermedia).

2. El otro componente de las pérdidas por transmisión se debe al efecto de absorción de la energía acústica por el medio, TL_α .

$$TL_\alpha = \alpha \cdot d \quad (5)$$

Donde, α (dB/km) es el coeficiente de absorción, que depende de los parámetros del agua y de la frecuencia de la onda. Una de las expresiones semi empíricas más utilizadas para este coeficiente es la de Thorp, validada hasta frecuencias en kilohercios, temperaturas de 4°C y una profundidad de 900 m [18].

$$\alpha = 0.11 \frac{f^2}{1+f^2} + 44 \frac{f^2}{4100+f^2} + 2.75 \cdot 10^{-4} f^2 + 0.0003 \quad (6)$$

Otra expresión más contemporánea es la dada por Francois y Garrison, que es apropiada para frecuencias entre 100 Hz y 1 MHz.

$$\alpha = \frac{A_1 P_1 f_1^2}{f^2 + f_1^2} + \frac{A_2 P_2 f_2^2}{f^2 + f_2^2} + A_3 P_3 f^2 \quad (7)$$

Así, las pérdidas por transmisión son:

$$TL = TL_g + TL_\alpha \quad (8)$$

» III. Modelos de Propagación

Existen varios modelos de propagación de señales acústicas, pero este artículo se centra en tres modelos que ponen de relieve la importancia de la forma del perfil de velocidad del sonido.

A. Propagación en aguas poco profundas

Según este concepto, la profundidad de la columna de agua es sólo un pequeño número de longitudes en tierra y, en consecuencia, la naturaleza ondulatoria del sonido determinará la distancia que puede recorrer. En este caso, también se indica que el número de reflexiones en la superficie aumenta por unidad de longitud. Esto significa que, en aguas poco profundas, la reflexión superficial y las pérdidas resultantes aumentan [19].

Para este caso, existe una interacción muy importante de la señal acústica con el fondo, posibles variaciones de profundidad, etc. que invocan el modelo de Colossus, obtenido a partir de una gama de frecuencias comprendida entre 100 Hz y 10 kHz [20]. Se tienen en cuenta la altura de las olas, el tipo de fondo, la profundidad de la columna de agua, la frecuencia y el perfil de velocidad del sonido.

Se considera que este perfil se compone de dos segmentos coherentes:

- Desde la superficie del océano hasta una profundidad de L (metros), la velocidad del sonido aumenta linealmente con la profundidad.
- A profundidades superiores a L, la velocidad disminuye a medida que aumenta la profundidad hasta llegar al fondo.

1. Distancia de transmisión (H): Distancia máxima a la que un rayo entra en contacto con la superficie o el fondo [21].

$$H = \sqrt{\frac{L + D}{3}} \tag{9}$$

Donde, D es la profundidad de la columna de agua en metros.

2. Pérdidas de transmisión (TL)

$$\left\{ \begin{array}{l} TL = 20\log R + \alpha R + 60 - k_L, \text{ para } R < H \\ TL = 15\log R + \alpha R + \alpha_T \left(\frac{R}{H} - 1 \right) + 5\log H + 60 \\ \quad - k_L, \text{ para } H < R < 8H \\ TL = 10\log R + \alpha R + \alpha_T \left(\frac{R}{H} - 1 \right) + 10\log H + 64.5 \\ \quad - k_L, \text{ para } R < 8H \end{array} \right.$$

Donde, R (Km) es la distancia, α (dB/Km) es el coeficiente de absorción, K_L (dB) es la anomalía de campo cercano, mide la ganancia debida a los rebotes entre el fondo y la superficie, y A_T (dB/rebote) es el coeficiente de atenuación efectiva, considera las pérdidas debidas al acoplamiento de energía entre la superficie y el fondo.

B. Canal superficial

El conducto superficial se refiere al hecho de que cuando los vientos superficiales y las olas mezclan las capas poco profundas del mar, se produce una capa isotérmica en la que domina el efecto de presión y la velocidad del sonido aumenta al aumentar la profundidad, con valores de profundidad en el rango de 50 a 100 m [22].

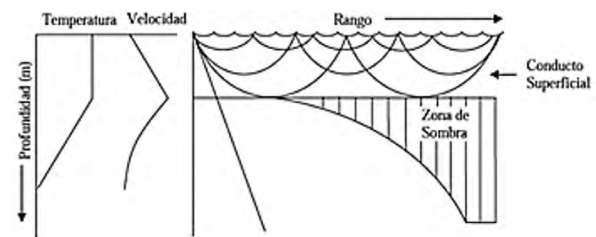


Fig. 2. Propagación del sonido a través del conducto superficial.

La señal se propaga esféricamente al principio, pero después de una distancia de transición r_t , la propagación puede considerarse cilíndrica, ya que la energía está confinada.

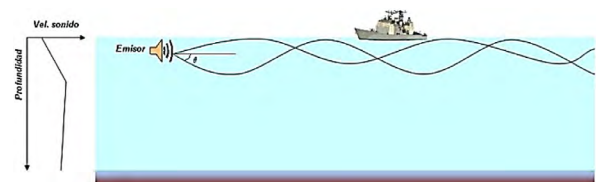


Fig. 3. Propagación a través del canal de superficie con ángulo de inclinación.

Expresando así las ecuaciones de pérdida de transmisión y distancia de transición.

1. Distancia de transición

$$r_t = \frac{0.3048}{2} H \sin \theta \tag{11}$$

Donde, H (m) es la profundidad del canal, y θ el ángulo del haz atrapado con la pendiente más pronunciada dentro del canal.

2. Pérdidas de transmisión

$$TL = 10\log r_t + 10\log r + (\alpha + \alpha_L)r \cdot 10^{-3} \quad (12)$$

Donde: r (m) es la distancia, α (dB/km) es el coeficiente de absorción y α_L (dB/km) es el coeficiente de fuga, que considera la energía que escapa del canal debido a la dispersión de la señal en la superficie y a la difusión transversal, originada por la discontinuidad del perfil de velocidad del sonido en la base del canal.

C. Canal acústico profundo

El haz del sonar se enfoca hacia abajo, hacia ángulos con una inclinación considerable respecto a la horizontal. La eficacia del método depende de las características del fondo marino, que puede ser absorbente o reflectante. Además, las pérdidas provocadas por el fondo dependen del ángulo de incidencia [23]. En este perfil, a una profundidad de aproximadamente 1 km, hay un mínimo en la velocidad del sonido que sirve de límite del canal acústico. Si una señal acústica se emite cerca y se curva hacia este mínimo, y el ángulo de emisión es suficientemente pequeño, la señal se propaga sin interactuar ni con la superficie ni con el suelo, formando un canal acústico profundo.

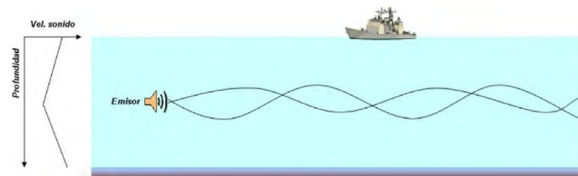


Fig. 4. Propagación a través del canal acústico profundo

La divergencia geométrica será inicialmente esférica hasta que alcance la distancia de transición r_t , momento en el que puede decirse que es cilíndrica.

1. Distancia de transición

$$r_t = \frac{r_s}{8} \sqrt{\left(\frac{D_s}{z_s}\right)} \quad (13)$$

Donde, D_s la profundidad a la que se encuentra la velocidad mínima del sonido en el canal superficial z_s es la profundidad del emisor medida desde la

base del canal superficial (que marca el inicio del canal más profundo), y r_s es la distancia del salto, que depende de las distancias entre el ecuador del canal superficial y sus límites.

2. Pérdidas de transmisión (TL): si y sólo si la distancia es tal que la divergencia ya es sustancial.

$$TL = 10\log r_t + 10\log r + (\alpha)r \cdot 10^{-3} \quad (14)$$

Donde: r (m) es la distancia, y α (dB/Km) es el coeficiente de absorción.

» IV. Metodología

Para poder evolucionar en el proceso del análisis comparativo de los modelos de propagación acústica descritos anteriormente, es importante conocer los resultados de los modelos expuestos en el software Matlab para poder ver los parámetros importantes, el perfil de velocidad del sonido, las pérdidas por transmisión, y una trayectoria de trazado de rayos donde se puede determinar cómo y cuántos han rebotado en la superficie o fondo de cada uno de los modelos.

Más adelante se mostrarán los gráficos de las simulaciones realizadas para los tres casos presentados: el canal de aguas poco profundas, el canal poco profundo y el canal acústico profundo. Recordando que el método de trazado de rayos es el utilizado en este tema.

En todas las simulaciones, se ha tenido en cuenta utilizar una cimentación de arena fina con una densidad de 1941 Kg/m³, una columna de agua con una densidad de 1024 Kg/m³, no se ha tenido en cuenta la presencia de ondas transversales en el fondo, haciendo que el fondo sea completamente plano como la superficie del océano.

Dado que se han supuesto superficies completamente planas y, por tanto, no hay incertidumbre en cuanto a la interacción de la señal con estas superficies, se ha tenido en cuenta la fase de los distintos rayos en el caso de pérdidas de transmisión (cálculo coherente).

A. Propagación en aguas poco profundas

Lo que se muestra en este modelo son los parámetros ya descritos anteriormente, pero en este caso con su respectiva simulación.

1. Perfil de la velocidad del sonido

Los datos considerados son los siguientes:

- El fondo es de 100 m de profundidad.
- La profundidad máxima es de 250 m.
- Velocidad constante en el agua de 1500 m/s.
- Velocidad constante en la arena final comparable a 1749 m/s.

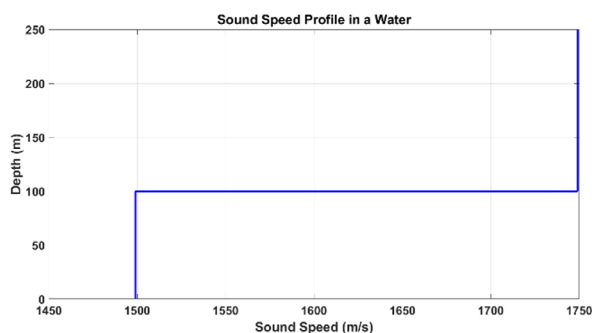


Fig. 5. Perfil de velocidad del sonido en aguas poco profundas.

En la Fig. 5, lo que se puede observar según los datos establecidos es que el fondo se identifica con la línea horizontal permaneciendo estable desde una velocidad constante en el agua igual a 1500 m/s hasta 1749 m/s (velocidad constante de la arena fina).

En la Fig. 5, lo que se puede observar según los datos establecidos es

2. Propagación de rayos

Los datos considerados son los siguientes:

- Número de rayos: 25 por razones de claridad visual.
- Se propone una red de receptores espaciados a 2 kilómetros de la fuente y colocados cada 5 metros de profundidad, comenzando las trayectorias de los rayos a 10 metros de profundidad.
- El ángulo de incidencia entre cada rayo es de 5° y la frecuencia es de 30 kHz.

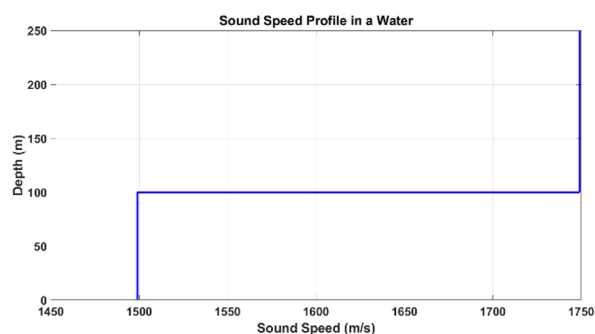


Fig. 6. Camino seguido por los rayos del sol en un entorno de aguas poco profundas.

En la Fig. 6, se puede observar que la trayectoria comienza a partir de los 10 metros de profundidad como se indica en los datos anteriores, la figura se ha adaptado para una mejor visualización, ya que los rebotes del fondo y la superficie se producen más allá de los 1500 metros, por este motivo la simulación se ha expuesto de esta forma, además en este modelo hay que tener en cuenta que hay rayos que llegan sin rebotar a la red receptora, mientras que otros sufren algún rebote con el fondo o la superficie, o varios rebotes con ambos.

3. Pérdidas de transmisión

Para este parámetro se tuvo en cuenta lo siguiente:

- El número de rayos es superior a 25, ya que para las pérdidas por transmisión la propia simulación tomó como referencia un número adecuado.
- A una profundidad de 10 metros empiezan a aparecer pérdidas por transmisión.
- La distancia es la misma en 2 km.

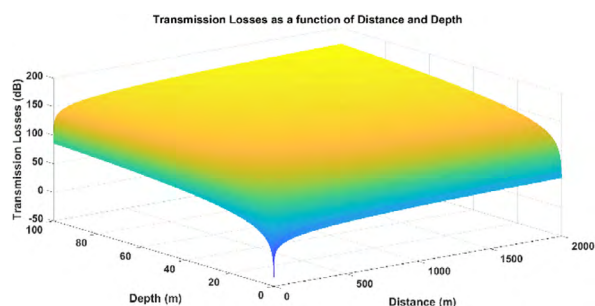


Fig. 7. Pérdidas de transmisión en entornos de aguas poco profundas en función de la distancia y la profundidad.

La Fig. 7 ilustra las pérdidas de transmisión en función de la distancia y la profundidad. Esta

ilustración muestra cómo hay zonas en las que la junta interactúa destructivamente en función de las fases de las juntas que convergen en esa zona, dando lugar a regiones en las que las pérdidas por transmisión disminuyen significativamente cerca del emisor.

B. Canal superficial

El canal de superficie desempeña un papel fundamental en el modelo de propagación de las comunicaciones submarinas y, para comprender sus características y considerar sus efectos en el diseño de los sistemas de comunicación, se han tenido en cuenta determinados valores de los criterios con los que se trabaja. Del mismo modo, se presentan los gráficos de las simulaciones de los tres parámetros considerados.

1. Perfil de la velocidad del sonido

Los datos considerados son los siguientes:

- El fondo es de 500 m de profundidad.
- La profundidad máxima es de 700 m.
- Velocidad en la superficie es de 1485 m/s.
- Velocidad constante en el agua de 1500 m/s.
- Velocidad constante en la arena final comparable a 1749 m/s.

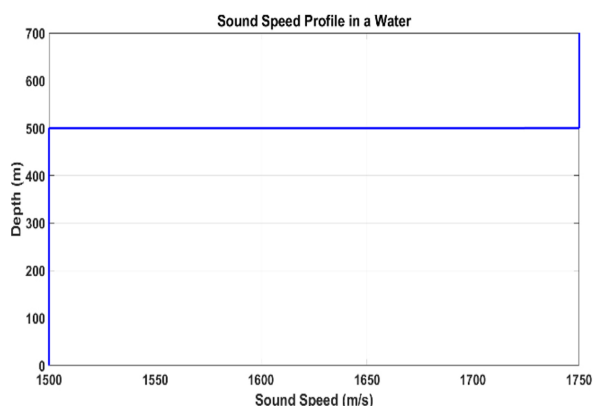


Fig. 8. Perfil de velocidad del sonido para el canal de superficie.

En la Fig. 8, lo que se observa es que el fondo está claramente representado por una horizontal que se mantiene constante a 500 metros, desde una velocidad de 1500 m/s hasta 1749 m/s o casi cerca de 1750 m/s. Estos datos se consideran debidos al modelo que estamos tratando.

2. Propagación de rayos

Los datos considerados son los siguientes:

- Número de rayos: 25 por razones de claridad visual.
- Se propone una red de receptores espaciados a 2 kilómetros de la fuente y colocados cada 5 metros de profundidad, iniciándose la trayectoria de los rayos a 50 metros de profundidad.
- El ángulo de incidencia entre cada rayo es de 5° y la frecuencia es de 20 kHz.

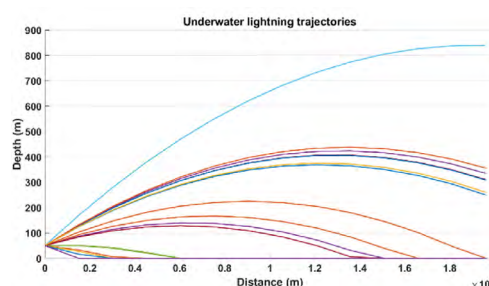


Fig. 9. Trayectoria seguida por los rayos en el canal de superficie.

La curvatura de los rayos hacia la superficie, donde se encuentra la velocidad mínima de la onda sonora, puede verse en la Fig. 9. En este caso, sólo hay repulsión con la superficie del océano a la distancia a la que se encuentran los receptores; no hay interacción con la subsuperficie.

3. Pérdidas de transmisión

Para este parámetro se tuvo en cuenta lo siguiente:

- El número de rayos es superior a 25, ya que para las pérdidas por transmisión la propia simulación tomó como referencia un número adecuado.
- A una profundidad de 50 metros empiezan a aparecer pérdidas por transmisión.
- La distancia se mantiene en 2 km.

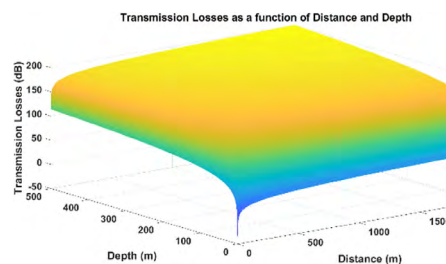


Fig. 10. Pérdidas de transmisión en el canal superficial en función de la distancia y la profundidad.

En la Fig. 10, se muestran las pérdidas por transmisión en función de la distancia y la profundidad. También se muestra un patrón de interferencias, formado por la interacción de los rayos con diversas fases. Parece que existe una región a 50 metros de profundidad y alejada de los receptores en la que las pérdidas son más conocidas.

C. Canal acústico profundo

Se debe recalcar que este patrón se produce generalmente a lo largo de cientos de metros hasta varios kilómetros, y que las señales acústicas pueden propagarse a grandes distancias.

La simulación final que se muestra es para el canal acústico profundo. Cabe mencionar que, para simular mejor en este modelo, se tomaron mayores medidas de profundidad, distancia y velocidad en comparación con los otros dos modelos.

1. Perfil de la velocidad del sonido

Los datos considerados son los siguientes

- La profundidad máxima es de 4500 m.
- El fondo es de 4000 m de profundidad.
- La velocidad en la superficie es de 1485 m/s.
- Velocidad constante en el agua de 1510 m/s.
- Velocidad constante en la arena final comparable a 1749 m/s.

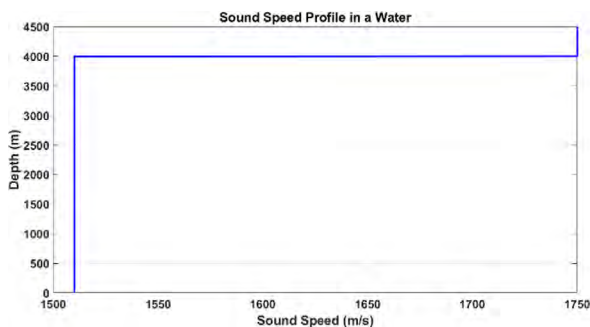


Fig. 11. Pérdidas de transmisión en el canal superficial en función de la distancia y la profundidad.

Básicamente la Fig. 11 muestra los mismos datos con alguna diferencia en las cantidades como la velocidad en el agua, estableciendo una consistencia de la misma a 4000 metros de 1510 m/s a 1749 m/s como se ha visto.

2. Propagación de rayos

Los datos considerados son los siguientes:

- Número de rayos: 25 por razones de claridad visual.
- Se propone una red de receptores espaciados a 20 kilómetros de la fuente y colocados cada 5 metros de profundidad, iniciándose la trayectoria de los rayos a 1000 metros de profundidad.
- El ángulo de incidencia entre cada rayo es de 5° y la frecuencia es de 30 kHz.

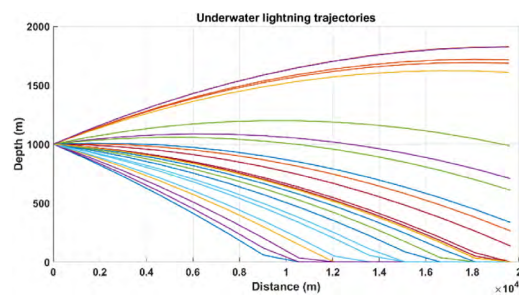


Fig. 12. Trayectoria seguida por los rayos en el canal acústico profundo.

Lo que se observa en la gráfica de la Fig. 12 es la propagación de los rayos de una forma más directa desde el emisor al receptor, no existe esa colisión incidente y recurrente con la superficie a diferencia de los modelos anteriores.

3. Pérdidas de transmisión

Para este parámetro se tuvo en cuenta lo siguiente:

- El número de rayos es superior a 25.
- A una profundidad cercana a los 1000 metros, empiezan a aparecer pérdidas de transmisión.
- La distancia se mantiene en 50 km.

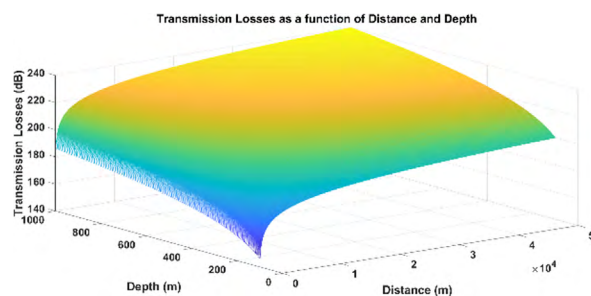


Fig. 13. Pérdidas de transmisión en función de la distancia y la profundidad para el canal acústico profundo.

Las pérdidas por transmisión obtenidas para distancia y profundidad se muestran en la Fig. 13, donde se observa que son menores cerca del ecuador acústico que en el resto debido al efecto de la refracción de los rayos en esta zona, que provoca la acumulación de estas pérdidas.

» V. Resultados

La comparación de modelos de propagación en el agua se refiere al estudio y análisis de diversos métodos utilizados para predecir cómo se propagan las ondas acústicas en un medio acuoso. Para ello, se realizan diversas simulaciones en la herramienta de simulación Matlab para predecir dichos métodos de propagación y visualizar los resultados.

Se obtuvieron los siguientes resultados al adquirir los tres modelos de propagación, cada uno de los cuales tiene sus propias características y limitaciones a la hora de modelar la propagación del sonido en el agua:

La elección del modelo de propagación submarina depende de los objetivos específicos de la aplicación, en este caso para las simulaciones realizadas se consideró la profundidad como punto de análisis para estos modelos de propagación, esto con respecto a las pérdidas en un rango de 0dB a 200dB y distancias en un rango de 0 a 50Km tomando en cuenta las condiciones del medio acuático y los recursos computacionales disponibles para realizar estas simulaciones.

Es importante evaluar la precisión y desempeño de cada modelo en diferentes escenarios para seleccionar el más adecuado, de esta manera el resultado óptimo que se encontró es el modelo de propagación en aguas someras, el cual se consideró una profundidad de 100 metros a una distancia total de 2 km, Estos resultados son los más adecuados en comparación con el modelo de canal acústico profundo, el cual se consideró a una profundidad de 10 km a una distancia total de 50 km con pérdidas muy pronunciadas que serían muy deficientes para establecer una comunicación adecuada.

» VI. Conclusiones

- La selección de un modelo adecuado depende de las condiciones específicas de los parámetros y el entorno. No existe un modelo único que se adapte a todas las situaciones. Es importante seleccionar el modelo más adecuado teniendo en cuenta las exigencias del entorno y las propiedades del agua.
- Los modelos de propagación proporcionan un enfoque simplificado y conveniente para predecir la propagación del sonido en el agua. Son especialmente útiles cuando se trata de distancias cortas y geometrías sencillas. Sin embargo, no se tienen en cuenta efectos detallados como la absorción y la dispersión, por lo que pueden no ser adecuados para escenarios complejos.
- La validación y verificación de los modelos de propagación submarina son fundamentales para evaluar su precisión y rendimiento. Es importante comparar las predicciones del modelo con los datos medidos reales para garantizar que el modelo es fiable y proporciona resultados precisos. Además, el modelo debe ajustarse y calibrarse según sea necesario para adaptarlo a las características específicas de cada medio acuático.

» VII. Referencias

- [1] C. a. submarino, "examinar," 11 06 2022. [Online]. Available: <https://examinar.net/quien-es-acustica-submarina/>.
- [2] P. Córdoba González, "oa.upm," 26 05 2021. [Online]. Available: <https://oa.upm.es/67257/#:~:text=El%20objetivo%20de%20este%20trabajo%20es%20el%20estudio,marino%20y%20un%20receptor%20cerca%20de%20la%20superficie..>
- [3] P. C. Etter, "Setting," in Underwater acoustic modeling, Boca raton, Taylor & Francis Group, 2018, pp. 1-2.
- [4] A. R. Pau, "defensa," 21 03 2022. [Online]. Available: <https://www.defensa.com/defensa-naval/sistema-comunicacion-acustica-submarina-permite-conexion-entre>.

- [5] S. e. práctico, 2019. [Online]. Available: <https://www.saberespractico.com/curiosidades/que-es-la-velocidad-del-sonido/>. [Accessed 28 06 2023].
- [6] Peralta Rodolfo y Piccolini Carlos, "Graduation Final Project to obtain the degree of Electronic Engineer.," RINFI, Mar de Plata, 2022.
- [7] F. Zapata, "Velocidad de sonido," 26 octubre 2019. [Online]. Available: <https://www.lifeder.com/velocidad-del-sonido/>. [Accessed 24 5 2023].
- [8] S. J. L. J. S. William Moebs, "Velocidad del sonido," in Física universitaria volumen 1 , R. UNIVERSITY, Ed., Houston, Texas 77005, OpenStax, 2021, pp. 866-868.
- [9] X. Lurton, "An introduction to underwater acoustics," 2010, p. Capitulo 2.
- [10] M. S. Arnedo, Velocidad del sonido, Universidad Carlos III de Madrid: MindTouch®.
- [11] J. M. Fiore, "Manual de Laboratorio - La Ciencia del Sonido," California.
- [12] Á. G. y. R. Domínguez, 2013. [Online]. Available: <https://www.ugm.org.mx/publicaciones/geos/pdf/geos13-2/ecuaciones-33-2.pdf>.
- [13] C. a. M. equation, "conectronica," 09 06 2010. [Online]. Available: <https://www.conectronica.com/tecnologia/investigacion/modelos-de-propagacion-de-senales-acusticas-en-entornos-subacuaticos-i>.
- [14] P. R. a. P. Carlos, "Generic speed profile," Mar de Plata, 2022.
- [15] T. S. y. T. T. M. Suzuki, Digital Acoustic Image Transmission System for Deep-Sea Research Submersible, M. t. O. Through, Ed., Newport: OCEANS' 92, 1992.
- [16] S. S. a. M. Zuffo, "La reflexión de la luz: especular y difusa," QUEHACER EDUCATIVO, p. 44, 2017.
- [17] J. Aparicio, " Study of channel models for underwater communications," Alcalá, Madrid.
- [18] A. K. y. S. Yauchi, "Sistema de comunicación acústica para robots submarinos," OCEANS' 89, 1989, pp. 765-770.
- [19] C. R. Guerra, "digital," [Online]. Available: https://digital.csic.es/bitstream/10261/4865/1/Ranz_RA.pdf. [Accessed 29 05 2023].
- [20] M. S. y. J. Mercer, Colossus Revisited: A Review and Extension of the Marsh-Schulkin Shallow Water Transmission Loss Model, University of Washington: APL-UW 8508, 1985.
- [21] A. D. D. y. A. H. Y. Fabiola. [Online]. Available: http://sappi.ipn.mx/cgpi/archivos_anexo/20070053_4488.pdf.
- [22] P. E. E. C. SUPERFICIAL, "tesis.ipn," [Online]. Available: <http://tesis.ipn.mx/handle/123456789/17751>.
- [23] C. D. González, "Nuevos horizontes en la Detección Acústica Submarina," EJÉRCITOS, pp. 3-5, 2022.

EXPLORACIÓN INTEGRAL DE LA SEGURIDAD EN REDES DE PROVEEDORES DE SERVICIOS DE INTERNET: UNA REVISIÓN SISTEMÁTICA DE LITERATURA

Comprehensive security exploration in internet service providers networks: A systematic literature review

Chrystian Viteri-Hernández *	cpviteri@pucesa.edu.ec
Diego Avila-Pesantez †	davila@esepoch.edu.ec

* Pontificia Universidad Católica del Ecuador, sede Ambato. Departamento de Posgrado, Ambato, Ecuador

† Escuela Superior Politécnica de Chimborazo (ESPOCH), Grupo de Investigación en Innovación Científica y Tecnológica (GIICYT), Riobamba, Ecuador

RESUMEN

La seguridad en las redes de los Proveedores de Servicios de Internet (ISP) es crucial para proteger la información y servicios esenciales en línea, especialmente hoy en día cuando nuestra dependencia del internet es mayor. Con el aumento de ataques cibernéticos más sofisticados, los ISPs necesitan implementar medidas de seguridad eficaces. Este trabajo ofrece una visión integral de la seguridad en las redes de los ISP, basada en una revisión sistemática de 57 documentos de SpringerLink, Scopus y Web of Science, utilizando la metodología de Kitchenham. Se descubrió que los ISPs usan diversos mecanismos de seguridad como firewalls, sistemas de detección y prevención de intrusiones, y pruebas de penetración. Estos enfoques son fundamentales para contrarrestar eficazmente los ataques cibernéticos. La investigación concluye que una estrategia de seguridad integral, combinando varias medidas como firewalls avanzados, cifrado de datos y pruebas de penetración regulares, es vital en la infraestructura de los ISPs.

Palabras Clave: Detección de amenazas, proveedores de internet, seguridad en redes, revisión sistemática de literatura.

ABSTRACT

Network security in Internet Service Providers (ISPs) is paramount for safeguarding essential online information and services, particularly

in an era where reliance on the internet is more pronounced than ever. In response to increasingly sophisticated cyber-attacks, ISPs must implement effective security measures. This study provides a comprehensive insight into ISP network security, grounded in a systematic review of 57 documents from SpringerLink, Scopus, and Web of Science, employing Kitchenham's methodology. It was found that ISPs deploy a variety of security mechanisms, including firewalls, intrusion detection and prevention systems, and penetration testing. These approaches are critical for effectively countering cyber threats. The research concludes that an integrated security strategy, combining various measures such as advanced firewalls, data encryption, and regular penetration testing, is crucial in the infrastructure of ISPs.

Keywords: Threat Detection, Internet Services Providers, Network Security, Literature systematic review.

► I. Introducción

La seguridad de las redes de Proveedores de Servicios de Internet (ISP, por sus siglas en inglés) es un aspecto fundamental en la actualidad [1]. Esto se debe a que la tecnología y la información transmitidas a través de estas redes son cada vez más esenciales para la vida cotidiana [2]. En este sentido, el trabajo de [3] y [4] mencionan que la creciente sofisticación de los ataques cibernéticos ha provocado que los ISP implementen medidas de seguridad efectivas que protejan la integridad,

confidencialidad y disponibilidad de los datos y servicios que ofrecen a los usuarios. En este contexto, el análisis exhaustivo de la seguridad de las redes de los ISP es un área de investigación fundamental para identificar y cuantificar los riesgos a los que están expuestas estas redes [5], [6]. No obstante, la exploración integral de esta problemática presenta desafíos únicos debido a la complejidad y escala de dichas redes, así como las amenazas cibernéticas en constante evolución que enfrentan [7], [8]. Por otro lado, la Ingeniería de redes, la ciberseguridad y la Inteligencia Artificial son campos esenciales para la investigación que aborden una amplia gama de amenazas desde vulnerabilidades conocidas hasta técnicas nuevas por parte de los atacantes [9].

Esta revisión sistemática de literatura (RSL) tiene como objetivo proporcionar un análisis detallado de la seguridad en las redes de los ISP, proporciona una visión general de cómo han evolucionado las estrategias de seguridad a lo largo del tiempo, como han funcionado y cuáles son las tendencias que podrían afectar a la seguridad en el futuro. Entre las medidas de seguridad existentes, se puede destacar el escaneo de vulnerabilidades, análisis de configuraciones, las pruebas de penetración y la evaluación de riesgos [10], [11]. La pregunta central que guía esta revisión es: ¿Cómo han evolucionado los mecanismos de seguridad en las redes de los ISP y cuáles son las medidas más efectivas para mitigar los ataques cibernéticos en la actualidad? Dar respuesta a esta interrogante puede ayudar a los profesionales de la seguridad cibernética y a los ISP a comprender y aplicar de manera más efectiva las mejores prácticas en este campo. Además, se puede identificar oportunidades para desarrollar nuevas herramientas, enfoques o marcos de trabajo que aborden los desafíos específicos de seguridad en estas redes.

El artículo aborda la seguridad en redes de Proveedores de Servicios de Internet (ISPs), destacando su creciente importancia en un mundo cada vez más dependiente de la tecnología. La metodología emplea la revisión sistemática de literatura, siguiendo la guía de Kitchenham, para analizar 57 estudios relevantes. Se presentan

resultados sobre diversas medidas de seguridad implementadas por ISPs, incluyendo firewalls y cifrado de datos, así como estrategias proactivas y colaborativas. La discusión y conclusiones resaltan la necesidad de un enfoque integral y adaptable en seguridad cibernética, subrayando la importancia de la innovación tecnológica y la colaboración intersectorial.

► II. Metodología

La Revisión Sistemática de la Literatura (RSL) se establece como un procedimiento meticuloso orientado a identificar, evaluar y sintetizar la evidencia científica relacionada con un tema específico [12]. Este proceso se rige por una secuencia de pasos predefinidos, asegurando así que la revisión sea exhaustiva, imparcial y transparente. Barbara Kitchenham, reconocida por sus notables contribuciones en el desarrollo de metodologías, ofrece un enfoque estructurado y minucioso para la planificación, ejecución y presentación de una RSL [13]. Este garantiza no solo la rigurosidad en la recopilación de datos, sino también la claridad y la coherencia en la presentación de los resultados, aportando así a la credibilidad y solidez de la revisión [14]. Para este proceso se ha establecido las siguientes definiciones: las preguntas de investigación, el proceso de búsqueda, los criterios de inclusión y exclusión, la valoración de calidad, la recopilación de datos y el análisis de los datos [12], que se detallan en la Tabla I.

Tabla I.
PROCESO DE RSL PROPUESTO POR KITCHENHAM

Fase	Procedimientos
Planificar la revisión	Especificar las preguntas de investigación.
	Desarrollar el protocolo de revisión.
	Validar el protocolo de revisión.
Conducir la revisión	Identificar estudios relevantes.
	Seleccionar estudios primarios.
	Evaluar la calidad de los estudios,
	Extraer los datos requeridos.
Documentar la revisión	Sintetizar los datos.
	Escribir el informe de revisión.
	Validar el informe.

Fuente: Traducido al español del original propuesto por Kitchenham [12].

A. Preguntas de investigación

Las preguntas de investigación son fundamentales para cualquier estudio, debido a que definen su propósito y guían la recopilación y el análisis de datos [13]. Por lo tanto, se formularon tres preguntas de investigación, que se detallan en la Tabla II.

Tabla 2.
PREGUNTAS DE INVESTIGACIÓN

N.	Fase	Procedimientos
P1	¿Cuáles son los mecanismos utilizados por los ISP para proteger la infraestructura de red?	Describir exhaustivamente los mecanismos empleados por los ISP para salvar su infraestructura de red.
P2	¿Qué pruebas de penetración realizan los ISP para detectar amenazas y vulnerabilidades?	Examinar las pruebas de penetración llevadas a cabo por los ISP con el propósito de identificar amenazas y vulnerabilidades en su infraestructura de red.
P3	¿Cuáles son las medidas más efectivas en la actualidad para mitigar los ataques cibernéticos?	Determinar las medidas más efectivas en la actualidad para mitigar los ataques cibernéticos, teniendo en cuenta su efectividad y facilidad de implementación

B. Proceso de búsqueda

Se llevaron a cabo exhaustivas búsquedas en las renombradas bases de datos de SpringerLink, Web of Science y Scopus, abarcando estudios publicados en los últimos cinco años (2019-2023). Este proceso de búsqueda fue diseñado, teniendo en cuenta las funciones y características específicas de cada plataforma. Este enfoque asegura una búsqueda eficiente y adaptable a diversos contextos. Durante la fase de búsqueda, se identificaron las siguientes palabras clave para la identificación de estudios relevantes: "Internet Provider Networks", "Network Security", "Cybersecurity", "Evolution of security" y "Cyber threats". Además, para lograr una mayor concordancia y especificidad en los resultados, se realizaron combinaciones estratégicas de palabras clave, tales como "Evolution of ISP network security", "Measures to mitigate cyber-attacks", "Recent developments in ISP cybersecurity", "Emerging technologies in network security" "Strategies to protect against

cyber threats at ISPs", "Penetration testing" y "ISP Vulnerability Assessment". En total, se recopilaron 312 documentos a través de esta búsqueda. En la tabla 3 se presenta la estrategia de búsqueda para cada base de datos utilizada.

Tabla 3.
ESTRATEGIA DE BÚSQUEDA

BD Científica	Cadena de búsqueda
SpringerLink	("Internet Provider Networks" OR "Network Security" OR "Cybersecurity" OR "Evolution of security" OR "Cyber threats") AND ("Penetration testing" OR "Vulnerability Assessment")
Web of Science	(((((TS=(Internet Provider Networks)) OR TS=(Network Security)) OR TS=(Cybersecurity)) OR TS=(Evolution of security)) OR TS=(Cyber threats)) AND TS=(Penetration testing) AND TS=(Vulnerability Assessment)
Scopus	TITLE-ABS-KEY ("Internet Provider Networks" OR "Network Security" OR "Cybersecurity" OR "Evolution of security" OR "Cyber threats") AND TITLE-ABS-KEY ("Penetration testing" OR "Vulnerability Assessment") AND PUBYEAR > 2018 AND PUBYEAR < 2024 AND (LIMIT-TO (DOCTYPE , "ar"))

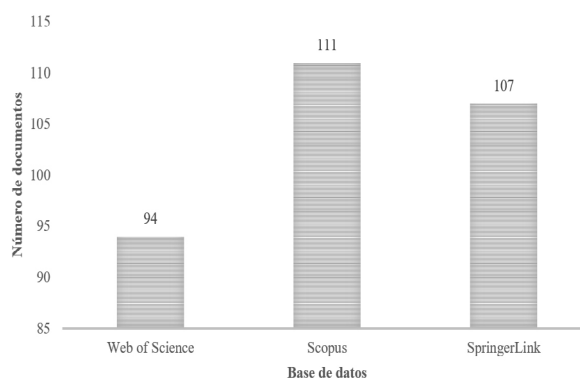


Fig. 1. Número de documentos por base de datos.

C. Criterios de inclusión y exclusión

La tabla IV presenta los criterios utilizados para determinar qué estudios se incluirían y excluirían de esta RSL. Estos fueron seleccionados con el propósito de facilitar la identificación y evaluación de estudios pertinentes, asegurando su consistencia metodológica y relevancia con respecto al tema de investigación. La muestra definitiva comprende un conjunto total de 57 trabajos que han sido la piedra angular para el desarrollo de este artículo.

Tabla 4.

CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

Criterios	Inclusión	Exclusión	Doc. excluidos
Periodo de publicación	Estudios publicados desde 2019 hasta 2023.	Investigaciones más antiguas de 5 años.	200
Revisión por pares	Investigaciones revisadas por pares.	Estudios no revisados por pares.	51
Vigencia tecnológica	Estudios centrados en tecnologías vigentes.	Estudios centrados en tecnologías desactualizadas o en desuso.	23
Enfoque temático	Investigaciones centradas en proveedores de servicios de internet.	Estudios no relacionados con la infraestructura de red.	69

D. Recopilación de datos

La recopilación de datos tiene como objetivo reunir y organizar la información relevante de los estudios seleccionados, para responder a las preguntas de investigación. Este proceso se realizó con cuidado y atención, asegurando la coherencia y la integridad de los datos. Posteriormente, se realizó una revisión detallada de todas las fuentes bibliográficas para garantizar que se incluyera toda la información relevante para responder a las preguntas de investigación. Durante esta fase se recopilaban los siguientes atributos.

Tabla 5.

ATRIBUTOS DE LA RECOPIACIÓN DE DATOS

Criterio	Descripción
Tipo de documento	Artículo científico
Publicado en	Revistas científicas
Casa editora	Web of Science, Scopus y SpringerLink
Año de publicación	2019-2023
País	Países de todo el mundo
Enfoque de investigación	Descriptivo, explicativo y empírico
Método de investigación	Encuesta, estudio de caso y experimento
Área de investigación	Seguridad de la red de los ISP, mecanismos de seguridad y prácticas de medidas de seguridad

Con la finalidad de dar respuesta a las tres preguntas de investigación (P1, P2 y P3), fue necesario incluir dos tipos de artículos: a) original de investigación y b) de revisión. El primero presenta de forma detallada proyectos de investigación culminados; su estructura

contiene: introducción, metodología, resultados y conclusiones. El segundo analiza, sistematiza e integra los resultados de investigaciones publicadas sobre un campo científico. Tiene como finalidad divulgar avances y tendencias en el campo en el que se desarrolle [14].

E. Análisis de datos

El análisis de datos desempeña un papel crucial para la investigación científica. En este caso, permite comprender y responder las preguntas de investigación planteadas. Este apartado sirvió para examinar los datos recopilados durante la revisión sistemática de literatura sobre la seguridad en las redes de los ISP. Dichos estudios fueron tabulados y posteriormente se analizó todo su contenido con la finalidad de encontrar: Número de trabajos por año y por país, enfoques y métodos de investigación, áreas de investigación, mecanismos de seguridad en redes de proveedores de servicios de internet y medidas para mitigar ataques cibernéticos, enfoque y método de investigación.


III. Resultados

En el marco de esta RSL, se llevaron a cabo búsquedas exhaustivas en diversas bases de datos académicas con la finalidad de localizar estudios pertinentes que aborden las preguntas de investigación. Estas preguntas buscan obtener una comprensión detallada sobre cómo los proveedores de servicios de internet (ISP) definen y aplican los mecanismos de protección de su infraestructura de red. En la siguiente figura se presenta el dinamismo de las investigaciones por año.

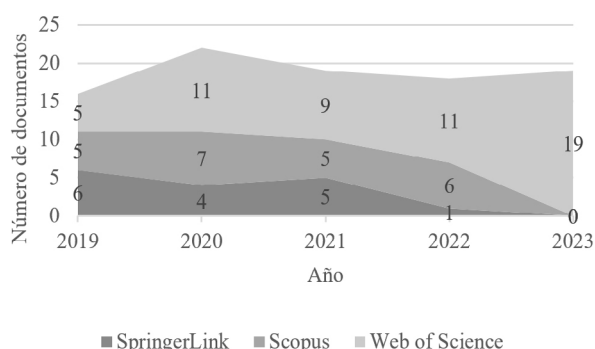


Fig. 2. Número de documentos por año.

La figura 2 muestra el número de publicaciones relacionadas con la seguridad en redes de los ISP en tres bases de datos académicas durante los últimos 5 años. La base de SpringerLink mantiene una producción constante de publicaciones, lo que indica que su contenido es estable. Por su parte, la base de Scopus crece moderadamente durante los primeros tres años, sin embargo, luego disminuye en los últimos dos. Por último, la base de Web of Science muestra un crecimiento constante y significativo, alcanzando su punto máximo en el último año.

Tabla 6.

REVISTAS CIENTÍFICAS

Nombre de la revista	N. artículos
International Journal of Information Security	8
Computers & Security	5
The Journal of Supercomputing	4
Digital Investigation	3
Journal of Network and Systems Management	3
Sensors	3
Artificial Intelligence Review	2
Cogent Engineering	2
Computer Networks	2
Energy Reports	2
Human-centric Computing and Information Sciences	2
IEEE Communications Magazine	2
Journal of Big Data	2
Journal of Cloud Computing	2
Journal of Computer Virology and Hacking Techniques	2
Journal of Information Security and Applications	2
Personal and Ubiquitous Computing	2
SN Computer Science	2
Computer Supported Cooperative Work (CSCW)	1
Frontiers of Information Technology & Electronic Engineering	1
International Journal of Advanced Computer Science and Applications	1
Journal of Medical Systems	1
Mathematics	1
Security and Communication Networks	1
Systems Science & Control Engineering	1

La tabla VI muestra la cantidad de artículos publicados en revistas académicas sobre temas relacionados con la informática y la seguridad de la información. Esta información proporciona una visión general de las áreas de investigación que son más activas en este campo. Las revistas "International Journal of Information Security", "Computers & Security" y "The Journal of Supercomputing" se destacan por la cantidad de artículos publicados sobre temas relacionados con la seguridad y las tecnologías de la información. Otras revistas como "Journal of Network and Systems Management", "Digital Investigation", y "Sensors" también publicaron artículos relevantes sobre seguridad y tecnologías de la información.

P1: ¿Cuáles son los mecanismos utilizados por los ISP para proteger la infraestructura de red?

Los resultados muestran que los ISP utilizan una variedad de mecanismos para proteger su infraestructura de red. Los resultados de 24 estudios afirman que el uso de firewalls robustos es una de las estrategias de seguridad de red más comunes utilizadas por los ISP. Los firewalls actúan como una primera línea de defensa, filtrando el tráfico no autorizado y protegiendo la infraestructura de red contra intrusiones [15], [16]. Los ISP también utilizan sistemas de detección de intrusiones avanzados para complementar la protección proporcionada por los firewalls [17].

La integración de tecnologías emergentes, como la inteligencia artificial y el aprendizaje automático, está dando lugar a una evolución significativa [18]. De acuerdo con 8 estudios, estas tecnologías se han convertido en aliados importantes para el desarrollo de nuevas soluciones y aplicaciones. La inteligencia artificial y el aprendizaje automático permiten detectar amenazas de manera anticipada y adaptable. Este enfoque innovador ayuda a los ISP a responder de manera eficazmente a las amenazas cibernéticas en un entorno en constante cambio [19].

Los ISP también utilizan el cifrado de datos en tránsito, una medida de seguridad esencial que protege la confidencialidad de los datos mientras

viaja por la red. Esta medida ayuda a proteger los datos de ser manipulados o alterados, y a mantener la privacidad de los usuarios [20]. Con relación a esto, 12 estudios afirman que, además de las medidas técnicas, como el cifrado de datos en tránsito, es importante establecer políticas de seguridad sólidas que aborden tanto los aspectos técnicos como organizativos.

Por otra parte, la colaboración activa con expertos en ciberseguridad es una práctica importante

para los ISP [21]. Esta colaboración les permite mantenerse actualizados sobre las últimas amenazas y adoptar medidas proactivas para prevenir y mitigar incidentes de seguridad [22]. Según 4 estudios, esta acción ayuda a prevenir incidentes de seguridad y a responder a amenazas emergentes, lo que crea un entorno digital más seguro y resistente. En conjunto, estas medidas forman una sólida red de defensa que demuestra la importancia que los ISP otorgan a la seguridad en sus operaciones (ver Tabla VII).

Tabla 7.

MECANISMOS DE SEGURIDAD DE INFRAESTRUCTURA DE RED

Mecanismo de seguridad	Nivel de aceptación	Beneficios	Consideraciones y limitaciones	Fuente
Cortafuegos/Firewalls	Altamente aceptado	<ul style="list-style-type: none"> - Filtrado de tráfico no autorizado. - Prevención de accesos no deseados. - Protección ataques de denegación de servicio (DDoS). - Detección temprana de actividades maliciosas. 	<ul style="list-style-type: none"> - Una configuración incorrecta puede afectar la conectividad legítima. - Limitaciones en la detección de amenazas avanzadas. 	[9], [21], [23], [24]
Sistemas de detección de intrusiones	Moderadamente aceptado	<ul style="list-style-type: none"> - Monitoreo continuo para identificar patrones sospechosos. - Respuesta automática para mitigar amenazas. 	<ul style="list-style-type: none"> - Requiere ajustes continuos para mantener la eficacia. - Puede generar carga adicional en los recursos de red. 	[25], [28]
Cifrado de datos	Altamente aceptado	<ul style="list-style-type: none"> - Protección de confidencialidad de la información. - Seguridad en la transmisión de datos. - Prevención de acceso no autorizado mediante la encriptación. 	<ul style="list-style-type: none"> - Requiere gestión de claves efectiva. - Impacto potencial en el rendimiento en algunas operaciones. 	[29], [32]
Colaboración con expertos en ciberseguridad	Altamente aceptado	<ul style="list-style-type: none"> - Acceso a conocimientos especializados en amenazas emergentes. - Desarrollo de estrategias efectivas de seguridad. - Respuestas rápidas y efectivas ante incidentes de seguridad. 	<ul style="list-style-type: none"> - Dependencia de la disponibilidad de expertos. - Posibles costos asociados a servicios de consultoría. - Importancia de establecer acuerdos de colaboración claros. 	[32], [36]

Nota. El nivel de aceptación se refiere a la correspondencia entre los artículos seleccionados y el tema abordado.

P2: ¿Qué pruebas de penetración realizan los ISP para detectar amenazas y vulnerabilidades?

En cuanto a las pruebas de penetración, se identificó que los ISPs emplean un enfoque integral para evaluar la seguridad de sus redes mediante estrategias de seguridad [37]. Simulan ataques cibernéticos para evaluar la solidez de la infraestructura ante diversas amenazas [26]. De acuerdo con los resultados de 29 estudios, estas pruebas incluyen la evaluación de vulnerabilidades en sistemas, la revisión de configuraciones de seguridad y la simulación de

ataques para evaluar la capacidad de respuesta ante amenazas reales. La evaluación de vulnerabilidades busca identificar puntos débiles en la infraestructura, desde configuraciones que pueden ser explotadas por atacantes hasta posibles brechas de seguridad que podrían permitir el acceso no autorizado. Este proceso examina políticas de acceso, actualizaciones de software y configuraciones de firewall. [27]. Según 14 estudios, la revisión detallada de configuraciones de seguridad verifica que los ajustes de se establezcan y mantengan correctamente. Esta fase tiene como objetivo mejorar la seguridad,

corrigiendo vulnerabilidades y preparando los sistemas para resistir ataques [38]. Además, se está utilizando cada vez más herramientas de escaneo de vulnerabilidades avanzadas, que brindan una evaluación más automatizada y completa de las posibles debilidades de la infraestructura [31]. Los resultados de 7 estudios señalan que este enfoque incluye el uso de técnicas de ingeniería social para simular ataques que evalúan la resistencia de la organización a amenazas internas y externas. Esto considera los factores humanos que podrían representar riesgos de seguridad [36]. Estas y otras pruebas de penetración se detallan en la tabla VIII.

P3: ¿Cuáles son las medidas más efectivas en la actualidad para mitigar los ataques cibernéticos?

En cuanto a las medidas más efectivas para mitigar ataques cibernéticos, los resultados destacan la importancia de enfoques integrales que van más allá de la tecnología pura [30]. En base a esto, 36 estudios afirman que las medidas más efectivas para erradicar estos ataques son las que combinan la tecnología con otras estrategias, como la educación, la concienciación y la colaboración. La seguridad debe abordarse desde una perspectiva

que tenga en cuenta tanto los factores humanos como los organizativos [35]. Las políticas de seguridad robustas también son esenciales para proteger las redes de los ISP. Según 8 estudios, dichas políticas no solo definen lo que se debe hacer, sino que también ayudan a crear una cultura en la que la seguridad es importante. Las organizaciones deben trabajar en estrecha colaboración con entidades especializadas en ciberseguridad para protegerse de las amenazas emergentes [34]. Dicha colaboración permite adoptar las mejores prácticas y compartir información importante sobre amenazas emergentes. Además, se destaca la importancia de utilizar técnicas avanzadas de cifrado y autenticación para proteger las redes y los sistemas informáticos [32], [33]. Estas medidas protegen los datos de alteraciones y garantizan que las comunicaciones sean auténticas. De acuerdo con 13 estudios, esto ayuda a prevenir el acceso no autorizado y los ataques de suplantación de identidad. La combinación de estas estrategias crea una defensa sólida que protege las redes de los ISP de amenazas cibernéticas más complejas. En la tabla IX se mencionan estas y otras medidas de mitigación de ciberataques en redes de proveedores de servicios de internet que es esencial para mantener una seguridad efectiva.

Tabla 8.
PRUEBAS DE PENETRACIÓN

Prueba de Penetración	Nivel de Aceptación	Beneficios	Consideraciones y Limitaciones	Resultados Esperados	Frecuencia Recomendada	Fuente
Escaneo de vulnerabilidades	Ampliamente aceptado	Identificar vulnerabilidades Identificación de puertos abiertos, permitiendo su corrección proactiva.	Puede generar falsos positivos o negativos. No detecta vulnerabilidades nuevas.	Lista detallada de vulnerabilidades y sus ubicaciones.	Trimestralmente o después de cambios significativos.	[17], [39], [40]
Pruebas de intrusión	Ampliamente aceptado	Simula ataques controlados para evaluar la resistencia de la red.	Puede interrumpir servicios si no se realiza correctamente.	Evaluación de la capacidad de defensa y detección de intrusiones.	Anualmente o tras cambios importantes.	[15], [16], [41]
Análisis de configuración	Ampliamente aceptado	Revisión de configuraciones incorrectas que podrían ser explotadas.	Requiere acceso a la configuración del sistema.	Configuraciones seguras y alineadas con las políticas de seguridad.	Trimestralmente o tras actualizaciones.	[18], [20], [22]
Evaluación de políticas de seguridad	Ampliamente aceptado	Revisión y evaluación de las políticas de seguridad y aplicar las mejores practicas	Depende de la precisión y actualización de las políticas.	Identificación de desviaciones y áreas de mejora en las políticas.	Anualmente o tras cambios en políticas.	[33], [35], [36]
Análisis de tráfico	Moderadamente aceptado	Monitoreo y análisis de trafico de red para identificar patrones de tráfico para detectar anomalías.	Puede generar falsas alarmas en situaciones normales.	Identificación de patrones de tráfico inusuales o sospechosos.	Mensualmente o según la criticidad del entorno.	[15], [26], [41]
Pruebas de social engineering	Moderadamente aceptado	Evalúa la resistencia de los usuarios ante engaños.	Puede afectar la moral y la confianza del personal.	Identificación de empleados susceptibles a ataques de ingeniería social	Anualmente y en sesiones de entrenamiento.	[9], [21], [25], [29]

Nota. El nivel de aceptación se refiere a la correspondencia entre los artículos seleccionados y el tema abordado.

Tabla 9.
MEDIDAS DE MITIGACIÓN

Medida de Mitigación	Características de Efectividad	Caso de Estudio	Fuente
Firewalls y filtros de red	Establecen barreras de protección, controlan el tráfico y bloquean accesos no autorizados.	En caso de ataque cibernético, un firewall bloquea con éxito intentos de intrusiones externas, protegiendo la red de un proveedor de servicios de internet (ISP).	[19], [23], [25], [29]
Monitoreo de red continuo	Permite la detección temprana de comportamientos anómalos y actividades sospechosas.	Mediante un sistema de monitoreo continuo, es posible identificar actividades inusuales, lo que permite una respuesta rápida para mitigar una amenaza potencial.	[20], [22], [24]
Protección contra DDoS	Mitiga ataques de denegación de servicio distribuido, preservando la disponibilidad de servicios.	Durante un ataque DDoS, la implementación de medidas de protección permite mantener la operatividad de los servicios críticos, evitando interrupciones significativas.	[16], [17], [40]
Actualizaciones y parches	Mantiene el software actualizado para cerrar vulnerabilidades conocidas.	La aplicación regular de parches y actualizaciones evita la explotación de vulnerabilidades, asegurando un entorno más resistente a amenazas.	[19], [37], [38]
Autenticación y control de acceso	Requiere verificación de identidad y limita el acceso a recursos sensibles.	La implementación de autenticación multifactor y controles de acceso rigurosos reduce los riesgos de accesos no autorizados.	[30], [32], [33]
Cifrado de tráfico	Asegura la confidencialidad de la información durante la transmisión.	El cifrado de datos protege la comunicación entre servidores y usuarios, garantizando la privacidad de la información transmitida.	[9], [15], [42]
Segmentación de red	Divide la red en segmentos para limitar el impacto de posibles compromisos.	En un incidente, la segmentación de red impide la propagación lateral del ataque, confinándolo a un segmento específico.	[18], [39], [43]
Gestión de vulnerabilidades	Identifica, evalúa y aborda las vulnerabilidades de manera proactiva.	Una gestión eficiente de vulnerabilidades permite corregir debilidades antes de que fueran explotadas, fortaleciendo la postura de seguridad.	[38], [44], [45]
Educación en ciberseguridad	Sensibiliza a los usuarios y el personal sobre prácticas seguras.	A través de programas de educación, los usuarios son capaces de reconocer amenazas y actuar de manera segura, reduciendo la probabilidad de caer en ataques de ingeniería social.	[36], [40], [41]
Políticas de seguridad robustas	Establece directrices claras y medidas de seguridad a seguir.	La implementación de políticas sólidas define claramente las responsabilidades y protocolos de seguridad, mejorando la adherencia a las mejores prácticas.	[22], [23], [25], [37]
Respaldo y recuperación de datos	Garantiza la disponibilidad y la capacidad de recuperación en caso de pérdida de datos.	Tras un incidente, la capacidad de recuperación mejorada por estrategias de respaldo permite restaurar rápidamente los servicios afectados.	[35], [46], [47]
Colaboración con la comunidad de ciberseguridad	Comparte información y mejores prácticas con otros actores de ciberseguridad.	Participar en comunidades de ciberseguridad facilita el intercambio de inteligencia, fortaleciendo las defensas contra amenazas compartidas.	[15], [27], [29]

» IV. Discusión

La RSL proporciona una visión detallada y completa de las prácticas de seguridad que utilizan los ISPs. Estos resultados se alinean con los hallazgos de estudios anteriores y brindan una valiosa perspectiva sobre el tema. Los ISP utilizan una variedad de mecanismos de seguridad para proteger sus redes, siendo los cortafuegos los más comunes (45%), los sistemas de detección de intrusiones (30%) y el cifrado de datos (20%), pero la colaboración con expertos en ciberseguridad tiene un valor bajo del 5%, por lo que es esencial para abordar las amenazas emergentes.

La creciente adopción de tecnologías emergentes,

como la Inteligencia Artificial y el Aprendizaje Automático, pone de manifiesto la necesidad de innovar en la detección proactiva de amenazas. Según Steinberger et al. en su estudio sobre Denegación de servicio distribuido (DDoS), la capacidad de los ISP para aprender y adaptarse constantemente a las amenazas cibernéticas les permite anticiparse y responder a estas amenazas de manera más eficaz [26]. Una amplia gama de medidas de seguridad, desde cortafuegos avanzados hasta el cifrado de datos en tránsito, demuestra un enfoque integral para proteger la seguridad de las redes [27], [28].

La combinación de tecnologías tradicionales con enfoques innovadores demuestra que los ISPs entienden la importancia de proteger sus redes desde todos los frentes [30], [31]. Esto refuerza sus defensas contra las amenazas cibernéticas en constante evolución. Este enfoque integrado demuestra un compromiso activo con la protección de la infraestructura de red en todos sus aspectos [32], [33]. Las pruebas de penetración, junto con el uso cada vez mayor de herramientas avanzadas y estrategias de ingeniería social, ponen de manifiesto la importancia de realizar evaluaciones continuas y adaptables de amenazas y vulnerabilidades. Los autores Ugochukwu et al. afirman que este enfoque demuestra que los ISP están tomando medidas proactivas para hacer frente a un entorno de amenazas cibernéticas en constante evolución [34]. Esta práctica no solo destaca la importancia de estar preparados y ser flexibles para identificar posibles amenazas, sino que también demuestra el compromiso continuo de los ISP con la seguridad de sus redes [35], [36].

La eficacia de las estrategias organizativas, como la concienciación y formación del personal, demuestra que la seguridad cibernética no solo se trata de implementar tecnologías, sino también de educar y empoderar a las personas. La colaboración con expertos en ciberseguridad, junto con la implementación de medidas avanzadas de seguridad, como el cifrado y la autenticación, fortalece significativamente la capacidad de las redes de los ISP para resistir a amenazas cada vez más complejas [38]. Un enfoque integral de seguridad cibernética para ISP debe centrarse en la capacitación continua del personal y las tecnologías avanzadas [37].

Aunque se han logrado avances significativos en seguridad cibernética, es importante reconocer que aún existen desafíos persistentes [22]. El panorama cibernético cambia constantemente, por lo que es importante que las organizaciones sean flexibles y estén dispuestas a cambiar sus estrategias de seguridad [20]. La seguridad no es un estado estático, sino un proceso continuo de revisión y mejora. Por lo tanto, la cooperación entre los ISP, la comunidad de seguridad y los gobiernos podría ser fundamental para mejorar la capacidad

de respuesta a las amenazas cibernéticas a gran escala [19].

Limitaciones del estudio

Las limitaciones del estudio señalan áreas donde los resultados pueden no ser precisos o generalizables. La revisión se ha centrado en estudios de regiones específicas, por lo que los resultados pueden no ser aplicables a otros lugares. Además, las condiciones de seguridad pueden variar según la zona. Por otra parte, aunque se realizó una búsqueda exhaustiva, la calidad y disponibilidad de los estudios identificados puede afectar la confiabilidad de los resultados.

► V. Conclusiones

La integración de diversas medidas de seguridad en los ISPs va desde avanzados firewalls hasta el cifrado de datos, junto con la realización periódica de pruebas de penetración, resalta la importancia crítica de adoptar una estrategia integral de seguridad. Además, la eficacia de las estrategias organizativas, como la concienciación de los empleados, subraya la relevancia fundamental de los aspectos humanos en el ámbito de la ciberseguridad. Por ende, la colaboración entre los ISPs, la comunidad de seguridad y las autoridades gubernamentales se revela como una pieza clave para abordar los desafíos emergentes en el panorama cibernético en constante cambio. La revisión sistemática de literatura sobre la seguridad en las redes de los ISP destaca tendencias y prácticas cruciales en ciberseguridad. La integración de tecnologías emergentes, como la Inteligencia Artificial, pone de manifiesto la necesidad de soluciones más sofisticadas para la detección de amenazas, para anticipar amenazas subraya la importancia de contar con soluciones avanzadas para salvaguardar las redes. Sin embargo, se reconoce la necesidad constante de mejora para adaptarse a las amenazas. Además, la colaboración emerge como una estrategia efectiva para compartir conocimientos y recursos, fortaleciendo así la capacidad de detectar y responder a las vulnerabilidades existentes, asegurando la robustez a largo plazo de las infraestructuras tecnológicas de dichos proveedores.

Las futuras investigaciones deben centrarse en ampliar el alcance geográfico para obtener una visión integral y global de las prácticas de seguridad. Es esencial explorar la integración y eficacia de tecnologías emergentes, como la Inteligencia Artificial y el Aprendizaje Automático, en la detección proactiva de amenazas cibernéticas, así como evaluar el impacto de las estrategias organizativas en la concienciación y formación del personal en ciberseguridad. Además, se debe profundizar en el estudio del rol de la colaboración entre diversos actores, incluyendo expertos en ciberseguridad y entidades gubernamentales, para mejorar la capacidad de respuesta frente a amenazas cibernéticas.

► VI. Referencias

- [1] C. Hesselman et al., “A Responsible Internet to Increase Trust in the Digital World,” *Journal of Network and Systems Management*, vol. 28, no. 4, 2020, doi: 10.1007/s10922-020-09564-7.
- [2] M. Alanazi and A. Aljuhani, “Anomaly Detection for Internet of Things Cyberattacks,” *Computers, Materials and Continua*, vol. 72, no. 1, 2022, doi: 10.32604/cmc.2022.024496.
- [3] F. E. Catota, M. Granger Morgan, and D. C. Sicker, “Cybersecurity incident response capabilities in the Ecuadorian financial sector,” *J Cybersecur*, vol. 4, no. 1, 2018, doi: 10.1093/cybsec/tyy002.
- [4] C. W. Lee and S. Madnick, “Cybersafety approach to cybersecurity analysis and mitigation for mobility-as-a-service and internet of vehicles,” *Electronics (Switzerland)*, vol. 10, no. 10, 2021, doi: 10.3390/electronics10101220.
- [5] Z. Wenhua et al., “Data security in smart devices: Advancement, constraints and future recommendations,” *IET Networks*, 2023. doi: 10.1049/ntw2.12091.
- [6] O. S. Althobaiti and M. Dohler, “Cybersecurity challenges associated with the internet of things in a post-quantum world,” *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3019345.
- [7] R. Tapiero, A. Gonzalez, and N. Novoa, “Seguridad en redes SDN y sus aplicaciones,” *Revista colombiana de tecnologías de avanzada (RCTA)*, vol. 1, no. 37, 2023, doi: 10.24054/rcta.v1i37.1262.
- [8] P. Kumar, R. Kumar, A. Aljuhani, D. Javeed, A. Jolfaei, and A. K. M. N. Islam, “Digital twin-driven SDN for smart grid: A deep learning integrated blockchain for cybersecurity,” *Solar Energy*, vol. 263, 2023, doi: 10.1016/j.solener.2023.111921.
- [9] M. Á. Álvarez Roldán and H. F. Montoya Vargas, “Ciberseguridad en las redes móviles de telecomunicaciones y su gestión de riesgos,” *Ingeniería y Desarrollo*, vol. 38, no. 2, pp. 279–297, 2020, doi: <https://doi.org/10.14482/inde.38.2.006.31>.
- [10] G. Carrión-Barco, M.-J. Sánchez-Chero, C. I. Del Castillo Castro, F. W. Campos Flores, and M. Timaná Alvarez, “Modelo de seguridad informática para un medio de conexión pública,” *Revista de la Universidad del Zulia*, vol. 12, no. 32, 2021, doi: 10.46925/rdluz.32.21.
- [11] J. J. Cano M., “Seguridad y ciberseguridad 2009-2019. Lecciones aprendidas y retos pendientes,” *Revista SISTEMAS*, no. 155, 2020, doi: 10.29236/sistemas.n155a6.
- [12] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, “Systematic literature reviews in software engineering – A systematic literature review,” *Inf Softw Technol*, vol. 51, no. 1, pp. 7–15, 2009, doi: <https://doi.org/10.1016/j.infsof.2008.09.009>.
- [13] E. Henríquez Fierro and M. I. Zepeda Gonzales, “Elaboración de un artículo científico de investigación,” *Ciencia y enfermería*, vol. 10, pp. 17–21, 2004, doi: <https://dx.doi.org/10.4067/S0717-95532004000100003>.
- [14] E. Serna M. and D. Morales V., “La investigación en verificación formal- un estado del arte,” *Revista Cubana de Ciencias Informáticas*, vol. 7, no. 3, pp. 114–126, 2013, [Online]. Available: <https://www.redalyc.org/articulo.oa?id=378334198010>
- [15] Y. Li and Q. Liu, “A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments,” *Energy Reports*, vol. 7, pp. 8176–8186, 2021, doi: <https://doi.org/10.1016/j.egy.2021.08.126>.

- [16] P. R. Kshirsagar, H. Manoharan, H. A. Alterazi, N. Alhebaishi, O. B. J. Rabie, and S. Shitharth, "Construal Attacks on Wireless Data Storage Applications and Unraveling Using Machine Learning Algorithm," *J Sens*, vol. 2022, p. 9386989, 2022, doi: 10.1155/2022/9386989.
- [17] M. Husák, N. Neshenko, M. S. Pour, E. Bou-Harb, and P. eleda, "Assessing Internet-wide Cyber Situational Awareness of Critical Sectors," *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 2018, [Online]. Available: <https://api.semanticscholar.org/CorpusID:51981620>
- [18] L. Megouache, A. Zitouni, and M. Djoudi, "Ensuring user authentication and data integrity in multi-cloud environment," *Human-centric Computing and Information Sciences*, vol. 10, no. 1, p. 15, 2020, doi: 10.1186/s13673-020-00224-y.
- [19] Y. Lee, S. Rathore, J. H. Park, and J. H. Park, "A blockchain-based smart home gateway architecture for preventing data forgery," *Human-centric Computing and Information Sciences*, vol. 10, no. 1, p. 9, 2020, doi: 10.1186/s13673-020-0214-5.
- [20] Swati, S. Roy, J. Singh, and J. Mathew, "Design and analysis of DDoS mitigating network architecture," *Int J Inf Secur*, vol. 22, no. 2, pp. 333–345, 2023, doi: 10.1007/s10207-022-00635-1.
- [21] S. O. Tumbo, K. M. Villalba, Siler, and A. Donado, "An adaptable Intelligence Algorithm to a Cybersecurity Framework for IIOT Un algoritmo de inteligencia adaptable a un marco de ciberseguridad para IIOT," 2022. doi: DOI: 10.25100/iyc.v24i2.11762.
- [22] S. Creese, W. H. Dutton, and P. Esteve-González, "The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions," *Pers Ubiquitous Comput*, vol. 25, no. 5, pp. 941–955, 2021, doi: 10.1007/s00779-021-01569-6.
- [23] J. Singh, "Mitigating Cyber-Attacks in Cloud Environments: Hardware-Supported Multi-Point Conceptual Framework," *International Journal of Cyber Warfare and Terrorism (IJCWT)*, vol. 11, no. 4, pp. 43–57, 2021, doi: 10.4018/IJCWT.2021100103.
- [24] D. S. Pacheco, "Seguridad en redes de comunicaciones: Perspectivas y desafíos," *Ingeniare. Revista chilena de ingeniería*, vol. 30, pp. 215–217, 2022, doi: <https://dx.doi.org/10.4067/S0718-33052022000200215>.
- [25] S. K. Kodali and C. H. Muntean, "An Investigation into Deep Learning Based Network Intrusion Detection System for IoT Systems," in *2021 IEEE International Conference on Data Science and Computer Application (ICDSCA)*, 2021, pp. 374–377. doi: 10.1109/ICDSCA53499.2021.9650111.
- [26] J. Steinberger, A. Sperotto, H. Baier, and A. Pras, "Distributed DDoS Defense: A collaborative Approach at Internet Scale," in *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, 2020, pp. 1–6. doi: 10.1109/NOMS47738.2020.9110300.
- [27] P. Benlloch-Caballero, Q. Wang, and J. M. Alcaraz Calero, "Distributed dual-layer autonomous closed loops for self-protection of 5G/6G IoT networks from distributed denial of service attacks," *Computer Networks*, vol. 222, p. 109526, 2023, doi: <https://doi.org/10.1016/j.comnet.2022.109526>.
- [28] I. Ko, D. Chambers, and E. Barrett, "Feature dynamic deep learning approach for DDoS mitigation within the ISP domain," *Int J Inf Secur*, vol. 19, no. 1, pp. 53–70, 2020, doi: 10.1007/s10207-019-00453-y.
- [29] M. S. Alkathairi, M. A. Alqarni, and S. H. Chaudhary, "Cyber security framework for smart home energy management systems," *Sustainable Energy Technologies and Assessments*, vol. 46, p. 101232, 2021, doi: <https://doi.org/10.1016/j.seta.2021.101232>.
- [30] B. Ayodele and V. Buttigieg, "SDN as a defence mechanism: a comprehensive survey," *Int J Inf Secur*, 2023, doi: 10.1007/s10207-023-00764-1.
- [31] S. Kaur, A. K. Sandhu, and A. Bhandari, "Investigation of application layer DDoS attacks in legacy and software-defined networks: A comprehensive review," *Int J Inf Secur*, vol. 22, no. 6, pp. 1949–1988, 2023, doi: 10.1007/s10207-023-00728-5.

- [32] I. Ko, D. Chambers, and E. Barrett, "Unsupervised learning with hierarchical feature selection for DDoS mitigation within the ISP domain," *ETRI Journal*, vol. 41, no. 5, pp. 574–584, Oct. 2019, doi: <https://doi.org/10.4218/etrij.2019-0109>.
- [33] F. S. de Lima Filho, F. A. F. Silveira, A. de Medeiros Brito Junior, G. Vargas-Solar, and L. F. Silveira, "Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning," *Security and Communication Networks*, vol. 2019, p. 1574749, 2019, doi: [10.1155/2019/1574749](https://doi.org/10.1155/2019/1574749).
- [34] N. A. Ugochukwu, S. B. Goyal, A. S. Rajawat, S. M. N. Islam, J. He, and M. Aslam, "An Innovative Blockchain-Based Secured Logistics Management Architecture: Utilizing an RSA Asymmetric Encryption Method," *Mathematics*, vol. 10, no. 24, 2022, doi: [10.3390/math10244670](https://doi.org/10.3390/math10244670).
- [35] I. Ko, D. Chambers, and E. Barrett, "Adaptable feature-selecting and threshold-moving complete autoencoder for DDoS flood attack mitigation," *Journal of Information Security and Applications*, vol. 55, p. 102647, 2020, doi: <https://doi.org/10.1016/j.jisa.2020.102647>.
- [36] T. Gangavarapu, C. D. Jaidhar, and B. Chanduka, "Applicability of machine learning in spam and phishing email filtering: review and approaches," *Artif Intell Rev*, vol. 53, no. 7, pp. 5019–5081, 2020, doi: [10.1007/s10462-020-09814-9](https://doi.org/10.1007/s10462-020-09814-9).
- [37] A. Papanikolaou, A. Alevizopoulos, C. Ilioudis, K. Demertzis, and K. Rantos, "An autoML network traffic analyzer for cyber threat detection," *Int J Inf Secur*, vol. 22, no. 5, pp. 1511–1530, 2023, doi: [10.1007/s10207-023-00703-0](https://doi.org/10.1007/s10207-023-00703-0).
- [38] M. Repetto, D. Striccoli, G. Piro, A. Carrega, G. Boggia, and R. Bolla, "An Autonomous Cybersecurity Framework for Next-generation Digital Service Chains," *Journal of Network and Systems Management*, vol. 29, no. 4, p. 37, 2021, doi: [10.1007/s10922-021-09607-7](https://doi.org/10.1007/s10922-021-09607-7).
- [39] Y. Palmo, S. Tanimoto, H. Sato, and A. Kanai, "IoT Reliability Improvement Method for Secure Supply Chain Management," in *2021 IEEE 10th Global Conference on Consumer Electronics (GCCE)*, 2021, pp. 364–365. doi: [10.1109/GCCE53005.2021.9622088](https://doi.org/10.1109/GCCE53005.2021.9622088).
- [40] N. Yakin, M. Zhitkov, A. Chernikov, and P. Pepelyaev, "Security Threats and Service Degradation Detection in LoRaWAN Networks," in *2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBREIT)*, 2021, pp. 455–458. doi: [10.1109/USBREIT51232.2021.9455123](https://doi.org/10.1109/USBREIT51232.2021.9455123).
- [41] D. Mendez Mena and B. Yang, "Decentralized Actionable Cyber Threat Intelligence for Networks and the Internet of Things," *IoT*, vol. 2, no. 1, pp. 1–16, 2021, doi: [10.3390/iot2010001](https://doi.org/10.3390/iot2010001).
- [42] B. Rodrigues, E. Scheid, C. Killer, M. Franco, and B. Stiller, "Blockchain Signaling System (BloSS): Cooperative Signaling of Distributed Denial-of-Service Attacks," *Journal of Network and Systems Management*, vol. 28, no. 4, pp. 953–989, 2020, doi: [10.1007/s10922-020-09559-4](https://doi.org/10.1007/s10922-020-09559-4).
- [43] P. M. Santos et al., "Towards a Distributed Learning Architecture for Securing ISP Home Customers," in *Artificial Intelligence Applications and Innovations. AIAI 2021 IFIP WG 12.5 International Workshops*, I. Maglogiannis, J. Macintyre, and L. Iliadis, Eds., Cham: Springer International Publishing, 2021, pp. 311–322.
- [44] D. Mustefa and S. Punnekkat, "Cybersecurity Analysis for a Remote Drug Dosing and Adherence Monitoring System," in *IoT Technologies for HealthCare*, R. Goleva, N. R. da C. Garcia, and I. M. Pires, Eds., Cham: Springer International Publishing, 2021, pp. 162–178. Accessed: Dec. 18, 2023. [Online]. Available: https://doi.org/10.1007/978-3-030-69963-5_12
- [45] A. U. Sudugala, W. H. Chanuka, A. M. N. Eshan, U. C. S. Bandara, and K. Y. Abeywardena, "WANHEDA: A Machine Learning Based DDoS Detection System," in *2020 2nd International Conference on Advancements in Computing (ICAC)*, 2020, pp. 380–385. doi: [10.1109/ICAC51239.2020.9357130](https://doi.org/10.1109/ICAC51239.2020.9357130).
- [46] F. M. Isiaka, S. A. Audu, and M. A. Umar, "Developing a fail-safe culture in a cyber environment using MySQL replication

technique,” *International Journal of Crowd Science*, vol. 4, no. 2, pp. 149–170, Jan. 2020, doi: 10.1108/IJCS-04-2018-0008.

- [47] D. Suvarna and S. Pathak, “Threat Modeling for Breaking of CAPTCHA System,” in *Intelligent Computing, Information and Control Systems*, A. P. Pandian, K. Ntalianis, and R. Palanisamy, Eds., Cham: Springer International Publishing, 2020, pp. 94–104. Accessed: Dec. 18, 2023. [Online]. Available: https://bv.unir.net:2133/10.1007/978-3-030-30465-2_12

CIFRADO DE TEXTO MEDIANTE ATRACTORES CAÓTICOS: CRYPTOGUARD

Text encryption using chaotic attractors: Cryptoguard

Jemmy Anahí Puzma Granda ¹	jemmy.puzma@esPOCH.edu.ec
Danilo Mauricio Pástor Ramírez ²	danilo.pastor@esPOCH.edu.ec
Raúl Hernán Rosero Miranda ³	raul.rosero@esPOCH.edu.ec
Maricela Jiménez Rodríguez ⁴	maricela.jrodriguez@academicos.udg.mx
Omar S. Gómez ⁵	ogomez@esPOCH.edu.ec

^{1,2,3,5} Facultad de Informática y Electrónica, Escuela Superior Politécnica del Chimborazo (ESPOCH), Riobamba, Ecuador.

⁴ Profesora-investigadora en el Centro Universitario de la Ciénega, Universidad de Guadalajara.

RESUMEN

El presente estudio se embarca en la exploración de la criptografía basada en atractores caóticos, desarrollando una aplicación web destinada al cifrado y descifrado de cadenas de texto utilizando la sincronización de estos atractores. El primer paso de este estudio involucró una revisión detallada de cuatro sistemas caóticos para comprender a fondo las fórmulas de cada atractor. A través de una combinación de análisis matemático y programación, se implementó la sincronización de cada atractor en la aplicación web, utilizando la metodología SCRUMBAN, una combinación de los marcos de trabajo ágiles Scrum y Kanban. Las pruebas de Kruskal-Wallis, una prueba estadística no paramétrica utilizada para comparar tres o más grupos independientes de datos, revelaron diferencias significativas en los tiempos de sincronización, cifrado y descifrado entre los cuatro atractores. En términos concretos, estos resultados sugieren que el atractor de Lorenz es el más rápido para realizar la sincronización, cifrado y descifrado de cadenas de texto.

Palabras Clave: Cifrado de texto, Atractores caóticos, Seguridad web, Cifrado simétrico, Sistemas dinámicos caóticos.

we develop a web application intended for the encryption and decryption of text strings using the synchronization of these attractors. The first step of this study involved a detailed review of four chaotic systems to fully understand the formulas of each attractor. Through a combination of mathematical analysis and programming, the synchronization of each attractor was implemented in the web application, using the SCRUMBAN methodology, a combination of the agile frameworks Scrum and Kanban. Kruskal-Wallis tests, a nonparametric statistical test was used to compare three or more independent sets of data, revealed significant differences in synchronization, encryption, and decryption times between the four attractors. In concrete terms, these results suggest that the Lorenz attractor is the fastest to perform synchronization, encryption and decryption of text strings.

Palabras Clave: Text encryption, Chaotic attractors, Web security, Symmetric encryption, Chaotic dynamic systems.

ABSTRACT

The present study embarks on the exploration of cryptography based on chaotic attractors,

► I. Introducción

En la era digital actual, la seguridad de los datos se ha convertido en una prioridad crítica. La criptografía, el arte y la ciencia de cifrar información, es fundamental para proteger la comunicación en la extensa red de Internet. Con la evolución constante de las amenazas cibernéticas,

se requieren métodos de cifrado avanzados que no solo sean robustos sino también adaptables. En este contexto, la criptografía basada en atractores caóticos emerge como una alternativa prometedora, aprovechando la imprevisibilidad inherente a los sistemas caóticos para fortalecer la seguridad del cifrado.

Este artículo presenta el desarrollo de una aplicación web innovadora diseñada para el cifrado y descifrado de cadenas de texto, utilizando atractores caóticos como su piedra angular. Los atractores caóticos, derivados de sistemas dinámicos no lineales, ofrecen propiedades únicas como la sensibilidad a las condiciones iniciales y la mezcla topológica, las cuales son explotadas en este estudio para mejorar la seguridad del cifrado.

La contribución principal de este estudio es la implementación de un algoritmo de cifrado basado en atractores caóticos dentro de una interfaz de aplicación web accesible y fácil de usar. Se discutirá los atractores caóticos utilizados, desarrollo del algoritmo, la arquitectura de la aplicación y la evaluación de la seguridad del sistema propuesto. Además, se examinará la eficacia del cifrado en términos de comportamiento temporal.

► II. Marco teórico

A. Trabajos relacionados

Córdova Ramírez [1] tuvo como objetivo el desarrollo de un sistema en la cual se propone sistematizar el proceso de la redacción y generación de historiales médicos para reducir el tiempo de firma y aprobación de estos. Se utilizó el sistema RSA (Rivest, Shamir y Adleman) y la función hash SHA-256 para crear una firma digital.

Sheikholeslam utilizó sistemas dinámicos con atractores caóticos en el cifrado. Se basó en el sistema Encryption Dynamical para generar una clave de sincronización, y conseguir que el descifrado pueda actualizarse a las condiciones iniciales antes de generar el bloque. Como resultado se consiguió realizar una modificación discreta del sistema de Lorenz [2].

Gómez, Rosero, Estrada y Jiménez agregaron un mecanismo de seguridad a los objetos JSON mediante el uso de sincronización caótica. Y el resultado fue que este enfoque se puede aplicar como JSON Web Encryption (JWE) [3].

Montalván desarrolló el mecanismo de cifrado basado en el algoritmo criptográfico simétrico AES (MECIB-AES) para comparar la seguridad que brinda este a la información cifrada. Como resultado se obtuvo que la implementación de las modificaciones Mix-Shift, Mix-Key y Move-C ayudó a realizar diferentes pruebas donde se aceptó la hipótesis nula la cual midió la entropía, con un nivel de confiabilidad del 95% y un error del 5%, el análisis de frecuencias presentó variaciones en cada prueba realizada, la autocorrelación dió como resultado una mayor similitud de secuencias a favor del MECIB-AES, aunque puede tomarse como desventaja que los valores no son grandes por lo cual se consideró viable el algoritmo [4].

A pesar de que en el trabajo de Gómez et al. Agrega un mecanismo de seguridad a los objetos JSON mediante la sincronización caótica, no utiliza cadenas de texto para observar el cifrado y descifrado de la misma. De igual manera, en los trabajos revisados se utilizan sistemas de cifrado como RSA, SHA-256 y AES sin embargo, ninguno implementa cifrados con sistemas caóticos.

B. Caos

Ribero y Ramírez Proponen la manera en que un fenómeno presenta fluctuaciones en el tiempo es a menudo descrita por una ecuación diferencial. Por ejemplo, cuando una observación de un fenómeno en el periodo $n+1$ es una función de la observación del período n , que se puede expresar en general en la Ec. 1 [5].

$$(1) \quad X(n + 1) = F[X(n)]$$

Donde $F[X]$ sea una ecuación diferencial no lineal y de primer orden.

Desde el punto de vista matemático, se trata de ecuaciones diferenciales ordinarias, esto quiere decir que, poseen una única variable independiente

que cumplen las condiciones necesarias para asegurar la existencia y la unicidad de sus soluciones para cada conjunto de valores de las variables dependientes [6].

C. Sincronización caótica

La sincronización caótica consiste en hacer coincidir y converger en la misma trayectoria varios sistemas caóticos después de un tiempo suficiente. La idea general de la sincronización caótica utilizada en comunicaciones seguras es la siguiente. Primero, el transmisor cifra la información mediante un sistema caótico. Después, la información cifrada es enviada a través de un canal para ser recibida por el receptor. Finalmente, el receptor utiliza la sincronización para recuperar el mensaje original de la información cifrada [7].

D. Atractores

El término atractor extraño se usa para describir una región o forma hacia la cual los puntos son llevados como resultado de cierto proceso que muestra una dependencia sensible de las condiciones iniciales (es decir, puntos que inicialmente están cerca del atractor se separa exponencialmente con el tiempo) [8].

1. Atractor de Rossler

El atractor de Rössler es un sistema de tres ecuaciones diferenciales ordinarias no lineales estudiadas por el autor. Estas ecuaciones diferenciales definen un sistema dinámico del tiempo continuo que muestra dinámicas caóticas asociadas con las propiedades fractales del atractor. Algunas propiedades pueden ser deducidas a través de métodos lineales como auto vectores, pero las principales características del sistema requieren métodos no lineales como Aplicaciones de Poincaré o diagramas de bifurcación [9].

Se considera al sistema de Rossler mediante las Ec. 2, Ec. 3, y Ec. 4. [3].

$$\begin{aligned} (2) \quad & \dot{x}(t) = -y(t) - z(t) \\ (3) \quad & \dot{y}(t) = x(t) + ay(t) \\ (4) \quad & \dot{z}(t) = b + z(t)(x(t) - c) \end{aligned}$$

Se sabe que en los parámetros $\begin{cases} a = 0,2 \\ b = 0,2 \\ c = 5,7 \end{cases}$ este

sistema presenta comportamiento caótico (nótese que solo se cuenta con un término no lineal) [10].

Una imagen referencial de como se ve el atractor de Rossler es la que se muestra en la Fig:1.

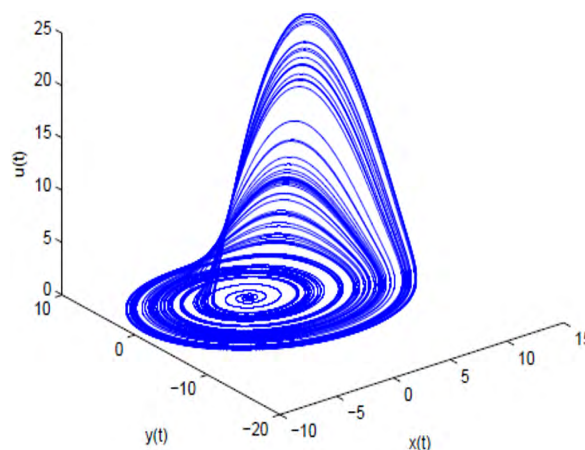


Fig. 1. Atractor de Rossler

2. Atractor de Lorenz

El atractor de Lorenz, es un sistema determinístico tridimensional derivado de las ecuaciones simplificadas de rolos de convección que se producen en las ecuaciones dinámicas de la atmósfera terrestre [9].

En el caso del sistema de Lorenz, el esquema maestro está representado por las Ecuaciones diferenciales ordinarias no lineales, ver en la Ec. 5, Ec. 6 y Ec.7 [3].

$$\begin{aligned} (5) \quad & \dot{x}(t) = \sigma(y(t) - x(t)) \\ (6) \quad & \dot{y}(t) = -x(t)z(t) + \rho x(t) - y(t) \\ (7) \quad & \dot{z}(t) = x(t)y(t) - \beta z(t) \end{aligned}$$

donde x_1, y_1, z_1 son las condiciones iniciales, y

$\begin{cases} a = 0,2 \\ b = 0,2 \\ c = 5,7 \end{cases}$ son los parámetros del sistema.

Se visualiza el Atractor de Lorenz en la Fig. 2.

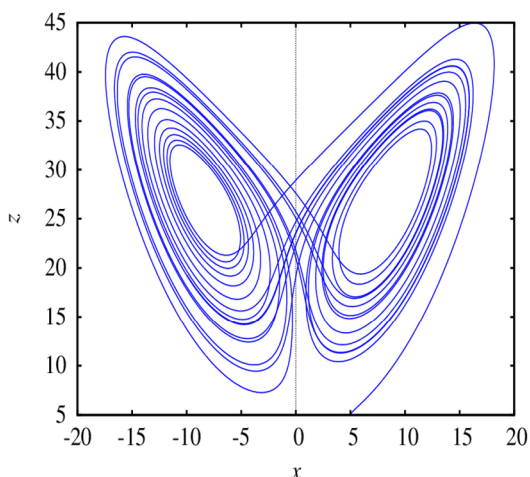


Fig. 2. Atractor de Lorenz

3. Atractor de Chen

Es un nuevo atractor caótico en un sistema autónomo tridimensional simple, que se asemeja a algunas características familiares de los atractores de Lorenz y Rossler [11].

Este sistema representado por la Ec. 8, Ec.9 y Ec. 10.

$$\begin{aligned} (8) \quad & \dot{x} = a(y - x) \\ (9) \quad & \dot{y} = (c - a)x - xz + cy \\ (10) \quad & \dot{z} = xy - bz \end{aligned}$$

donde x, y, z son las condiciones iniciales del sistema y $\begin{cases} a = 35 \\ b = 3 \\ c = 28 \end{cases}$ son los parámetros del sistema.

Se observa el atractor en la Fig. 3.

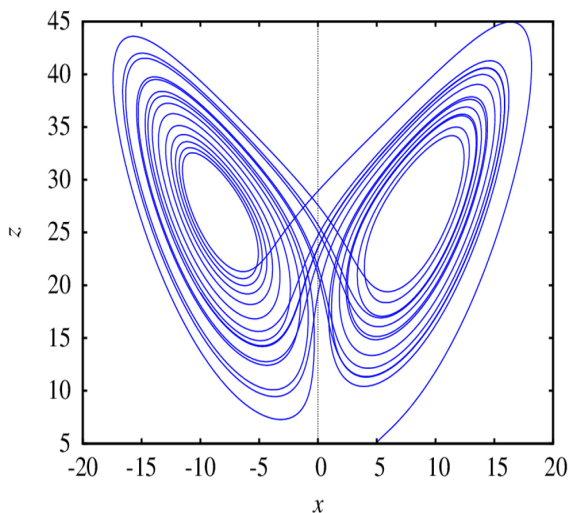


Fig. 3. Atractor de Chen

A finales del siglo pasado J. C. Sprott, introdujo una ecuación que producía caos en ciertos valores de parámetros, una característica importante de esta ecuación era la siguiente: Era una ecuación diferencial de tercer orden, que podría llevarse a tres de primer orden. Sprott construyó una serie de ecuaciones, que desde un punto de vista matemático eran muy sencillas, pero sus soluciones muestran estructuras muy complejas [12].

Está representado por las Ec. 11, Ec. 12 y Ec. 13 [13].

$$\begin{aligned} (11) \quad & \dot{x} = a(y - x) \\ (12) \quad & \dot{y} = bxz \\ (13) \quad & \dot{z} = c - xy \end{aligned}$$

Con sus parámetros correspondientes a $\begin{cases} a = 5 \\ b = 2 \\ c = 1,6 \end{cases}$

El atractor se lo grafica de la siguiente manera, como se muestra en la Fig. 4.

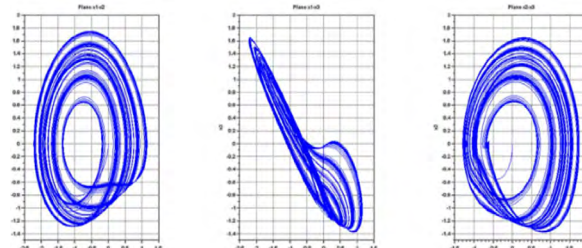


Fig. 4. Atractor de Sprott a), en planos x_1-x_2, x_1-x_3 y x_2-x_3

► III. Desarrollo de la aplicación web

A. Elicitación de requerimientos

En este sistema, los usuarios solicitan la capacidad de seleccionar entre distintos atractores para el cifrado y descifrado de textos, enfatizando la necesidad de una interfaz que permita esta selección de manera sencilla. Además, requieren funcionalidades para registrarse e iniciar sesión, lo que subraya la importancia de un sistema de acceso seguro y eficiente. Los usuarios también piden poder ingresar cadenas de texto para cifrar o descifrar, y desean visualizar el resultado del cifrado junto con información detallada sobre los tiempos de procesamiento. Por otro lado, los administradores del sistema requieren habilidades similares para registrarse e iniciar sesión, pero con capacidades adicionales como la eliminación

de usuarios y datos de cifrado/descifrado para mantener la actualidad y relevancia de los datos. Además, necesitan generar informes estadísticos a partir de los datos de cifrado y descifrado para análisis y seguimiento, así como la capacidad de monitorear las IPs y ubicaciones de inicio de sesión de los usuarios para asegurar un uso adecuado del sistema. Tanto usuarios como administradores enfatizan la necesidad de una función de cierre de sesión para mantener la seguridad y la integridad del sistema.

B. Conceptualización del sistema para el administrador

En la Fig. 5 se observa que el administrador se tiene que autenticarse para ingresar a la página principal, una vez ingresado puede escoger entre las opciones: Inicio, Atractores, Usuarios, Inicios de Sesión e Informes. En la opción de Inicio podrá visualizar información del cifrado y los informes datos estadísticos, se realizará la petición en la base de datos.

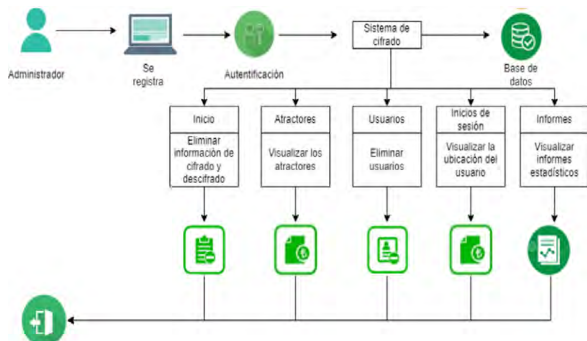


Fig. 5. Conceptualización del sistema para el administrador.

C. Conceptualización del sistema para el usuario

Se observa en la Fig. 6. que el usuario se autentica para ingresar al menú principal, donde constará de un inicio y opciones de cifrado, mediante Rossler, Lorenz, Chen y Sprott. En cada atractor se podrá ingresar una cadena de texto y al dar clic en el botón cifrar se mostrará información de tiempos de sincronización, cifrado, también tendrá la opción de descifrar en donde se ingresa la cadena de texto cifrada y mostrará la cadena descifrada, y el atractor utilizado con su tiempo. Se almacenará en la base de datos.

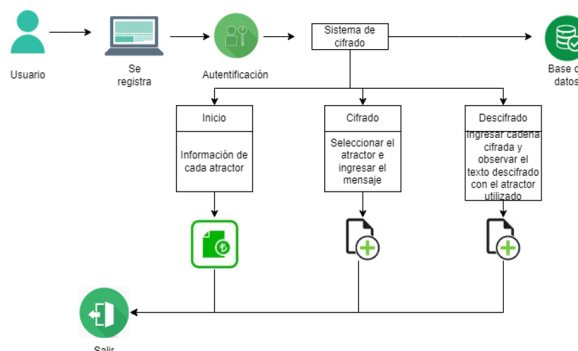


Fig. 6. Conceptualización del sistema para el usuario.

D. Diseño del algoritmo

El diseño del algoritmo es una fase crítica en la creación de una solución de cifrado efectiva y segura. Este proceso se dividió en dos etapas principales: la sincronización caótica y la construcción de las funciones de cifrado y descifrado. A continuación, se detallan los pasos y consideraciones metodológicas que guiaron el desarrollo del algoritmo.

1. Sincronización caótica

La sincronización caótica es el fundamento sobre el cual se construye la seguridad del algoritmo de cifrado. Para lograr una sincronización efectiva, se seleccionaron atractores caóticos basados en su complejidad dinámica y sensibilidad a las condiciones iniciales. Se implementó el método de sincronización mediante el vector de acoplamiento, asegurando que el emisor y el receptor pudieran generar secuencias caóticas idénticas en ausencia de diferencias en las condiciones iniciales. En la Fig. 7, Fig. 8, Fig. 9 y Fig. 10 se muestra como se sincronizan el sistema maestro y esclavo de cada uno de los atractores.

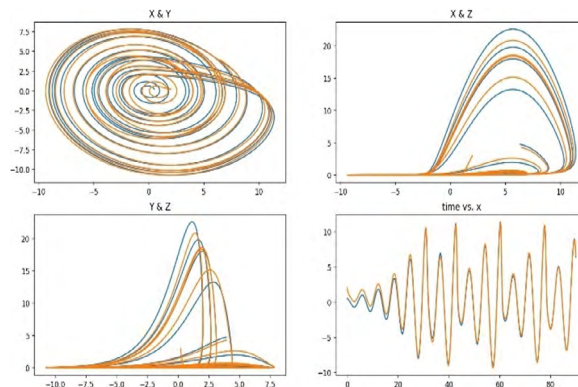


Fig. 7. Sincronización del atractor de Rossler.

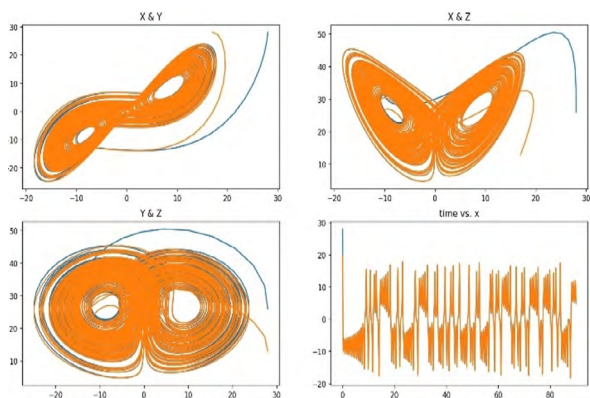


Fig. 8. Sincronización del atractor de Lorenz.

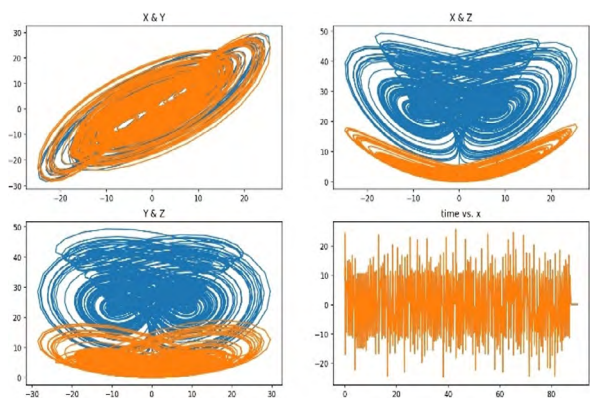


Fig. 9. Sincronización del atractor de Chen.

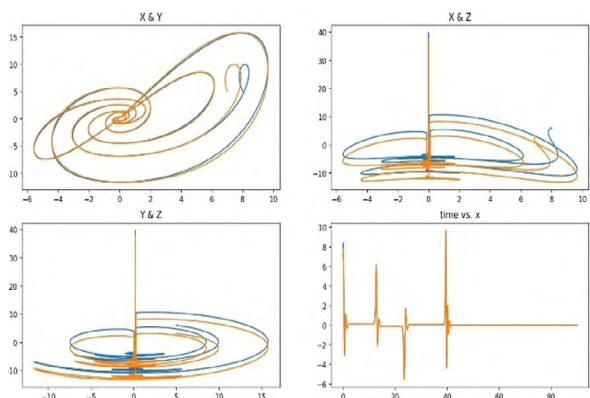


Fig. 10. Sincronización del atractor de Sprott.

1. Función de cifrado y descifrado

En base a la sincronización caótica, se creó las funciones de cifrado y descifrado que reciben como parámetros una cadena de texto y la opción dependiendo al atractor seleccionado, de acuerdo con esto se aplican las ecuaciones pertenecientes a cada uno de los atractores.

Esta función cifra un mensaje de texto utilizando la dinámica de sistemas caóticos sincronizados. Cada

carácter del mensaje se integra en una trayectoria caótica, y el resultado se codifica en base64. La sincronización caótica entre dos sistemas (maestro y esclavo) es clave en este proceso, ya que asegura que solo quien conozca las condiciones iniciales y las ecuaciones del sistema pueda descifrar el mensaje correctamente.

2. Arquitectura MVC

Para documentar la arquitectura se utiliza el modelo 4+1 de Krutchen, ver Fig. 11. Cada vista aborda un conjunto específico de preocupaciones de los diferentes interesados en el sistema.

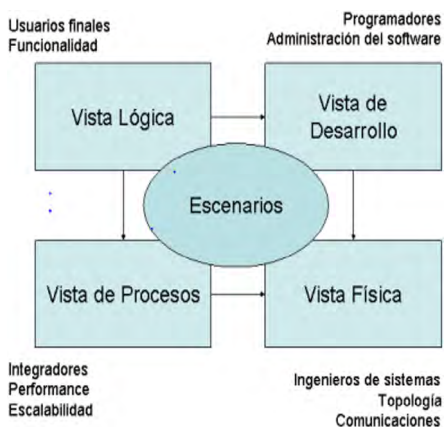


Fig. 11. Vistas del modelo 4+1 de Krutchen

1. Vista lógica

En la Fig. 12. de la vista lógica se observa el diagrama de clases que compone la aplicación web de cifrado. Esta vista es de gran interés para los desarrolladores de software y los analistas de sistemas, ya que se relaciona con la funcionalidad principal del sistema.

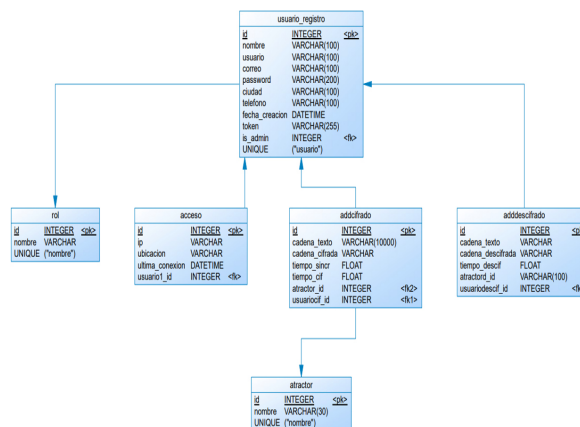


Fig. 12. Diagrama de clases

2. Vista de despliegue

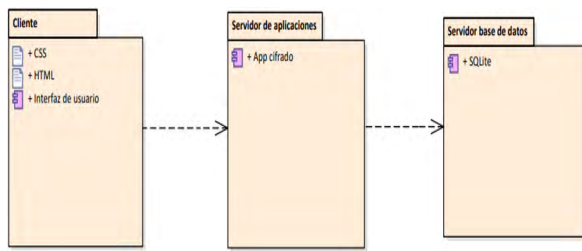


Fig. 13. Diagrama de componentes.

En esta vista se ha elegido representarla mediante el diagrama de componentes, que se visualiza en la Fig. 13. Incluye aspectos como la gestión de la configuración y la organización de software en unidades de implementación como archivos de código fuente, scripts, bibliotecas.

3. Vista de procesos

En la Fig. 14 se muestra el diagrama de actividades del cifrado y en el Fig.15 del descifrado. Se ocupa de los aspectos dinámicos del sistema, explicando cómo se ejecuta el sistema en términos de procesos o hilos.

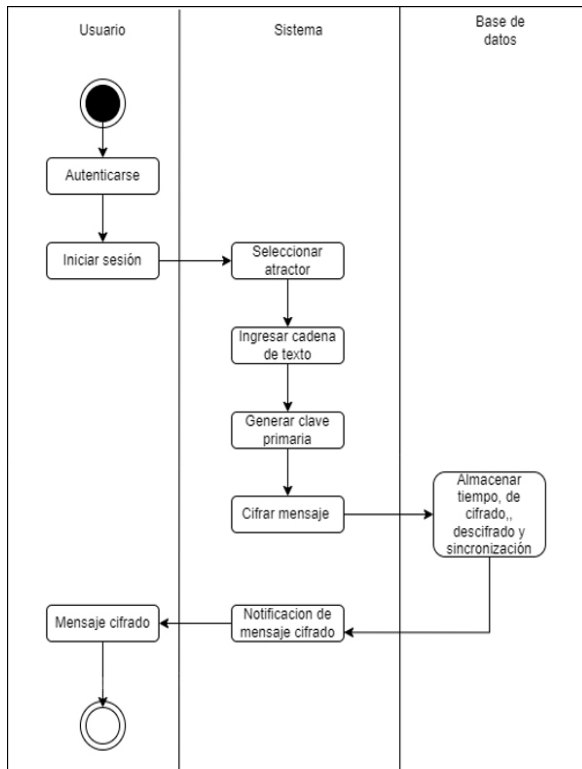


Fig. 14. Diagrama de actividades del cifrado.

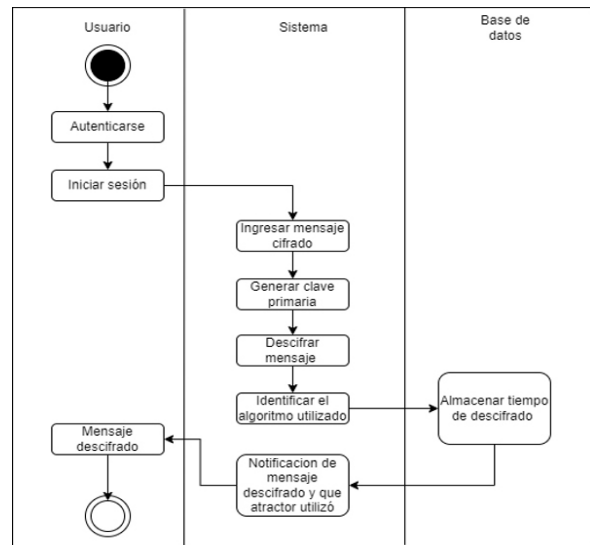


Fig. 15. Diagrama de actividades del descifrado.

4. Vista física

La siguiente Fig. 16. muestra el usuario que utiliza una computadora para ingresar al sistema, y solicitar las peticiones al servidor.

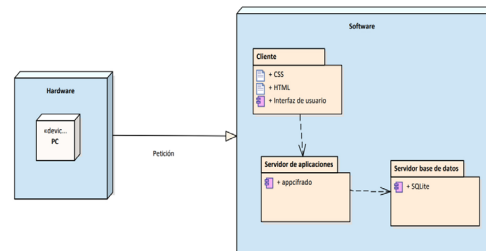


Fig. 16. Diagrama de despliegue.

5. Vista de escenario

Para la vista de escenario se muestra el diagrama de caso de uso, ver Fig. 17.

Este diagrama permite observar el funcionamiento del sistema completo con las interacciones de los usuarios y administradores.

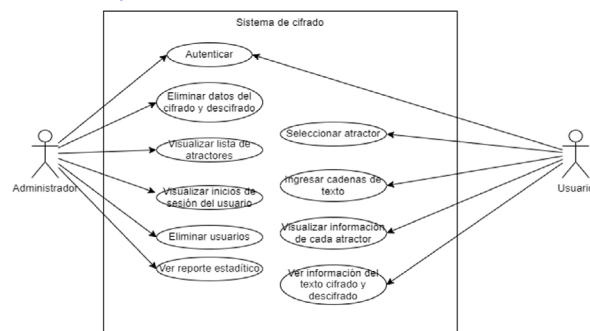


Fig. 17. Diagrama de caso de uso

F. Pruebas

En la Fig. 18 se muestra el menú del cifrado para que el usuario pueda seleccionar el atractor con el cual desea trabajar.



Fig. 18. Aplicación web, menú cifrado.

Para el descifrado se creó una sola entrada de texto cifrado, e internamente se identifica el atractor utilizado y se muestra en pantalla. Ver Fig. 19.



Fig. 19. Aplicación web, descifrado

► **IV. Análisis e interpretación de resultados**

Se presenta los resultados obtenidos con el desarrollo de la aplicación web para cifrar y descifrar cadenas de texto mediante la selección de un atractor caótico. Estos resultados se obtuvieron mediante técnicas de medición del comportamiento temporal, y la confidencialidad, según los resultados obtenidos se aplicó test no paramétrico de Kruskal Wallis y diagramas de dispersión respectivamente.

A. Evaluación del comportamiento temporal

2. Proceso cifrado

Tiempo de sincronización

En la Tabla II se muestran los resultados de las 25 muestras por cada atractor, obteniendo el promedio de tiempo de sincronización en microsegundos.

Atractor	Promedio del tiempo de sincronización.
Chen	213428,44 μ s
Lorenz	34650,96 μ s
Rosler	314535,92 μ s
Sprott	74541,6 μ s

Para tener una mejor visualización de los resultados se muestra en la Fig. 20. barras generado desde la aplicación web de cifrado y descifrado.

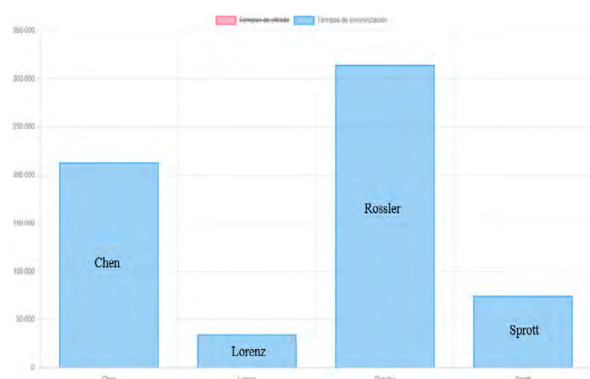


Fig. 20. Barras del tiempo de sincronización.

Se demuestra que el atractor de Lorenz es el más rápido en realizar la sincronización y el atractor de Rossler es el que tarda más.

Evaluación de supuestos del modelo

Se realiza una evaluación de supuestos del modelo para determinar si es factible realizar un análisis de varianza, o de lo contrario utilizar una prueba no paramétrica.

Para los análisis se utiliza un nivel de significancia de 0.05.

Igualdad de varianzas

Se utilizó levenetest para observar si existe una igualdad en las varianzas. Ver Fig. 21.

```
> leveneTest(tiempo_sincr ~ atractor_id, cifradotabla3)
Levene's Test for Homogeneity of Variance (center = median)
  Df F value Pr(>F)
group 3 4.791 0.003736 **
    96
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
```

Fig. 21. Test de levene para el tiempo de sincronización

Dado que el p-valor (0.003736) es significativamente menor que 0.05, se puede rechazar la hipótesis nula (H0) de igualdad de varianzas entre los atractores. Esto significa que existe evidencia suficiente para afirmar que las varianzas de los tiempos de sincronización son diferentes entre al menos dos de los grupos definidos por el atractor_id.

Normalidad de los residuos del modelo

En la prueba de normalidad de Lilliefors (Kolmogorov-Smirnov) se obtuvo lo siguiente ver Fig. 22.

```
> lillie.test(standard_res)

Lilliefors (Kolmogorov-Smirnov) normality test

data: standard_res
D = 0.31297, p-value < 2.2e-16
```

Fig. 22. Prueba de normalidad de Lilliefors del tiempo de sincronización.

La hipótesis nula (H0) de la prueba de Lilliefors es que los datos siguen una distribución normal. La hipótesis alternativa (H1) es que los datos no siguen una distribución normal.

Dado que el p-valor es extremadamente pequeño (< 2.2e-16) y es menor que el nivel de significancia

de 0.05, se puede concluir que hay evidencia suficiente para rechazar la hipótesis nula (H0). Es decir, los datos de la variable "standard_res" no siguen una distribución normal.

Según los resultados observados se determinó que es necesario realizar una prueba no paramétrica, en este caso se utiliza la prueba de Kruskal Wallis. Fig. 24.

```
> kruskal.test(tiempo_sincr ~ atractor_id, cifradotabla3)
```

```
Kruskal-wallis rank sum test

data: tiempo_sincr by atractor_id
Kruskal-wallis chi-squared = 43.833, df = 3, p-value = 1.638e-09
```

Fig. 23. Test de Kruskal Wallis para el tiempo de sincronización

La hipótesis nula (H0) de la prueba de Kruskal-Wallis es que no hay diferencias entre las medianas de los grupos definidos por el atractor_id. La hipótesis alternativa (H1) es que al menos una mediana es diferente.

Dado que el valor p obtenido en la prueba (1.638e-09) es mucho menor que el nivel de significancia de 0.05, se puede concluir que hay evidencia suficiente para rechazar la hipótesis nula (H0). Esto significa que al menos una de las medianas del tiempo de sincronización en microsegundos difiere significativamente entre los grupos definidos por el atractor_id.

Tiempo de cifrado

En la Tabla III se muestran los resultados de las 25 muestras por cada atractor, obteniendo el promedio de tiempo de cifrado en microsegundos.

Tabla 2.
Promedios del tiempo de cifrado

Atractor	Promedio del tiempo de cifrado.
Chen	200683,48 μs
Lorenz	46287,52 μs
Rosler	349716,92 μs
Sprott	74817,28 μs

Para tener una mejor visualización de los resultados se muestra un gráfico de barras generado desde la aplicación web. Fig. 24.



Fig. 24. Barras del tiempo de cifrado.

Se demuestra que el atractor de Lorenz es el más rápido para realizar el cifrado de cadenas de texto y Rössler es el más lento.

Evaluación de supuestos del modelo

Se realiza una evaluación de supuestos del modelo para determinar si es factible realizar un análisis de varianza, o de lo contrario utilizar una prueba no paramétrica.

Para los análisis se utiliza un nivel de significancia de 0.05.

Igualdad de varianzas

Se utilizó levenetest para observar si existe una igualdad en las varianzas. Ver Fig. 25.

```
> leveneTest(tiempo_cif ~ atractor_id, cifradotabla3)
Levene's Test for Homogeneity of Variance (center = median)
Df F value Pr(>F)
group 3 4.4282 0.005836 **
    96
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
```

Fig. 25. Test de levene para el tiempo de cifrado.

Los resultados del test de Levene indican que existe una diferencia significativa en la variabilidad del tiempo de cifrado entre los diferentes grupos de atractores. El valor p (0.005836) es menor que el nivel de significancia establecido (0.05), lo que significa que hay una fuerte evidencia para rechazar la hipótesis nula de que las varianzas de los tiempos de cifrado son iguales para todos los atractores.

Normalidad de los residuos del modelo

En la prueba de normalidad de Lilliefors (Kolmogorov-Smirnov) se obtuvo lo siguiente. Fig. 26.

```
> lillie.test(standard_res1)

Lilliefors (Kolmogorov-Smirnov) normality test

data: standard_res1
D = 0.23238, p-value = 1.442e-14
```

Fig. 26. Test de normalidad para el tiempo de cifrado

El valor p en esta prueba es extremadamente bajo (1.442e-14, es decir, 0.000000000000001442). Un valor p bajo sugiere que se debe rechazar la hipótesis nula. En el caso de la prueba de Lilliefors, la hipótesis nula es que los datos siguen una distribución normal.

Según los resultados observados se determinó que es necesario realizar una prueba no paramétrica, en este caso se utiliza la prueba de Kruskal Wallis. Fig. 27.

```
> kruskal.test(tiempo_cif ~ atractor_id, cifradotabla3)

Kruskal-wallis rank sum test

data: tiempo_cif by atractor_id
Kruskal-wallis chi-squared = 39.107, df = 3, p-value = 1.647e-08
```

Fig. 27. Test de Kruskal Wallis para el tiempo de cifrado.

Dado este valor p extremadamente bajo, hay fuertes evidencias para rechazar la hipótesis de que los tiempos de cifrado son iguales para todos los atractores. Esto sugiere que al menos un atractor tiene un tiempo de cifrado mediano significativamente diferente a los demás.

2. Proceso descifrado

En la Tabla IV se muestran los resultados de las 25 muestras por cada atractor, obteniendo el promedio de tiempo de descifrado en microsegundos.

Tabla 3. Resultados del proceso de descifrado

Atractor	Promedio del tiempo de descifrado.
Chen	387290,32 μs
Lorenz	287799,44 μs
Rössler	379987,72 μs
Sprott	301363,72 μs

Para tener una mejor visualización de los resultados se muestra un gráfico de barras generado desde la aplicación web. Fig. 28.



Fig. 28. Barras del tiempo de descifrado.

Se comprueba que existe una similitud entre los atractores, lo que indica que cualquier atractor es recomendado para realizar el descifrado.

Evaluación de supuestos del modelo

Se realiza una evaluación de supuestos del modelo para determinar si es factible realizar un análisis de varianza, o de lo contrario utilizar una prueba no paramétrica.

Para los análisis se utiliza un nivel de significancia de 0.05.

Igualdad de varianzas

Se utilizó levenetest para observar si existe una igualdad en las varianzas. Ver Fig. 29.

```
> leveneTest(tiempo_descif ~ atractord_id, descifradotabla3)
Levene's Test for Homogeneity of Variance (center = median)
  Df F value Pr(>F)
group 3  0.8316 0.4797
```

Fig. 29. Test de levene para el tiempo de descifrado

Según la Prueba de Levene, no hay una diferencia significativa en la varianza del tiempo de descifrado entre los diferentes atractores en el conjunto de datos. Esto significa que la variabilidad del tiempo de descifrado es la misma para todos los atractores.

Normalidad de los residuos del modelo

En la prueba de normalidad de Lilliefors (Kolmogorov-Smirnov) se obtuvo lo siguiente Fig. 30.

```
> lillie.test(standard_res2)

Lilliefors (Kolmogorov-Smirnov) normality test

data: standard_res2
D = 0.26212, p-value < 2.2e-16
```

Fig. 30. Prueba de Lilliefors para el tiempo de descifrado.

El valor p de esta prueba es extremadamente bajo, menos de 2.2e-16 (esto es prácticamente cero). Un valor p muy bajo sugiere que se puede rechazar la hipótesis nula. En este caso, la hipótesis nula es que los datos siguen una distribución normal.

Según los resultados observados se determinó que es necesario realizar una prueba no paramétrica, en este caso se utiliza la prueba de Kruskal Wallis. Fig. 31.

```
> kruskal.test(tiempo_descif ~ atractord_id, descifradotabla3)

Kruskal-Wallis rank sum test

data: tiempo_descif by atractord_id
Kruskal-Wallis chi-squared = 21.513, df = 3, p-value = 8.237e-05
```

Fig. 31. Test de Kruskal Wallis para el tiempo de descifrado.

Dado este valor p muy bajo (que es mucho menor que el nivel de significancia definido de 0.05), hay fuertes evidencias para rechazar la hipótesis de que los tiempos de descifrado son iguales para todos los atractores. Esto sugiere que al menos un atractor tiene un tiempo de descifrado mediano significativamente diferente a los demás.

3. Resultados finales

En conclusión, los resultados de los tests Kruskal-Wallis para el tiempo de sincronización, cifrado y descifrado demuestran que se debe rechazar la hipótesis nula (H0) en favor de la hipótesis alternativa (H1). Esto significa que al menos uno de los cuatro atractores difiere sustancialmente del resto en términos de tiempo de sincronización, cifrado y descifrado.

B. Evaluación de la confidencialidad

Los resultados que se obtuvieron se basaron en una cadena de texto de 118 caracteres.

En la Fig. 32 se muestra un gráfico de dispersión de la comparación de los valores del texto plano con el texto cifrado.

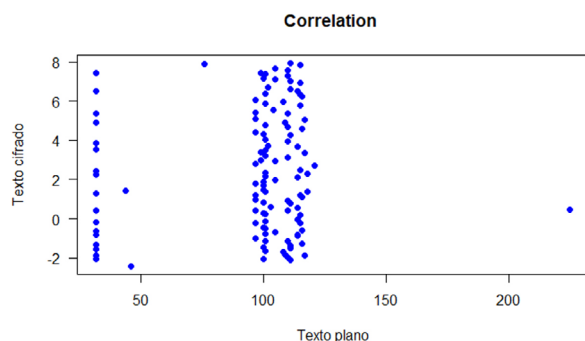


Fig. 32. Correlación del texto plano con el cifrado del atractor Rossler.

Se puede prestar atención que no tiene ninguna relación el texto plano y el texto cifrado, por lo que se determina que no existen patrones en los que se pueda lograr descifrar el mensaje sin conocer la llave.

El coeficiente de correlación de Pearson calculado fue de 0,08 con un valor p no significativo de 0,38, lo que sugiere que no hay evidencia suficiente para afirmar que existe una correlación lineal entre texto plano y texto cifrado.

A continuación, se muestra la Fig. 33 con la información del texto plano y el texto regenerado después del proceso de descifrado.

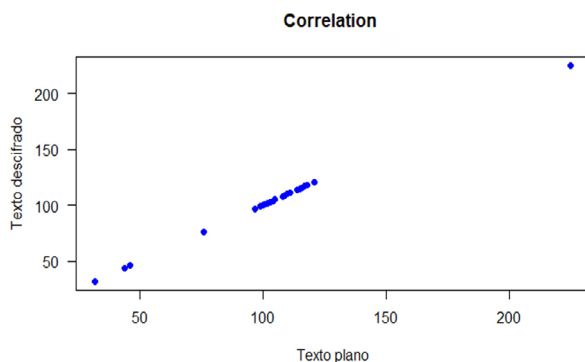


Fig. 33. Correlación entre el texto plano y el regenerado después del descifrado del atractor Rossler.

El texto se regenera por completo sin perder información después de descifrarse el mensaje. Se observó un coeficiente de correlación de 1, lo que indica que hay total similitud entre el mensaje original y el descifrado.

Se mantiene el mismo comportamiento en todos los atractores.

► V. Conclusiones

A lo largo del estudio, se efectuó un análisis minucioso de cuatro sistemas caóticos esenciales: Rossler, Lorenz, Chen y Sprott. Cada sistema, con su atractor característico y comportamiento dinámico, desempeña un papel vital en la comprensión del caos. Desde la estructura en espiral del Rossler, pasando por el icónico atractor con forma de "mariposa" de Lorenz, hasta las complejidades distintivas de Chen y Sprott, estos sistemas se han destacado por su naturaleza impredecible y altamente sensible a las condiciones iniciales. Esta singularidad y complejidad los convierten en herramientas poderosas, subrayando su significado y aplicabilidad en el mundo del cifrado y descifrado. La revisión de estos sistemas no solo ha permitido un entendimiento profundo del caos, sino que también ha establecido un fundamento sólido para futuras aplicaciones y estudios en el campo de la seguridad cibernética.

Más allá de una mera revisión teórica, el estudio se adentró en la práctica, llevando a cabo un proceso de sincronización caótica para cada uno de estos atractores. Los resultados revelaron detalles interesantes y esenciales para la implementación práctica de estos sistemas en la ciberseguridad. A través del uso del test Kruskal-Wallis, se pudo determinar diferencias significativas en los tiempos de sincronización entre los atractores. El atractor de Lorenz, con su complejo comportamiento y estructura, emergió como el más eficiente en términos de sincronización, lo que sugiere su gran potencial en aplicaciones de cifrado. Estos hallazgos no solo fortalecen la comprensión del comportamiento caótico, sino que también guían futuras investigaciones y aplicaciones en áreas críticas como la seguridad cibernética.

El desarrollo de la aplicación web representó un desafío técnico y metodológico, que se abordó con éxito mediante el empleo de SCRUMBAN como metodología de trabajo. SCRUMBAN combina elementos de SCRUM y Kanban, dos enfoques ágiles que promueven la flexibilidad, adaptabilidad y eficiencia en la producción.

Se llevó a cabo una evaluación rigurosa de la eficiencia y seguridad en el cifrado y descifrado en la aplicación desarrollada. Los análisis de tiempo revelaron diferencias significativas entre los atractores, subrayando la necesidad de equilibrar la velocidad y la seguridad en la elección de los métodos de cifrado. Quedando como el más eficiente en el cifrado y descifrado el atractor de Lorenz.

» VI. Agradecimientos

Quisiera expresar mi más profundo agradecimiento al grupo de investigación GrIISoft de la Facultad de Informática y Electrónica (FIE) de la Escuela Superior Politécnica de Chimborazo (ESPOCH), por su invaluable apoyo y colaboración en el desarrollo del proyecto titulado "Enfoque de cifrado de objetos JSON utilizando sincronización caótica a partir del análisis de un conjunto de atractores".

La oportunidad de trabajar junto a un equipo tan experimentado y dedicado ha sido una experiencia enriquecedora y fundamental para el éxito de esta investigación. La orientación, el conocimiento y los recursos proporcionados por GrIISoft han sido elementos clave en la realización de este estudio, permitiéndome explorar nuevas fronteras en el campo del cifrado y la seguridad de la información.

» VII. Referencias

- [1] J. Cordova Ramirez, H. Vega Huerta, C. Rodriguez Rodriguez, y F. Escobedo Bailón, «Firma digital basada en criptografía asimétrica para generación de historial clínico», 3C Technol. Innov. Apl. Pyme, pp. 65-85, dic. 2020, doi: 10.17993/3ctecno/2020.v9n4e36.65-85.
- [2] A. Sheikholeslam, «A chaos based encryption method using dynamical systems with strange attractors»: en Proceedings of the International Conference on Security and Cryptography, Milan, Italy: SciTePress - Science and Technology Publications, 2009, pp. 259-265. doi: 10.5220/0002105402590265.
- [3] O. S. Gómez, R. Rosero Miranda, J. Estrada-Gutiérrez, y M. Jiménez-Rodríguez, «An Approach for Securing JSON Objects through Chaotic Synchronization», Cybern. Inf. Technol., vol. 22, pp. 23-34, dic. 2022, doi: 10.2478/cait-2022-0037.
- [4] C. E. R. Montalván, «Desarrollo de un mecanismo de cifrado basado en el algoritmo criptográfico simétrico aes», p. 139, 2019.
- [5] R. Ribero Medina y M. Ramirez Gómez, «Caos: Definición, Detección y Ejemplos», 1992, doi: <https://revistas.uniandes.edu.co/doi/pdf/10.13043/dys.30.7>.
- [6] O. Lombardi, «La teoría del caos y el problema del determinismo», p. 22, 2020.
- [7] J. Zaqueros-Martínez, G. Rodríguez-Gómez, E. Tlelo-Cuatle, y F. Orihuela-Espina, «Sincronización de sistemas caóticos fraccionarios», p. 73, 2020.
- [8] J. C. P. Campuzano, «Strange Attractors», Strange Attractors. Accedido: 12 de enero de 2023. [En línea]. Disponible en: <https://jponce.github.io/>
- [9] E. Pacheco Cruz, «Atractor de Lorenz y Rossler | PDF | Teoría del caos | Atractor», Scribd. Accedido: 30 de diciembre de 2022. [En línea]. Disponible en: <https://es.scribd.com/document/398824115/Atractor-de-Lorenz-y-Rossler>
- [10] C. A. Ibanez, «Identificación del sistema de Rossler: enfoque algebraico y algoritmos genéticos», 2005.
- [11] G. Chen y T. Ueta, «Yet Another Chaotic Attractor», Int. J. Bifurc. Chaos - IJBC, vol. 9, pp. 1465-1466, jul. 1999, doi: 10.1142/S0218127499001024.
- [12] G. Paredes, «Los Flujos Caóticos Más Simples (FCMS) Un mito entre lo complejo y lo complicado». 2023. [En línea]. Disponible en: <http://casanchi.org/mat/flujoscaoticos01.pdf>

- [13] Q. Lai y S. Chen, «Generating Multiple Chaotic Attractors from Sprott B System», Int. J. Bifurc. Chaos, vol. 26, p. 1650177, oct. 2016, doi: 10.1142/S0218127416501777.

PÉRDIDAS ECONÓMICAS Y PELIGROS QUE REPRESENTAN LAS MALAS CONEXIONES ELÉCTRICAS

Economic losses and dangers represented by bad electrical connections

César Astudillo Machuca ¹	castudillo@epoch.edu.ec
Natali Astudillo Skliarova ²	nastudillo@est.ups.edu.ec

¹ Facultad de Mecánica, Posgrado en Electricidad, Escuela Superior Politécnica de Chimborazo (ESPOCH)

² Universidad Politécnica Salesiana, Riobamba, Ecuador; Guayaquil, Ecuador

RESUMEN

Este artículo aborda la importancia de comprender los principios básicos de la electricidad para evitar pérdidas económicas y mitigar los peligros derivados de malas conexiones eléctricas. El presente trabajo se divide en dos partes, la primera describe cómo el desconocimiento puede resultar en pérdidas económicas evitables, proponiendo normas sencillas para prevenir daños a dispositivos esenciales en nuestra vida diaria. La segunda parte analiza los riesgos inherentes a las conexiones eléctricas deficientes, subrayando la amenaza potencial que la electricidad representa en nuestras vidas. Se hace hincapié en la importancia de no subestimar los aspectos técnicos necesarios para evitar accidentes mortales, enfocándose en la seguridad como prioridad fundamental.

Palabras Clave: Conexiones, seguridad, electricidad, pérdidas.

ABSTRACT

This article addresses the importance of understanding the basic principles of electricity to avoid economic losses and mitigate the dangers associated with poor electrical connections. The present work is divided into two parts. The first part describes how ignorance can lead to avoidable economic losses, proposing simple standards to prevent damage to essential devices in our daily lives. The second part analyzes the risks inherent in faulty electrical connections, emphasizing the potential threat that electricity poses in our lives.

There is a strong emphasis on not underestimating the technical aspects necessary to prevent fatal accidents, with a focus on safety as a fundamental priority.

Palabras Clave: Connections, security, electricity, losses

► I. Introducción

Cuando las conexiones eléctricas son inadecuadas, existe un mayor riesgo de cortocircuitos, sobrecargas y sobrecalentamiento. Estos problemas pueden generar chispas, arcos eléctricos y puntos de ignición que pueden dar lugar a incendios.

En el ámbito económico, las malas conexiones eléctricas pueden provocar daños en los equipos y aparatos eléctricos, lo que implica costosos gastos de reparación o reemplazo.

Problemas como la desconexión del neutro conllevan el riesgo de que los aparatos eléctricos conectados al circuito se dañen irreparablemente, no solo maestros electricistas, sino también profesionales, han desconectado el neutro con cargas vivas en tableros, sean estos principales, de distribución o secundarios, sin ser conscientes de las consecuencias.

La profesión de ingeniero eléctrico brinda la oportunidad de presenciar de cerca los peligros y

las consecuencias asociadas con las instalaciones eléctricas deficientes.

El presente trabajo pretende abarcar dos aspectos importantes, los impactos económicos y los peligros que conllevan las malas prácticas al momento de hacer instalaciones eléctricas residenciales, para ellos se ha dividido en dos capítulos, el primero corresponde a un marco teórico que describe los problemas más comunes que se generan al momento de realizar instalaciones eléctrica desconociendo normas y los graves problemas que pueden surgir si las personas tienen contacto con redes eléctricas deficientes.

El segundo capítulo está dedicado a casos prácticos correspondientes a la actividad profesionalista “in situ” y las soluciones más adecuadas para cada tipo de problema.

» II. MARCO TEÓRICO

A. PRIMERA PARTE

Problemas que se generan debido a las instalaciones eléctricas deficientes

Cortocircuitos

Un cortocircuito es una conexión eléctrica accidental y no deseada entre dos puntos de diferente polaridad en un sistema eléctrico. Esto crea una ruta de baja resistencia para la corriente eléctrica, evitando su flujo normal a través del circuito.

Los cortocircuitos representan peligros significativos, como interrupción del suministro eléctrico, sobrecalentamiento de conductores, riesgo de incendio debido al calor generado, daño a equipos eléctricos, y descargas eléctricas para las personas.

Fallas a tierra

Una falla a tierra en instalaciones eléctricas de vivienda ocurre cuando hay un contacto no deseado entre un conductor eléctrico activo y una superficie conductora a tierra. Esto puede

llevar a peligros significativos, como descargas eléctricas potencialmente mortales para las personas que entran en contacto con la superficie conductora o el equipo afectado. Además, puede provocar incendios debido al sobrecalentamiento de los conductores y cables, daños a los equipos eléctricos conectados, interrupción del suministro eléctrico, riesgo de explosiones y lesiones graves o fatales.

Mal dimensionamiento o ausencia de la puesta a tierra

Sin la conexión adecuada a tierra, no hay una vía segura para que la corriente eléctrica fluya en caso de una falla. Esto puede resultar en descargas eléctricas para las personas que entran en contacto con equipos eléctricos defectuosos. Además, hay un mayor riesgo de incendios debido al sobrecalentamiento de cables, así como la posibilidad de daños graves a los equipos eléctricos y la interrupción del suministro eléctrico.

¿Qué es la puesta a tierra?

Se puede definir como “puesta a tierra” a un sistema de conexión eléctrico compuesto por electrodos y cables que se conectan directamente a los enchufes y carcasas de los equipos que utilizan energía para su funcionamiento. Su propósito principal es proteger contra descargas repentinas, ya sean naturales, como los rayos, o artificiales, como las sobrecargas, interferencias o errores humanos. La calidad de la puesta a tierra depende de dos parámetros fundamentales: la resistividad del suelo y la resistencia de tierra.

Resistividad del suelo

La resistividad del suelo es una propiedad intrínseca del suelo que indica su capacidad para resistir el flujo de corriente eléctrica.

Se mide en ohmios-metros y depende de factores como la composición del suelo, la humedad y la temperatura. Para calcular la resistencia de la toma a tierra se emplea la siguiente fórmula:

$$R = \rho \frac{L}{A} \quad (1)$$

Donde:

R: Resistencia de la toma tierra, medida en Ω

ρ Resistividad medida en Ωm

L: Longitud del enterramiento del electrodo

A: Área transversal del electrodo

La resistencia de puesta a tierra es directamente proporcional a la resistividad del suelo. Esto significa que a medida que la resistividad del suelo aumenta, la resistencia de puesta a tierra también aumenta.

Existen distintos tipos de electrodos, dependiendo del electrodo seleccionado, se aplica la fórmula para obtener la resistencia de la toma a tierra, a continuación en la tabla I se detallan las fórmulas para los tipos de electrodos más comúnmente utilizados:

Tabla 1

RESISTENCIA DE LA TOMA A TIERRA SEGÚN EL TIPO DE ELECTRODO

Tipo de electrodo	Fórmula
Placa	$R = \frac{0,8 \rho}{P}$
Pica Vertical	$R = \frac{\rho}{L}$
Conductor enterrado de forma horizontal	$R = \frac{2 \rho}{L}$

R: Resistencia de la toma tierra, medida en Ω

ρ Resistividad medida en Ωm

L: Longitud del enterramiento del electrodo

P: Perímetro de la placa

Tabla II

VALORES TÍPICOS DE LA RESISTIVIDAD DEL SUELO

Tipo de material	Ωm
Suelo húmedo y arcilloso	1.5 – 3
Suelos limosos y limo arcilloso húmedo	3 – 15.2
Suelos limosos y arenas semisecas	15.2 – 152.4
Roca fracturada en matriz de suelo húmedo	152.4– 304.8
Arena y gravas con limos	304.8
Roca ligeramente fracturada en matriz de suelo seco	304.8 – 2438
Roca masiva, arena seca y gruesa y depósitos de grava	2438 – sup







Cuando el valor de resistencia de tierra no cumple con los estándares requeridos por la empresa distribuidora, existen varios métodos para mejorarla. Estos métodos incluyen:

- Aumento de la longitud de la varilla de tierra.
- Utilización de varias varillas de tierra.
- Tratamiento del suelo para mejorar su conductividad.
- Aumento del diámetro de los electrodos de tierra.
- Cambio del terreno existente por otro con menor resistividad.
- Aplicación de tratamiento químico electrolítico al suelo.
- Construcción de mallas o zanjas de interconexión con cambio de tierra y tratamiento químico, utilizando cables desnudos de calibre adecuado para aprovechar las propiedades de los contrapesos radiales.

Para utilizar varias varillas los porcentajes de reducción de la resistividad del terreno se detallan en la tabla III:

Tabla III

MÉTODO DE VARILLAS PARA EL MEJORAMIENTO DE TIERRA

Configuración	Descripción	Porcentaje de reducción de la resistencia de la malla
	2 electrodos en paralelo	Reducción 55%
	3 electrodos en línea recta	Reducción 35%
	3 electrodos en delta	Reducción 38%
	4 electrodos en cuadro	Reducción 28%
	8 electrodos en cuadro	Reducción 17%
	8 electrodos en círculo	Reducción 16%

En los edificios residenciales, se establecen ciertas normas para la instalación de sistemas de puesta a tierra. La línea principal de tierra se colocará en la misma canalización que la línea general de alimentación. En los edificios de nueva construcción, antes de hormigonar, se instala un cable de cobre desnudo en el fondo de las zanjas de cimentación, formando un anillo cerrado que rodea todo el perímetro del edificio.

La estructura metálica del edificio se conecta a este anillo mediante soldadura para asegurar su fiabilidad. Las tomas de tierra se entierran a una profundidad mínima de 0.5m. El anillo de tierra será de cobre desnudo, si es necesario reducir la resistencia a tierra del anillo, se pueden agregar electrodos en forma de picas o placas verticalmente hincados en el suelo. Las picas de 2 metros de longitud son las más comunes como electrodos. El número de picas conectadas al anillo conductor dependerá de la resistencia requerida.

Si se necesitan dos picas conectadas en paralelo, se recomienda que la separación entre ellas sea al menos igual a la longitud enterrada de las picas. En el caso de varias picas conectadas en paralelo, la separación entre ellas debe ser mayor que en el caso anterior.

Desconexión del neutro en un circuito con carga

a. Desconexión del neutro en un sistema monofásico

En una instalación eléctrica típica, el cable de neutro lleva la corriente de retorno desde las cargas eléctricas a la fuente.

En el sistema de la Fig. 1(A), la cantidad de voltaje que llega a ambas resistencias es de 120 [V] sin importar si el sistema es balanceado o no (en un sistema balanceado ambas cargas son iguales), ya que el cable de neutro lleva la corriente de desbalance que existe entre las dos fases de regreso a la fuente.

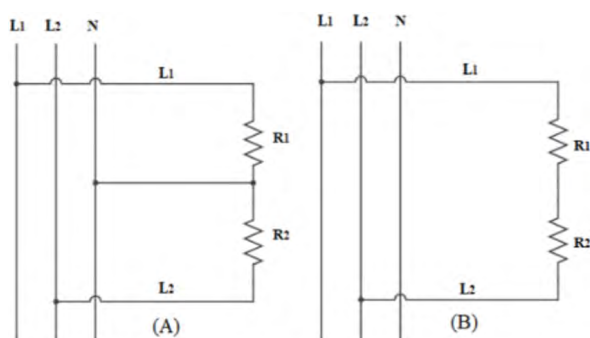


Fig. 1. Sistema 1φ 240/120V a tres hilos (Fuente: elaboración propia).

Cuando se desconecta el neutro (Fig. 1(B)), quedan en serie las fuentes de alimentación y las

resistencias, por lo que el voltaje final será la suma de los voltajes parciales para las dos resistencias $R_1 R_2$. Aquí se tendrá una nueva intensidad que será la misma para las dos resistencias. Mientras el sistema esté equilibrado, el voltaje será el mismo para las dos resistencias, pero si existe desequilibrio la situación se pondrá muy peligrosa para la resistencia menor, es decir, la que mayor carga va a soportar, porque podría llegar a quemarse.

b. Desconexión del neutro en un sistema trifásico

Un sistema trifásico (Fig. 2) se considera equilibrado cuando las cargas de las tres fases son iguales ($Z_1 = Z_2 = Z_3$), por lo tanto, no circula corriente por el neutro ya que las corrientes de las fases son iguales en magnitud ($|I_a| = |I_b| = |I_c|$) y el voltaje en las tres fases es el mismo, incluso cuando se desconecta el neutro.

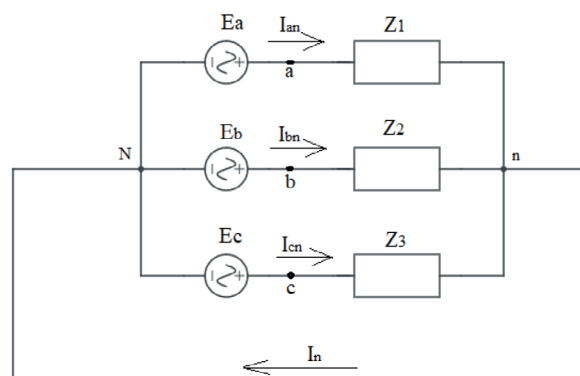


Fig. 2. Sistema trifásico (Fuente: Elaboración propia).

Cuando el sistema se desequilibra, es decir las cargas son distintas, comienza a circular corriente por el neutro, ya que las magnitudes de las tres corrientes de fase son diferentes. Cuando se desconecta el neutro los voltajes en las cargas serán distintos por lo que se toma el principio de que, a mayor impedancia mayor caída de tensión.

Pérdidas económicas debidas a instalaciones eléctricas deficientes

Incendios. - En Ecuador la principal causa de incendios estructurales son las fallas eléctricas, como: cortocircuitos, líneas recargadas por exceso de aparatos eléctricos conectados y el mal mantenimiento de las instalaciones eléctricas [1]

La mayor parte de los incendios en viviendas se registra en barrios urbano-marginales donde el factor socio-económico juega un factor importante a la hora de construir, es decir, las personas prefieren comprar materiales más económicos y realizar las conexiones de manera informal, sin contar con la ayuda de un profesional calificado.

Aumento de facturación. - Las instalaciones eléctricas deficientes pueden provocar un aumento en el consumo de energía eléctrica debido a pérdidas por resistencia, fugas de corriente, el uso de equipos ineficientes y el uso excesivo de extensiones y adaptadores. Estos problemas pueden resultar en una disipación de energía inútil, pérdidas constantes de electricidad y un consumo excesivo por parte de los equipos. Según [2] el aumento en el consumo de energía eléctrica podría rondar el 40%.

Daños en equipos. - Las malas instalaciones eléctricas pueden resultar en un suministro eléctrico inestable, picos de voltaje, caídas de energía y problemas de interferencia electromagnética. Como resultado, los equipos eléctricos y electrónicos pueden sufrir daños. Además de los costos de reparación o reemplazo de los equipos, los daños causados por malas instalaciones eléctricas pueden interrumpir las operaciones comerciales, generar pérdidas financieras y comprometer la seguridad de las personas.

B. SEGUNDA PARTE: SEGURIDAD ELÉCTRICA

Efectos de la corriente al atravesar el cuerpo humano

Los impactos causados por las descargas eléctricas pueden tener graves consecuencias en el cuerpo humano, como traumatismos, quemaduras de tercer grado, metalización de la piel, daños mecánicos y electro-oftalmia, entre otros. Además de la corriente eléctrica, también existen otros factores a tener en cuenta, como el arco eléctrico, el campo electromagnético y el campo electrostático.

Para combatir estos peligros, es necesario tomar medidas de seguridad y utilizar equipos de protección personal. A diferencia de otros peligros visibles, como caídas o incendios, la electricidad no puede ser fácilmente identificada hasta que ya es demasiado tarde y la persona ha sufrido una descarga. Por lo tanto, es necesario contar con instrumentos de medición que puedan cuantificar el voltaje con el que estamos trabajando.

Para determinar las medidas de seguridad adecuadas, es importante comprender cómo actúa la corriente eléctrica en nuestro cuerpo, cuál es la corriente máxima permitida en función del voltaje y la resistencia de cada persona, el tipo de corriente, la frecuencia y otros parámetros.

Cuando la corriente circula por nuestro cuerpo, se producen efectos termo-biológicos, como las quemaduras eléctricas, que pueden ocurrir cuando una corriente de considerable magnitud atraviesa el cuerpo humano. Es importante destacar que existen diferentes tipos de impactos eléctricos y traumatismos, que pueden ser locales o generalizados, llegando incluso a ser mortales. El daño causado por la corriente eléctrica depende del valor y la duración de la exposición. Las quemaduras causadas por la electricidad coagulan las proteínas, lo que resulta en quemaduras profundas en los tejidos del cuerpo, que son muy dolorosas y requieren una larga curación o incluso pueden causar discapacidad.

En altas tensiones, el choque eléctrico puede ocurrir sin necesidad de un contacto directo, basta con acercarse a una distancia peligrosa. En primer lugar, se produce una chispa que genera un arco voltaico con temperaturas superiores a los 1000°C.

En instalaciones con un voltaje de hasta 1000V, el contacto con partes energizadas a una distancia mayor puede provocar la metalización de la piel, que es la penetración de fragmentos de metal debajo de la piel. La electro-oftalmia se produce debido a la radiación ultravioleta del arco eléctrico, lo que causa daños graves en los ojos.

Las personas tienen diferentes valores de resistencia, que dependen de varios factores,

especialmente físicos, así como del estado nervioso, la salud y el cansancio, entre otros. Sin embargo, el tiempo de exposición es fundamental, ya que, a menor tiempo de exposición, menor es el peligro. Por lo general, una persona tiene dificultades para soltarse del punto de contacto, por lo que es necesario desconectarla antes de que se vea afectada la respiración y el ritmo cardíaco, esto tiene su razón de ser debido a que, durante el ciclo cardíaco, existen diferentes fases en las que el corazón es más o menos susceptible a la corriente eléctrica. [9]

Una de las fases críticas es la llamada fase T, que se refiere a un intervalo específico del ciclo cardíaco. En la mayoría de los casos, la fase T ocurre aproximadamente entre los 0,15 y 0,25 segundos después de la estimulación eléctrica previa (latido anterior). Durante esta fase, el músculo cardíaco se encuentra en un estado vulnerable y es más sensible a las perturbaciones eléctricas externas [9].

Si una corriente eléctrica pasa a través del cuerpo y no coincide con la fase T, es menos probable que cause fibrilación ventricular o detención del corazón. Por lo tanto, cuanto menor sea el tiempo de exposición a la corriente eléctrica, menor será la probabilidad de que coincida con la fase T y cause estos efectos adversos [9].

Recorrido de la corriente a través del cuerpo

El paso de corriente a través de los músculos respiratorios y del corazón se considera altamente peligroso debido a su impacto directo en las funciones vitales del cuerpo.

Sin embargo, en casos de descargas eléctricas, la corriente puede seguir diferentes trayectorias a lo largo del cuerpo humano, dependiendo de los puntos de entrada y salida, la afectación puede variar.

A continuación se presentan algunas trayectorias comunes de la corriente eléctrica durante una descarga eléctrica junto con el porcentaje aproximado de la corriente total que circula a través del corazón para cada trayectoria [9]

1. *Trayectoria de brazo a brazo:* La corriente entra por un brazo y sale por el otro, aproximadamente el 3,3% de la corriente total, atraviesa el corazón. Esta trayectoria está presente en alrededor del 10% de los accidentes eléctricos.
2. *Trayectoria de brazo izquierdo a piernas:* En esta trayectoria, la corriente entra por el brazo izquierdo y sale por las piernas, aproximadamente un 3,7% de la corriente total atraviesa el corazón. Esta trayectoria se observa en cerca del 5% de los accidentes eléctricos.
3. *Trayectoria de pierna a pierna:* Aquí, la corriente entra por una pierna y sale por la otra, a través del corazón pasa aproximadamente un 0,4% de la corriente total. Esta trayectoria está presente en alrededor del 20% de los accidentes eléctricos.
4. *Trayectoria de brazo derecho a piernas:* La corriente ingresa por el brazo derecho y sale por las piernas, a través del corazón pasa aproximadamente un 6,7% de la corriente total. Esta trayectoria se encuentra en cerca del 15% de los accidentes eléctricos.
5. *Trayectoria de cabeza a piernas:* En esta trayectoria, la corriente entra por la cabeza y sale por las piernas, aproximadamente un 6,8% de la corriente total, atraviesa el corazón. Esta trayectoria se encuentra en aproximadamente el 25% de los accidentes eléctricos.
6. *Trayectoria de cabeza a brazos:* En esta trayectoria, la corriente ingresa por la cabeza y sale por los brazos, a través del corazón pasa aproximadamente un 7% de la corriente total. Cerca del 25% de los accidentes eléctricos tienen esta trayectoria.

La pérdida de la capacidad de trabajar por tres días o más sucede cuando la corriente tiene una de las siguientes trayectorias: Brazo – brazo en el 83 % de los casos, brazo izquierdo – piernas 87 % de los casos y brazo derecho – piernas 80 % de los casos [9]

Género y frecuencia de la corriente

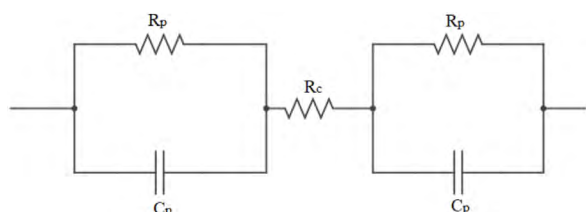


Fig. 3. Esquema de sustitución de la impedancia del cuerpo humano. *RP:* resistencia de la piel; *RC:* resistencia interna del cuerpo; *CP:* capacitancia de la piel (Fuente: Elaboración propia)

El cuerpo humano se comporta como una impedancia compuesta por resistencias y capacitancias, en primer lugar, se realizará un análisis de las resistencias. La primera resistencia

R_p , es la resistencia de contacto con el primer punto de contacto y la segunda resistencia R_p es el contacto final, aquí es donde radica la máxima resistencia del cuerpo, luego está la resistencia interna del cuerpo R_c que es la que menos resistencia tiene.

Analizando el esquema de la Fig. 4, se tiene dos resistencias en paralelo con las capacitancias y en serie con la resistencia interna del cuerpo. Cuando se tiene corriente continua, la intensidad no circula por los capacitores, por lo que quedan tres resistencias en serie, es decir la máxima resistencia que puede tener el cuerpo humano, como conclusión, la corriente continua es la menos peligrosa, al contrario cuando se tiene corriente de alta frecuencia, por ejemplo aquellas producidas por los rayos atmosféricos será la más peligrosa, ya que la X_c (reactancia capacitiva tenderá a cero, por cuanto es inversamente proporcional a la frecuencia) y la resistencia equivalente del cuerpo bajará considerablemente.

La resistencia de la piel varía en función del grado de humedad, grosor, suciedad y la presencia de afecciones o heridas, además de depender de la densidad de contacto, es decir, del área. Como factores externos, el peligro radica en la intensidad de la corriente, la cual está directamente relacionada con el voltaje y de forma inversamente proporcional a la resistencia del cuerpo (según la ley de Ohm), así como con el tiempo de exposición a dicha corriente (según la ley de Joule). En algunos

textos se menciona la corriente admisible, la cual es aquella corriente hasta la cual una persona puede soltarse sin riesgo real.

A continuación, un resumen de los efectos de la corriente eléctrica en el organismo según la intensidad.

Tabla IV

EFFECTOS DE LA CORRIENTE ALTERNA EN EL ORGANISMO

Efectos de la corriente alterna en el organismo	
Intensidad [mA]	Efectos de la corriente alterna en el organismo (50-60 Hz)
0.5 – 1.5	Umbral sensorial, ligero temblor en los dedos de la mano
2.0 – 3.0	Temblor fuerte de los dedos de la mano, la sensación llega a la muñeca
5.0 – 7.0	Calambres y dolor en las manos
8.0 – 10	Dificultad para soltarse (aunque es posible), dolor en dedos y antebrazo
20 – 25	Parálisis en las manos, soltarse es imposible, dificultad para respirar
50 - 80	Se detiene la respiración comienzo de la fibrilación del corazón
90 y más	Si tiene una duración mayor a 3 segundos se detiene el corazón

Accidentes eléctricos

El paso de la corriente eléctrica a través del cuerpo humano se da por el contacto con algún conductor o un elemento que está en tensión, el contacto puede ser directo si la persona interactúa con alguna parte activa de la instalación eléctrica o indirecto cuando interactúa con algún elemento que no debería estar energizado, pero lo está, por accidente.

Accidentes eléctricos por contacto indirecto

Para una persona que está de pie en el suelo y está tocando una carcasa conectada a tierra (Fig. 4), el voltaje de contacto se puede determinar de la siguiente manera [9]:

$$U_{pm} = \varphi P + \varphi m \tag{2}$$

Dónde: φP = potencial de la pierna φm = potencial de la mano

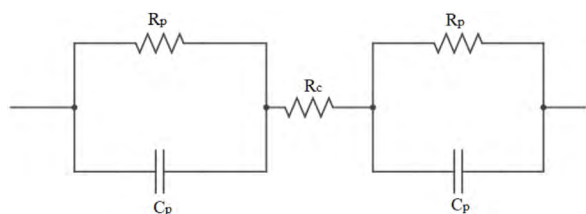


Fig. 4. Cambio en el voltaje de contacto (Fuente: Elaboración propia)

Dado que la persona toca la carcasa, el potencial de la mano ϕ_m es el potencial de la carcasa, o lo que es lo mismo el voltaje con respecto a tierra [9]:

$$\phi_m = U_e = \frac{I_{fp}}{2\pi X_p} \tag{3}$$

Donde: I_f = corriente de falla a tierra, ρ = resistencia específica del electrodo, X_e = distancia desde el centro del electrodo a tierra hasta el punto donde se encuentran las manos, X_e = Potencial respecto a la puesta a tierra.

Si las piernas de una persona están, por ejemplo, en el punto A, el potencial de las piernas ϕ_p , se obtiene de la Ec.3:

$$\phi_p = \phi_A = \frac{I_{fp}}{2\pi X_A} \tag{4}$$

Donde: ϕ_p = Potencial pierna, X_A = ubicación de la persona.

Para obtener las tensiones de contacto, es necesario obtener la tensión relativa correspondiente al desplazamiento que existe entre el electrodo de puesta a tierra y la ubicación de la persona en contacto con la carcasa, para la persona que está parada justo sobre el seccionador (Fig. 4(1)) la tensión de contacto es igual a cero, a medida que nos alejamos de la puesta a tierra la tensión de contacto va en aumento y llegado al último punto marcado con (3) en la Fig. 4, el potencial de contacto es igual al potencial relativo a la puesta a tierra [9]:

$$\phi_p/m = \phi_p = \frac{I_e \rho}{2\pi X_p} \tag{5}$$

Donde: ϕ_p/m = Potencial pierna/brazo, X_p = ubicación de la persona, tenemos también que: $\phi_p = \phi_m$

Para la persona parada sobre el electrodo de puesta a tierra y en contacto con la carcasa el voltaje del brazo y la carcasa es el mismo que el voltaje relativo a la puesta a tierra. A medida que aumenta la distancia desde el electrodo de puesta a tierra, el voltaje de contacto aumenta y en el último punto (Fig. 4(3)) es igual al voltaje relativo al suelo, porque una persona está parada en el suelo y el potencial de sus piernas ϕ_p es igual a cero, es decir:

$$U_{pm} = U_e - 0 \tag{6}$$

Sí en la Ec.3 se sustituye el valor del potencial de brazos y piernas ϕ_p y ϕ_m , obtenemos el voltaje de contacto:

$$U_{pm} = \frac{I_e \rho}{2\pi} \left\{ \frac{1}{X_e} - \frac{1}{X_p} \right\} \tag{7}$$

En esta expresión, el primer factor es el voltaje de la carcasa con respecto a la tierra U_e , el segundo factor se denota como:

$$\alpha_1 = \frac{X_p - X_e}{X_p} \tag{8}$$

Sustituyendo estos valores en (7), se obtiene el voltaje de contacto en el campo de expansión de un electrodo a tierra de cualquier configuración:

$$U_{pm} = U_e \alpha \tag{9}$$

Así, en el caso general, el voltaje de contacto es en parte la tensión relativa al suelo, ya que $\alpha_1 \leq 1$. El valor α_1 se llama factor de voltaje de contacto. Las expresiones (8) y (9) permiten calcular la tensión de contacto sin tener en cuenta resistencias adicionales en el circuito humano como por ejemplo la resistencia del calzado, o la resistencia de la superficie de apoyo de las piernas al paso de la corriente [9].

Accidentes eléctricos debidos a descargas atmosféricas.

¿Cómo se produce un relámpago?

Un relámpago se produce por la electrificación de las nubes durante una tormenta eléctrica. El proceso comienza cuando hay una separación de

cargas eléctricas dentro de una nube (Fig. 5), con cargas positivas acumulándose en la parte superior y cargas negativas en la parte inferior. Esta separación de cargas crea un campo eléctrico intenso entre la nube y la tierra. A medida que el campo eléctrico se vuelve lo suficientemente fuerte, puede ionizar el aire circundante y formar un conducto de plasma, conocido como canal líder, que permite que la corriente eléctrica fluya entre la nube y la tierra. Esta descarga eléctrica, visible como un relámpago, sigue el camino del canal líder y se produce rápidamente en forma de pulsos o "ramas". El relámpago puede viajar en zigzag o en línea recta, y se calienta a una temperatura extremadamente alta, generando un brillo intenso y liberando energía en forma de luz y calor. El sonido del trueno se produce debido al rápido calentamiento y enfriamiento del aire a medida que la corriente eléctrica pasa a través de él, creando una onda de choque que se propaga como sonido [6].

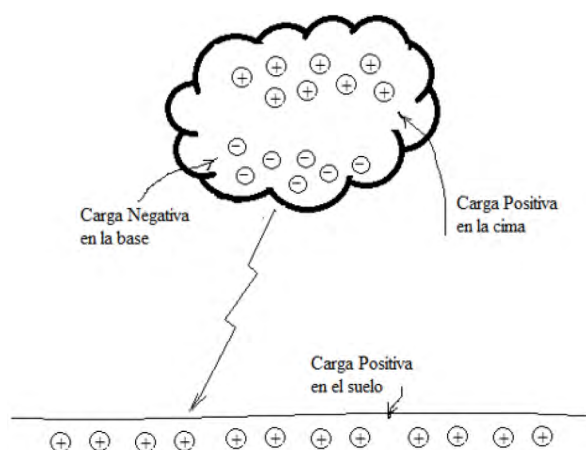


Fig. 5. Formación de un rayo (Fuente: elaboración propia)

¿Qué es un pararrayos?

Un pararrayos es un dispositivo instalado en edificios o estructuras para captar los impactos directos de los rayos y redirigir de manera segura su descarga hacia el suelo, evitando así que afecten zonas no deseadas o a las personas.

Para cumplir esta función, una instalación de pararrayos consta principalmente de tres elementos:

- Elemento de captación o punta.
- Un cuerpo metálico.
- Una red conductora que se conecta a un sistema de toma de tierra de baja impedancia, donde se

disipa la descarga del rayo.

Tipos de pararrayos: Los tipos de pararrayos más comunes son:

1. **Pararrayos de Franklin:** También conocido como pararrayos de punta, es uno de los tipos más antiguos y ampliamente utilizados en todo el mundo. Consiste en una punta metálica que se instala en la parte superior de los edificios u otras estructuras, y está conectada a un sistema de puesta a tierra. Cuando se produce una descarga atmosférica, el pararrayos de Franklin canaliza la corriente hacia la tierra de manera segura.
2. **Pararrayos de ionización:** Este tipo de pararrayos se basa en la liberación controlada de iones en el aire para crear un camino conductor que atraiga los rayos. Estos pararrayos utilizan una corona o una serie de electrodos para ionizar el aire y formar un camino de baja resistencia para la descarga eléctrica.
3. **Pararrayos PDC (Pararrayos de Cebado Diferencial Controlado):** Estos pararrayos generan un canal líder ascendente, o líder piloto, mediante la ionización del aire y la generación de un impulso eléctrico de alta frecuencia o tensión. Este canal líder atrae y captura el rayo hacia el pararrayos, proporcionando una ruta preferencial para que la descarga eléctrica fluya hacia la tierra.

La norma americana **NFPA 780** sugiere la instalación de pararrayos en función del índice de riesgo de la instalación a proteger, incluyendo casos como [7]:

- Áreas con una alta frecuencia anual de rayos por kilómetro cuadrado.
- Edificios donde se manejen sustancias tóxicas, radioactivas, altamente inflamables o explosivas, así como aquellos que alberguen equipos o documentos especialmente vulnerables o valiosos.
- Edificios o áreas abiertas con afluencia de público, construcciones de gran altura y en general, construcciones en terrenos elevados.

Aunque no es obligatorio instalar un pararrayos en casos que no se mencionan anteriormente, se recomienda hacerlo para protegerse contra sobretensiones. Con la instalación adecuada de un

pararrayos, se garantiza la seguridad de las personas y los dispositivos electrónicos en una vivienda.

PD: La norma **NEC2011** deja a discreción del ingeniero de obra determinar la necesidad de un pararrayos, como no existe una norma específica establecida por las autoridades, los sistemas de pararrayos suelen regirse por normas internacionales reconocidas, como la norma **IEC 62305** (Protección contra el rayo), que establece los principios y directrices para el diseño, instalación, inspección, mantenimiento y pruebas de sistemas de protección contra el rayo.

Peligros a los que se expone una persona cuando se produce una descarga atmosférica en una torre equipada con un pararrayos: En primer lugar, es importante tener en cuenta que el pararrayos tiene la función de proteger, actuando como un cono o un paraguas, brindando protección contra el impacto directo del rayo. Sin embargo, dentro de la zona de protección pueden existir otros riesgos, como la tensión de contacto y la tensión de paso. También se debe mencionar la tensión de transferencia, que es un caso especial de la tensión de contacto [6].

La tensión de contacto (U_c , Fig. 6) se refiere a la tensión que puede generarse en objetos conductores dentro de la zona de protección del pararrayos. Cuando un rayo es captado por el pararrayos, la corriente puede fluir a través de los conductores cercanos, creando un potencial eléctrico peligroso en esos objetos. Si una persona o equipo entra en contacto con esos conductores, puede estar expuesta a un riesgo de electrocución o descarga eléctrica [6].

La tensión de paso (U_p , Fig. 6) se refiere a la tensión que se genera en el suelo dentro de la zona de protección del pararrayos. Cuando un rayo impacta en la tierra, se generan ondas de potencial eléctrico similares a las ondas que se forman cuando lanzamos una piedra en un lago. Cada onda tiene un potencial eléctrico y la diferencia entre estos potenciales determinará el valor del voltaje al que estaremos expuestos al tener contacto. Es importante destacar que el potencial cero será el más alto y a medida que nos acerquemos a las ondas más alejadas, el voltaje será mayor [6].

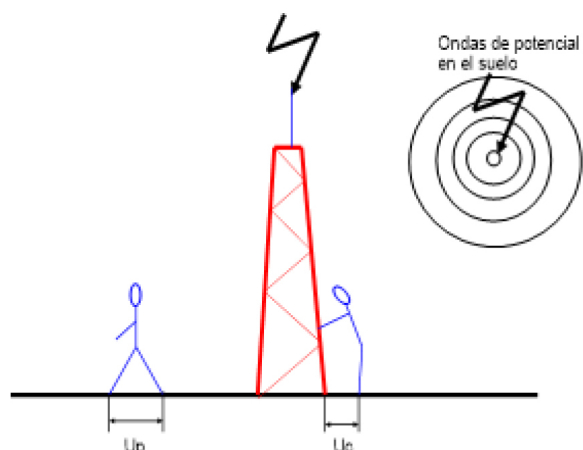


Fig. 6. Posibles circulaciones de los electrones (Fuente: Elaboración propia)

En la Fig. 6, la tensión de contacto U_c , será la diferencia entre la estructura que está tocando con las manos y la onda que tocan los pies, en cambio la tensión de paso U_p será la Diferencia de los voltajes de la onda que toque un pie con la onda que toque su segundo pie [6].

El voltaje de transferencia se produce cuando hay una diferencia de potencial entre dos puntos dentro de la zona de protección del pararrayos, lo que puede provocar una descarga eléctrica si una persona o equipo se encuentra en contacto con ambos puntos [6].

» III. Desarrollo

Este estudio se basa en un enfoque que es en gran parte empírico, fundamentado en el trabajo de campo, el recorrido de obras y entrevistas con personal a cargo de los trabajos eléctricos "in situ".

A. PRIMERA PARTE:

Ejemplos simplificados de problemas que se generan debido a las instalaciones eléctricas deficientes, y posibles soluciones

Conexión o puesta a tierra

Por ejemplo, en una lavadora con carcasa metálica, la corriente del cable puede desviarse a través de la carcasa, lo que implica que la carcasa se carga eléctricamente. Si alguien toca la carcasa, proporciona a la corriente el camino más directo y de

menor resistencia para desviarse, resultando en una descarga eléctrica a través de la persona. En la Fig. 7, se puede apreciar el esquema de una conexión a tierra típica, que ayuda a evitar este tipo de inconvenientes.

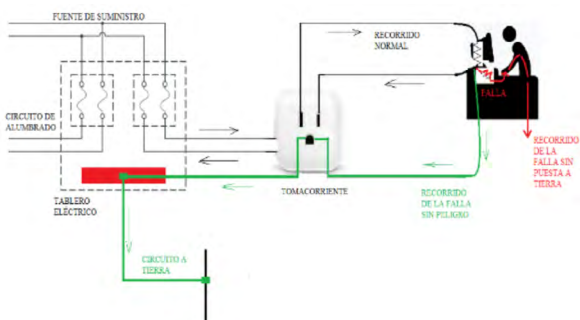


Fig. 7. Función del circuito de puesta a tierra (Fuente: Elaboración propia)

a. Desconexión del neutro en un sistema monofásico

Esto sucedió en un edificio de la ciudad de Riobamba, muchos aparatos eléctricos se dañaron, la respuesta del electricista fue que el daño se produjo porque no había la varilla de puesta a tierra, pero en realidad la falla sucedió por la desconexión del neutro (por un ratito), lo cual vamos a explicar a continuación

Ejemplo sencillo con dos aparatos eléctricos (Datos en Tabla V):

Tabla V
DATOS DE LOS APARATOS ELÉCTRICOS

Calentador	Computador (PC)
$P_C = 1500 [W]$	$P_{PC} = 100 [W]$
$V_C = 120 [V]$	$V_{PC} = 120 [V]$
$R_C = 9,6 [\Omega]$	$R_{PC} = 144 [\Omega]$

1. Intensidades con el neutro

$$I_C = \frac{V_C}{R_C} = \frac{120}{9,6} = 12.5 [A]$$

$$I_{PC} = \frac{V_{PC}}{R_{PC}} = \frac{120}{144} = 0.833 [A]$$

Intensidad desconectando el neutro.

$$I_T = \frac{V_T}{R_T} = \frac{V_C + V_{PC}}{R_C + R_{PC}} = \frac{120 + 120}{9,6 + 144} = 1.56 [A]$$

2. Caídas de tensión en cada resistencia.

$$V_C = \frac{(V_T \times R_C)}{(R_C + R_{PC})} = \frac{240 \times 9,6}{153,6} = 15 [V]$$

$$V_{PC} = \frac{(V_T \times R_{PC})}{(R_C + R_{PC})} = \frac{240 \times 144}{153,6} = 225 [V]$$

A simple vista es sencillo notar que la PC se quema si ocurre una desconexión del neutro, el calentador en cambio, ni siquiera funciona.

b. Desconexión del neutro en un sistema trifásico

También sucedió en la construcción de un edificio, cuando se llegó a la obra indicaron que se dañó el radio de la señora que administraba los baños. El recorrido de la obra mostró cables "pelados" de las soldadoras por el piso, con lo que el sistema estaba completamente desequilibrado, volviendo al tablero principal se indicó al arquitecto, que seguramente el maestro electricista quitó un "ratito" este cable, en referencia al neutro, el arquitecto contestó que eso era justamente lo que sucedió. A continuación, se explica el por qué.

Por el teorema de Millman, se puede determinar cuál sería el voltaje en cada uno de los elementos del circuito de la Fig. 8:

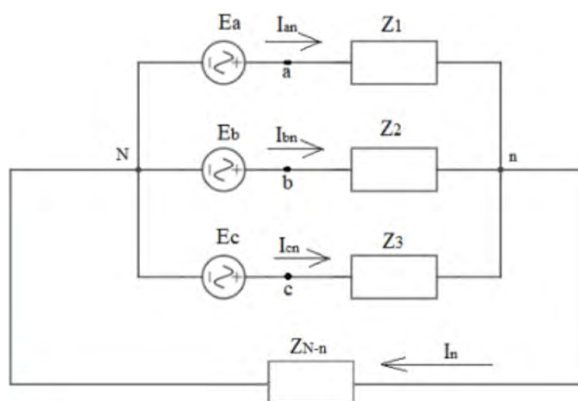


Fig. 8. Sistema Trifásico (Fuente: Elaboración propia)

$$U_{N-n} = \frac{E_A \cdot Y_A + E_B \cdot Y_B + E_C \cdot Y_C}{Y_A + Y_B + Y_C + Y_n} \quad (10)$$

Donde: U_{N-n} = Diferencia de potencial entre el neutro de las fuentes (N) y de las fases (n), E_A, E_B, E_C = Fuerzas electromotrices de las fases A, B y C,

$Y_A + Y_B + Y_C + Y_n =$ Admitancias de las cargas A, B, C y del neutro.

Se tiene también que: $Y = \frac{1}{Z}$ es decir la admitancia es el inverso de la impedancia. Para encontrar las intensidades se emplea las siguientes fórmulas:

$$I_A = (E_A - U_{N-n}) \times Y_A \tag{11}$$

$$I_B = (E_B - U_{N-n}) \times Y_B \tag{12}$$

$$I_C = (E_C - U_{N-n}) \times Y_C \tag{13}$$

Partiendo de las a ecuaciones anteriores se puede analizar los siguientes casos de la conexión de la Fig. 8.

1. En un sistema equilibrado, el voltaje entre neutros U_{N-n} , será cero, con o sin el neutro.
2. En el momento que el sistema se desequilibra el voltaje U_{N-n} , será cero si el conductor entre los neutros se lo considera de resistencia nula ($Z_{N-n} = 0$), pero sí se desconecta, la resistencia del neutro será infinita ($Z_{N-n} = \infty$).

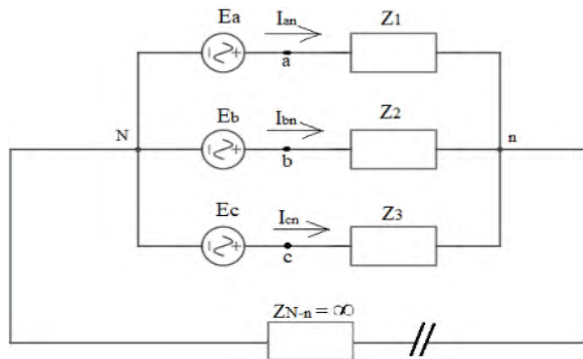


Fig. 9. Sistema trifásico. (Fuente: Elaboración propia)

Para la Fig. 9, el neutro se desconecta $Z_{N-n} = \infty$ y $Y_N = 0$, por lo que aparece U_{N-n} distinto de cero, por lo tanto, los voltajes en las cargas serán tan distintas como el desequilibrio del sistema. La caída de tensión en cada uno de los utilizadores será:

$$U_A = I_A \times Z_A \tag{14}$$

$$U_B = I_B \times Z_B \tag{15}$$

$$U_C = I_C \times Z_C \tag{16}$$

Lo que sucedió en el edificio es que los cables "pelados" que hacían contacto con el piso de

cemento y que servían para las soldadoras tenían una impedancia muy pequeña comparada con la del radio de la señora que atendía el pequeño bar, por lo tanto, cuando se desconectó el neutro, el voltaje que llegó al radio fue extremadamente superior a su valor nominal, por lo que se produjo la quema del aparato.

B. SEGUNDA PARTE: SEGURIDAD ELÉCTRICA

Medidas de prevención contra contactos eléctricos indirectos: Los contactos eléctricos indirectos se producen cuando hay un fallo en un dispositivo, este fallo hace que la corriente eléctrica se desvíe a través de las partes metálicas de los dispositivos, lo que puede ocasionar que las personas que entren en contacto con elementos que no forman parte del circuito eléctrico (que normalmente no deberían estar bajo tensión), reciban una descarga eléctrica [12].

Las medidas de protección contra contactos indirectos incluidos en la norma **NEC2011**, son:

1. **Puesta a tierra de las masas:** Se trata de conectar las partes metálicas de la instalación eléctrica (carcasas de máquinas, herramientas, etc.) a tierra.
2. **Uso de tensiones de seguridad de 24V:**

¿Cómo se obtiene la tensión de seguridad de 24 V? Como ya se ha mencionado con anterioridad la resistencia del cuerpo humano depende de muchos factores como: dureza de la piel, superficie de contacto, grado de la humedad en la piel, edad, sexo, textura física y estado fisiológico general, por ejemplo, grado de alcohol en la sangre o cansancio.

Si se toma en cuenta estos factores, cada persona presenta diferentes valores de resistencia eléctrica al paso de la corriente. Sin embargo, existe un consenso general según el cual, el cuerpo humano responde de manera distinta en entornos húmedos y secos. En el primer caso, se considera que la resistencia del cuerpo humano es de aproximadamente

800 [Ω], mientras que en el segundo caso esta resistencia aumenta a unos 1600 [Ω]. [14]

A partir de estos datos y considerando que una corriente de 30 [mA] durante 1 segundo no produce efectos irreversibles, surge el concepto de “*Tensión de seguridad*”. Esta tensión es aquella que, aplicada al cuerpo humano, no genera una circulación de corriente que represente un riesgo para el individuo. Las tensiones de seguridad resultantes son las siguientes [14]:

- En entornos húmedos: $800 \text{ [}\Omega\text{]} \times 0.03 \text{ [A]} = 24 \text{ [V]}$.
- En entornos secos: $1600 \text{ [}\Omega\text{]} \times 0.03 \text{ [A]} = 48 \text{ [V]}$.

¿En qué consiste el uso de tensiones de seguridad?

El objetivo de utilizar tensiones de seguridad es reducir el riesgo de daño eléctrico en caso de contacto con personas. Se aplica en herramientas eléctricas, juguetes motorizados, aparatos para el cuidado del cabello y la piel, entre otros.

3. **Separación de circuitos:** Consiste en mantener separados los circuitos de uso de la fuente de energía mediante el uso de transformadores con aislamiento de tierra, donde todos los conductores del circuito de uso, incluyendo el neutro, permanecen aislados de la tierra.
4. **Doble aislamiento:** Se basa en el uso de materiales que disponen de aislamiento de protección o aislamiento reforzado entre las partes activas y las masas accesibles. Este tipo de aislamiento adicional proporciona una capa de protección adicional contra los contactos indirectos.

Explicación básica sobre los peligros a los que se expone una persona cuando toca una torre equipada con un pararrayos y las zonas no han sido debidamente protegidas

¿Cómo protege un pararrayos?

El diseño de un pararrayos incluye una configuración cónica que crea un volumen protector en forma de cono alrededor del pararrayos. El ángulo (α) en la parte superior del cono se conoce como ángulo de protección. El concepto del cono de protección se utiliza para ubicar pararrayos en un edificio o en una torre, como se ilustra en la Fig. 10 (B). Es importante destacar que cuanto menor sea el ángulo de protección asumido en el análisis, menor será la separación entre los pararrayos adyacentes ubicados en una estructura (y más confiable será la protección). Los ángulos de protección más utilizados son 30° y 45° [6].

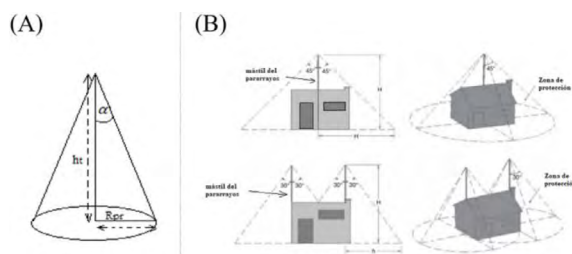


Fig. 10. (A) Cono de protección, (B) Zonas de protección que abarca el cono (Fuente: [6]).

La proximidad de los conductores de bajada de un pararrayos puede ser peligrosa para la vida incluso si el sistema de protección ha sido diseñado y construido de acuerdo a la norma IEC 62305. Por eso es necesario minimizar la presencia de las personas cerca de la estructura y aumentar la resistividad de la capa superficial del suelo con algún tipo de material aislante [6].

Conexión correcta de un interruptor: La conexión correcta, no solo debe de ser funcional, es decir, que cumpla la función de encender y apagar el interruptor, sino también de proteger a la persona cuando tenga que operar en el circuito, por ejemplo, al cambiar el foco, la boquilla no debe de estar energizada o la cuchilla de la palanca del disyuntor no debe de tener diferencia de potencial con respecto a la tierra.

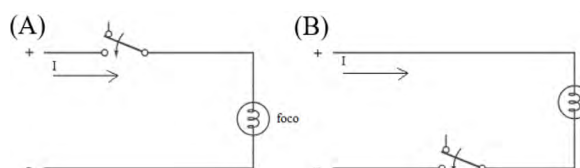


Fig. 11. Conexión correcta de un interruptor, (B) Conexión incorrecta de un interruptor (Fuente: Elaboración propia)

En la Fig. 11 (A), se puede ver que todo el circuito, desde el signo menos hasta la cuchilla de la palanca, tiene el mismo potencial, es decir, cero de diferencia de potencial con respecto a la masa. Fig. 11 (B), se puede ver que todo el circuito, desde el signo más hasta la cuchilla de la palanca, tiene el mismo potencial nominal, es decir, la diferencia de potencial con respecto a la masa es total, todo el circuito está energizado. Si se aplica a la corriente alterna, el negativo sería el neutro y el positivo la fase. En este caso el peligro es eminente, la boquilla está energizada por lo que es peligroso cambiar el foco, especialmente cuando se hace mantenimiento en túneles o coliseos, el accidente se produce no tanto por el choque eléctrico a la persona, sino porque puede perder el equilibrio y caer. La cuchilla de las palancas de conexión de una ducha, al estar energizada, es peligrosa, especialmente cuando la persona se está bañando. En los sistemas de distribución o subestaciones no pueden estar energizados los seccionadores de corte o fusibles.

» IV. Resultados y discusión

Desconexión del neutro en una instalación eléctrica ¿La varilla de puesta a tierra evitará este problema?

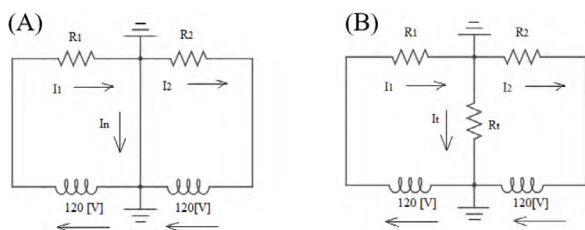


Fig. 12. (A) Esquema de un circuito con puesta a tierra y el neutro conectado, (B) Esquema de un circuito con puesta a tierra y el neutro desconectado (Fuente: Elaboración propia)

En el esquema de la Fig. 12(A), se tiene una varilla de puesta a tierra tanto en el transformador como en los usuarios del edificio. Si el neutro se desconecta, quedará solamente la resistencia de la puesta a tierra R_t , tal como en la Fig. 12(B), con un voltaje sumado de 240[V] para las dos resistencias, demostrando que el problema no se elimina.

La conexión a tierra de la carga y la conexión a tierra de la fuente crearán una trayectoria adicional en los circuitos existentes, pero esta

nueva trayectoria no puede reemplazar la función del neutro ni ofrecer la misma eficiencia de cierre del circuito [21], porque como indica la norma **NEC-SB-IE** “Es necesario que todos los circuitos de tomacorrientes y los circuitos de cargas especiales estén equipados con un conductor de tierra separado y distinto del conductor de neutro” [20].

Este escenario es especialmente común en las redes de distribución de baja tensión. Por lo tanto, se recomienda la instalación de un protector de sobretensiones para prevenir estos riesgos [3].

¿Qué es un protector de sobretensiones?

Un protector de sobretensiones, también conocido como supresor de sobretensiones, es un dispositivo diseñado para proteger los equipos eléctricos y electrónicos contra las sobretensiones en el suministro eléctrico.

El protector de sobretensiones funciona detectando las sobretensiones y desviando el exceso de energía hacia la tierra de manera segura. Cuando una sobretensión transitoria ocurre, el protector actúa como una vía de baja resistencia para que la corriente fluya hacia la tierra en lugar de afectar los equipos conectados. Esto ayuda a prevenir daños, averías o incluso la destrucción de los dispositivos.

Formas de protección para edificios: En los edificios multifamiliares, donde se tiene una cámara de transformación y su respectiva malla de tierra, el conductor de tierra debe de unirse al neutro en el tablero principal.

La opción recomendada para el Esquema de Conexión a Tierra (ECT) o Régimen de Neutro según la norma **NEC-SB-IE** es el TN-C-S (Fig.13). Esto implica que las Empresas Eléctricas deben poner a tierra el neutro del transformador, mientras que el usuario debe conectar todas las carcasas metálicas de sus equipos eléctricos al conductor de puesta a tierra, que en este caso es el conductor neutro cuando se trata del tablero de distribución principal. La letra "C" indica que las funciones de neutro y protección están combinadas en un solo conductor, mientras que la letra "S" significa que las funciones de neutro y protección se realizan con conductores separados. [20]

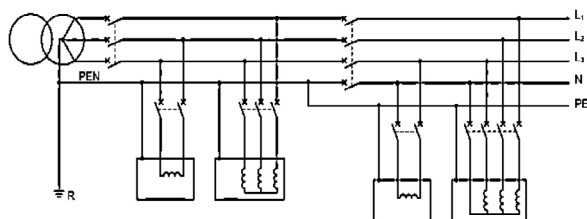


Fig. 13. Esquema de conexión a tierra TN-C-S (Fuente: Internet)

En el caso del esquema TN-C-S, la protección requerida incluye dispositivos contra sobrecorriente, así como interruptores o relés diferenciales. Estos dispositivos son necesarios cuando la corriente de falla no es lo suficientemente alta como para activar los dispositivos de protección por sobreintensidad. [22]

¿Qué es la protección por sobreintensidad?

La protección por sobreintensidad se puede lograr mediante el uso de dispositivos como fusibles, interruptores automáticos (disyuntores) y relés de sobrecorriente. Estos dispositivos están diseñados para interrumpir o limitar la corriente eléctrica cuando supera un valor predeterminado.

Existen tres tipos principales de protección por sobreintensidad:

- **Protección contra sobrecarga:** Se refiere a la protección contra corrientes excesivas prolongadas en un circuito. Los dispositivos de protección, como los fusibles térmicos o los disyuntores de sobrecarga, se activan cuando la corriente excede el límite seguro durante un período de tiempo prolongado.
- **Protección contra cortocircuitos:** Se utiliza para detectar y responder a corrientes eléctricas extremadamente altas que ocurren debido a una conexión directa entre conductores con baja resistencia. Los dispositivos de protección, como los fusibles de acción rápida o los disyuntores magnéticos, se activan instantáneamente para interrumpir la corriente en el circuito en caso de un cortocircuito.

- **Protección contra fallas a tierra:** Este tipo de protección se utiliza para detectar corrientes de fuga a tierra, que ocurren cuando hay un camino no intencionado hacia la tierra. Los dispositivos de protección, como los interruptores diferenciales o los relés de corriente residual (RCD), se activan cuando detectan una diferencia entre la corriente de entrada y la corriente de salida en un circuito, lo que indica una fuga a tierra.

¿Qué es la protección diferencial?

La protección diferencial es un tipo de medida de seguridad eléctrica que se utiliza para proteger a las personas y los equipos contra fugas de corriente y posibles descargas eléctricas. La protección diferencial se basa en el principio de que la corriente que ingresa a un equipo o circuito debe ser igual a la corriente que sale de él.

El dispositivo principal utilizado en la protección diferencial es el interruptor diferencial, también conocido como interruptor de falla a tierra o interruptor de circuito de fuga a tierra. Este dispositivo monitorea la corriente entrante y la corriente saliente de un circuito eléctrico o de un conjunto de equipos. Si existe una diferencia significativa entre la corriente de entrada y la corriente de salida, el interruptor diferencial se activa y desconecta el circuito eléctrico, lo que evita el riesgo de una descarga eléctrica.

Formas de protección para personal: Cuando se produce un contacto accidental entre partes no conductoras y tomas de tierra que están bajo voltaje en una instalación eléctrica, estas partes no conductoras normalmente no deberían estar energizadas. Sin embargo, en ocasiones, debido al deterioro del aislamiento, pueden estar energizadas o entrar en contacto eléctrico fortuitamente.

Si una fase entra en contacto con la carcasa de la instalación eléctrica, esto representa un peligro

potencial. Sin embargo, si la carcasa cuenta con una adecuada toma de tierra, el peligro se reduce dependiendo del tipo de toma de tierra que esté presente. En caso de que la carcasa no tenga una toma de tierra, toda la corriente fluirá a través del cuerpo humano si hay contacto, lo cual es extremadamente peligroso. Si la carcasa cuenta con una toma de tierra aislada del neutro, la corriente se dividirá, con la mayor parte pasando a través de la toma de tierra y una menor cantidad pasando a través del cuerpo humano.

Es importante destacar que estos escenarios representan un riesgo eléctrico significativo y deben ser abordados de manera adecuada. La implementación de un sistema de toma de tierra confiable, el mantenimiento regular de la instalación eléctrica y la realización de inspecciones periódicas son medidas fundamentales para prevenir y mitigar estos peligros. Además, es esencial seguir las normas y regulaciones eléctricas vigentes para garantizar la seguridad de las personas y las propiedades.

► V. Conclusiones

- Las conexiones eléctricas inadecuadas aumentan el riesgo de cortocircuitos, sobrecargas y sobrecalentamiento. Estos problemas pueden desencadenar chispas, arcos eléctricos y puntos de ignición que pueden resultar en incendios, lo que puede provocar pérdidas económicas, e incluso pérdidas de valiosas vidas humanas. Es por ello que es de vital importancia, contratar personal calificado para realizar las instalaciones eléctricas en las viviendas, y llevar a cabo mantenimientos periódicos de las redes eléctricas.
- La varilla de puesta a tierra no evitará los problemas que genera la desconexión del neutro en una instalación eléctrica, por ejemplo: se altera el equilibrio entre las fases y puede causar tensiones peligrosas en los equipos. La conexión a tierra proporciona una trayectoria adicional para la corriente en caso de fallas, pero no reemplaza la función del neutro ni garantiza la misma

eficiencia de cierre del circuito.

- Para proteger los equipos eléctricos y electrónicos contra las sobretensiones, se recomienda la instalación de protectores de sobretensiones. Estos dispositivos detectan las sobretensiones y desvían el exceso de energía hacia la tierra de manera segura, evitando daños en los dispositivos conectados.

► V. Referencias

- [1] El Telégrafo - Hay 80.000 hogares expuestos a incendios por cortocircuitos. (n.d.). Retrieved May 29, 2023, from <https://www.eltelegrafo.com.ec/noticias/guayaquil/1/hay-80000-hogares-expuestos-a-incendios-por-cortocircuitos>
- [2] SEMINARIO DE NORMATIVIDAD Y GESTIÓN PARA EDIFICACIONES SALUDABLES Y SOSTENIBLES Ministerio de Vivienda, Construcción y Saneamiento-DNC. (2010). <http://www.minem.gob.pe/>
- [3] Electricista24. (2017, 6 de enero). ¿Qué ocurre en una instalación eléctrica si se queda sin neutro? Recuperado de <https://electricista24.es/2017/01/06/que-ocurre-en-una-instalacion-electrica-si-se-queda-sin-neutro/>
- [4] Aguiar García, M. A. (2019, agosto). Falla en el neutro: Neutro cortado. Recuperado de <https://miguelangelaguilargarcia.blogspot.com/2019/08/falla-en-el-neutro-neutro-cortado.html>
- [5] Vásquez Villarruel, R. M., & Yépez Guevara, M. F. (2014). Estudio de fallas en instalaciones eléctricas domiciliarias y comerciales e implementación de un modelo didáctico para su corrección (Bachelor's thesis).
- [6] Cooray, Vernon., & Institution of Engineering and Technology. (2010). Lightning protection. 1036.
- [7] Sanders, M. K. (2011, May). NFPA 780 standard for the installation of lightning protection systems 2011 edition. In 2011 IEEE Industrial and Commercial Power Systems Technical Conference (pp. 1-4). IEEE.
- [8] Lujan Bravo, J. J. J. (2018). Análisis de

- los criterios de diseño basados en las recomendaciones de la NFPA 780 para el desarrollo de un sistema de protección contra descargas atmosféricas de una instalación eléctrica ubicada a la intemperie mediante pararrayos tipo Franklyn.
- [9] T. M. B. Knyazevsky, N. Chekalin, and N. Shipunov, *Protección laboral en instalaciones eléctricas*. Moscú: Energoatomizdat, 1983
- [10] Mullin, R. C., & Simmons, P. (2012). *Electrical Wiring Residential*. Cengage Learning.
- [11] AreaTecnológica.com.1999. “Puesta a Tierra”. Recuperado de https://www.areatecnologia.com/electricidad/puesta-a-tierra.html#La_Toma_de_Tierra_y_el_Diferencial
- [12] NEC Instalaciones Electromecánicas. (2011). Recuperado de http://www.fdseven.com/downloads/NEC_Inst_Electromec%C3%A1nicas_2013.pdf
- [13] Farina, A. L. (2015). *Riesgo eléctrico*. TECNIBOOK EDICIONES.
- [14] Universidad Politécnica de Madrid. (2006). *Riesgo Bajo Control*. Recuperado de <https://www.upm.es/sfs/Rectorado/Gerencia/Prevencion%20de%20Riesgos%20Laborales/Informacion%20sobre%20Prevencion%20de%20Riesgos%20Laborales/Manuales/folleto%20laboratorios%20el%C3%A9ctricos%201nov2006.pdf>
- [15] Méndez, P. V. (2009). *Reglamento de Prevención, Mitigación y protección contra Incendios*.
- [16] Norma IEC 62305-2: *Protección contra el rayo*. (2006). Ginebra, Suiza: Comisión Electrotécnica Internacional (IEC).
- [17] John Cadick, P. E., Capelli-Schellpfeffer, M., Neitzel, D. K., & Winfield, A. (2012). *Electrical safety handbook*. McGraw-Hill Education.
- [18] Toolbox, D. (2014). *Lightning Protection Guide 3rd Update Edition*.
- [19] Dorf, R., & Svoboda, J. (2015). *Circuitos eléctricos*. Alpha Editorial.
- [20] CONSTRUCCIÓN, N. (2018). *NEC-SB-IE (INSTALACIONES ELÉCTRICAS)*.
- [21] Aguilar García, M. A. (2019, agosto 20). *Falla en el neutro: Neutro cortado*. Blog de Miguel Ángel Aguilar García. Recuperado de <https://miguelangelaguilargarcia.blogspot.com/2019/08/falla-en-el-neutro-neutro-cortado.html>
- [22] Sectorelectricidad. (s.f.). *Regímenes de Neutro en Baja Tensión*. Recuperado de <https://www.sectorelectricidad.com/27258/regimenes-de-neutro-en-baja-tension/>
- [23] Carrasco, E. (2008). *Instalaciones eléctricas de baja tensión en edificios de viviendas*. Editorial Tébar.
- [24] Mora, J. F. (2002). *Introducción a las instalaciones eléctricas*. Colegio de Ingenieros de Camios, Canales y Puertos.

DESARROLLO DE UNA APLICACIÓN WEB PARA LA GRAFICACIÓN DE ATRACTORES CAÓTICOS UTILIZANDO LA METODOLOGÍA SCRUM

Development of a Web Application for Graphing Chaotic Attractors Using the SCRUM Methodology

Thalía Zárate Mora ^{1*}	talia.zarate@esPOCH.edu.ec
Raúl Rosero ^{1, †}	raul.rosero@esPOCH.edu.ec
Danilo Pastor ^{1, ‡}	danilo.pastor@esPOCH.edu.ec
Maricela Jiménez Rodríguez ^{2, ¶}	maricelajrodriguez@academicos.udg.mx
Omar S. Gómez	ogomez@esPOCH.edu.ec

¹ Facultad de Informática y Electrónica, Escuela Superior Politécnica de Chimborazo (ESPOCH), 060155, Riobamba, Ecuador,

² Profesora-Investigadora en el Centro Universitario de la Ciénega, Universidad de Guadalajara

³ Escuela Superior Politécnica de Chimborazo, Riobamba, Ecuador,

RESUMEN

El trabajo se enfoca en optimizar el proceso actual de la graficación de atractores en el Grupo de Investigación en Ingeniería de Software (GrIISoft) de la FIE-ESPOCH mediante el desarrollo de una aplicación web que automatiza dicho procedimiento con la metodología Scrum. La aplicación abarca atractores como Lorenz, Rossler, Sprott y Chen, incorporando funciones como gestión de usuarios y visualización de gráficos. A través de cuatro sprints, se implementaron 17 historias de usuarios y 8 historias técnicas. La evaluación comparativa entre el procedimiento actual de GrIISoft y la aplicación web reveló una reducción significativa del 98.9% en el tiempo de respuesta promedio, disminuyendo de 10501,67 ms a 116,57 ms. La aplicación demostró eficiencia en el uso de memoria y CPU en navegadores como Edge y Opera, con consumos más bajos, y exhibió la capacidad de manejar hasta 207 usuarios simultáneamente. Los resultados respaldan la mejora en los tiempos de respuesta.

Palabras Clave: Desarrollo de Aplicaciones Web, Metodología SCRUM, Atractores Caóticos, Modelo Vista Controlador, Norma ISO/IEC 25010, Eficiencia.

ABSTRACT

The work focuses on optimizing the current process of plotting attractors at the Software Engineering Research Group (GrIISoft) of FIE-ESPOCH by developing a web application that automates this procedure using the Scrum methodology. The application covers attractors such as Lorenz, Rossler, Sprott, and Chen, incorporating features such as user management and graph visualization. Through four sprints, 17 user stories and 8 technical stories were implemented. Comparative evaluation between GrIISoft's current procedure and the web application revealed a significant 98.9% reduction in average response time, decreasing from 10501.67 ms to 116.57 ms. The application demonstrated efficiency in memory and CPU usage on browsers like Edge and Opera, with lower consumptions, and exhibited the ability to handle up to 207 users simultaneously. The results support the improvement in response times.

Palabras Clave: Web Application Development, SCRUM Methodology, Chaotic Attractors, Model-View-Controller, ISO/IEC 25010 Standard, Efficiency.

► I. Introducción

En el ámbito de la visualización y representación gráfica de sistemas caóticos, el desarrollo de aplicaciones web modernas ha ganado relevancia como medio para mejorar la accesibilidad y eficiencia en la generación de atractores caóticos. El presente trabajo se centra en la creación de una aplicación web destinada a tal fin, específicamente dirigida al Grupo de Investigación en Ingeniería de Software (GrIISof), perteneciente a la FIE-ESPOCH. Este grupo se encuentra desarrollando el proyecto titulado: Enfoque de cifrado de objetos JSON utilizando sincronización caótica a partir de análisis de un conjunto de atractores (IDIPI-283), en donde uno de los procesos necesarios es la graficación de atractores caóticos. El propósito principal de este proyecto es abordar la necesidad de optimizar y agilizar el proceso actual de generación de atractores, incorporando la metodología ágil Scrum para su desarrollo.

La aplicación web desarrollada se estructura en módulos clave que abarcan desde la gestión de usuarios hasta la visualización y consulta de gráficos. Para asegurar su viabilidad y eficiencia, se realizó un estudio de los atractores caóticos utilizados por GrIISof, enfocándose en los atractores Lorenz, Rossler, Sprott y Chen. Se describe el proceso de desarrollo, destacando la metodología Scrum como enfoque de gestión que permite iteraciones regulares y una comunicación eficiente entre el equipo de desarrollo y los interesados.

Para evaluar el rendimiento de la aplicación web desarrollada se compararon los tiempos de respuesta promedio con los del actual proceso de graficación de atractores de GrIISof. Los resultados revelan una mejora significativa en términos de velocidad de respuesta, lo que se traduce en una experiencia de usuario más fluida y efectiva. Además, se llevó a cabo un análisis del consumo de recursos de la aplicación web en distintos navegadores, lo que evidenció su eficacia en términos de utilización de memoria RAM, CPU y GPU. Asimismo, se evaluó la capacidad de la aplicación para gestionar múltiples usuarios simultáneos, demostrando de manera concluyente

su escalabilidad y adaptabilidad. Estos hallazgos contribuyen a la comprensión integral del rendimiento de la aplicación en comparación con el proceso existente de graficación de GrIISof, subrayando sus beneficios tanto en términos de velocidad como de eficiencia en el manejo de recursos.

El análisis estadístico ANOVA aplicado a los tiempos de respuesta respalda las mejoras observadas, validando la significativa diferencia entre los períodos pretest y postest. En conjunto, este trabajo presenta una solución efectiva para la generación de atractores caóticos a través de una aplicación web, incorporando los principios ágiles de Scrum para su desarrollo y garantizando mejoras notables en términos de rendimiento y eficiencia en comparación con el proceso previo.

► II. Marco teórico

A. Caos.

El caos se refiere a un estado de desorden absoluto en sistemas dinámicos, donde la predicción precisa de su comportamiento a largo plazo se vuelve imposible debido a la sensibilidad extrema a pequeñas alteraciones iniciales, conocido como el "efecto mariposa". Aunque estos sistemas muestran regularidades a corto plazo, su comportamiento se vuelve cada vez más impredecible a medida que pasa el tiempo, debido a la amplificación de errores iniciales. La teoría del caos surge para comprender este fenómeno, pero se destaca que, a pesar de utilizar características estadísticas para hacer predicciones, las leyes fundamentales de la física siguen siendo aplicables [1].

B. Sistemas dinámicos

Los sistemas dinámicos, son modelos matemáticos que intentan prever el comportamiento de sistemas físicos a lo largo del tiempo. Estos modelos emplean ecuaciones diferenciales o en diferencias finitas según la naturaleza continua o discreta del sistema. Cuando un sistema no cumple con el principio de superposición, se considera no lineal, lo que conduce a un estudio cualitativo para comprender su dinámica, con la posibilidad

de comportamiento caótico. Se clasifican en sistemas discretos y continuos, donde los sistemas lineales muestran cambios proporcionales a las variaciones iniciales, mientras que los no lineales pueden generar cambios significativos [2].

En los sistemas lineales, la incertidumbre se mantiene constante, mientras que en los no lineales puede variar en el tiempo. Además, se destaca la diferencia en la resolución analítica entre sistemas lineales y no lineales, siendo estos últimos más complejos y con posibles propiedades de "mezclado topográfico", lo que dificulta la predicción a largo plazo [1], [3].

1) Sistema caótico

Los sistemas caóticos, son sistemas dinámicos especialmente sensibles a las condiciones iniciales. Incluso pequeñas variaciones en estas condiciones pueden llevar a resultados radicalmente diferentes con el tiempo, lo que hace difícil predecir su comportamiento a largo plazo. Estos sistemas muestran sensibilidad exponencial a las condiciones iniciales, lo que implica que pequeños cambios se amplifican enormemente a medida que el sistema evoluciona [4].

El matemático y meteorólogo Edward Lorenz fue pionero en el estudio de sistemas caóticos al descubrir la gran sensibilidad de modelos matemáticos simples de la atmósfera a las condiciones iniciales. Esto llevó al descubrimiento de atractores extraños en sistemas caóticos, conjuntos de puntos que el sistema visita repetidamente, pero sin repetirse exactamente en el mismo orden, y que tienen una estructura fractal, mostrando complejidad infinita a cualquier escala de observación [4], [5].

La teoría del caos y el estudio de sistemas caóticos tienen aplicaciones en campos como física, biología, economía y meteorología. Estos sistemas permiten comprender fenómenos complejos y no lineales que escapan a los modelos deterministas tradicionales. Además, el caos se aplica en áreas como criptografía y generación de números aleatorios [6].

a) Ventajas y desventajas del sistema caótico

Tabla I
Ventajas y desventajas del sistema caóticos

VENTAJAS		DESVENTAJAS	
1.	Capacidad para generar patrones complejos.	1.	Falta de predicción precisa del comportamiento futuro.
2.	Comportamiento no lineal y no predecible.	2.	Dificultad para encontrar soluciones analíticas.
3.	Adaptabilidad y capacidad de respuesta al cambio.	3.	Dificultad para reproducir resultados.
4.	Potencial para la exploración de nuevas soluciones.	4.	Sensibilidad a pequeñas perturbaciones.

2) Atractor caótico

Un atractor se define como un conjunto de estados hacia los cuales un sistema tiende a evolucionar, abarcando diversas condiciones iniciales. Estos valores permanecen cercanos incluso ante pequeñas alteraciones. En sistemas de dimensiones limitadas, el atractor constituye una región en el espacio n-dimensional, siendo n el número de dimensiones, que pueden representar, por ejemplo, coordenadas de posición en entidades físicas o variables separadas en sistemas económicos [7].

La representación geométrica del atractor puede ser bidimensional o tridimensional, dependiendo de la variable en evolución. Puede tomar diversas formas, como un punto, conjunto finito de puntos, curva, variedad o incluso un conjunto complejo con estructura fractal, conocido como atractor extraño. En sistemas dinámicos caóticos, la descripción de los atractores ha sido un logro fundamental de la teoría del caos. Una trayectoria en el atractor no requiere restricciones particulares, excepto permanecer dentro del atractor con el tiempo, pudiendo ser periódica o caótica. Si un grupo de puntos muestra una pauta, pero se aleja con el tiempo, se denomina repelente, no un atractor [8].

El atractor es la representación geométrica de cómo un sistema evoluciona en el tiempo, identificable por su número de dimensiones. Una dimensión 0 indica un sistema estático, dimensión 1 denota sistema periódico, mientras que dimensión 2

o superior sugiere sistema cuasi-periódico. Un ejemplo es el péndulo oscilante, cuyo atractor puede guiar en oscilaciones regulares, pero variar debido a otros factores, resultando en trayectorias irregulares. La cuenca de un atractor es el conjunto de condiciones iniciales para un comportamiento determinado, y las trayectorias pueden ser periódicas, cuasi periódicas o caóticas [9].

- Atractor extraño

En el ámbito de los sistemas dinámicos no lineales y caóticos, los atractores extraños son regiones en el espacio de fases hacia las cuales convergen las dinámicas de sistemas que muestran comportamiento caótico. Estos atractores, representados por trayectorias curvas, describen la evolución de sistemas sometidos a movimientos caóticos. El atractor de Lorenz es un ejemplo clave de un atractor extraño tridimensional, reconocido por su complejidad y singularidad, adoptando una forma peculiar similar a las alas de una mariposa según un conjunto de ecuaciones diferenciales no lineales [10].

Estos atractores encapsulan dos características esenciales de los sistemas caóticos: determinismo e impredecibilidad. Geométricamente, los atractores extraños se caracterizan por tener una dimensión fractal, lo que refleja su compleja estructura y comportamiento no lineal. Su relevancia radica en su capacidad para ilustrar y comprender la dinámica de sistemas complejos que exhiben comportamientos caóticos impredecibles pero deterministas [11].

3) *Atractor de Lorenz*

El concepto del atractor de Lorenz, presentado por Lorenz en 1963, revolucionó la comprensión de los sistemas dinámicos no lineales. Lorenz demostró que las predicciones lineales para sistemas atmosféricos en miniatura no eran ni periódicas ni asintóticamente periódicas. Este descubrimiento reveló un comportamiento caótico en ciertos valores de parámetros, generando una complejidad extrema conocida como el atractor de Lorenz [4]. Este atractor consiste en un conjunto de puntos en el espacio de estado que siguen trayectorias

caóticas en un sistema dinámico descrito por las ecuaciones de Lorenz. Se puede observar en la Figura 1. su forma en "mariposa" se repite a diversas escalas y su sensibilidad a las condiciones iniciales implica que cambios mínimos en estas condiciones pueden provocar comportamientos radicalmente diferentes en el sistema a largo plazo. Este fenómeno desafía las predicciones lineales y destaca la naturaleza impredecible y compleja de los sistemas no lineales y caóticos [12].

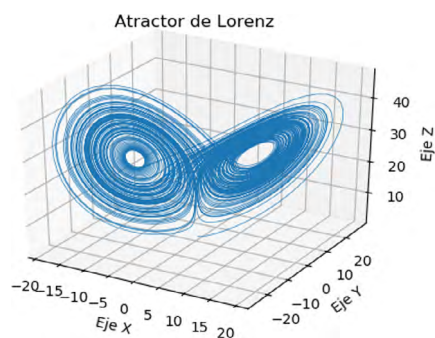


Fig. 1. *Atractor de Lorenz*

4) *Atractor de Rossler*

El artículo "An Equation for Continuous Chaos"[13] introduce el atractor de Rössler, un sistema dinámico no lineal definido por tres ecuaciones diferenciales ordinarias. Aunque tiene similitudes con el atractor de Lorenz, es más simple y muestra una estructura en forma de toro en su topología como se observa en la Figura 2. Este atractor exhibe dinámicas caóticas, caracterizadas por propiedades fractales, lo que significa que pequeñas variaciones en las condiciones iniciales pueden generar resultados radicalmente diferentes. Su comportamiento caótico lo hace sensible a las condiciones iniciales, lo que lo convierte en un fenómeno fascinante para el estudio de sistemas dinámicos y fractales [14].

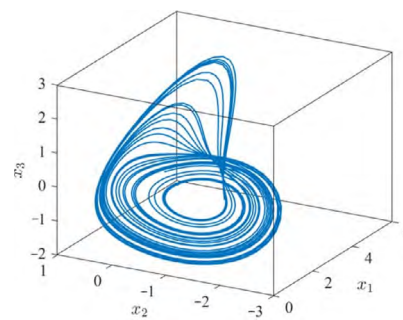


Fig. 2. *Atractor de Rossler*

5) *Atractor de Chen*

El descubrimiento de un atractor caótico por Guanrong Chen en 1999, que tiene similitudes, pero no es topológicamente equivalente al conocido Atractor de Lorenz [15]. Este nuevo atractor se encuentra en un sistema tridimensional autónomo de naturaleza simple. El atractor de Chen, también conocido como atractor de doble desplazamiento, presenta una estructura geométrica particular caracterizada por la presencia de un número infinito de capas fractales como se observa en la Figura 3. Cada sección del atractor muestra propiedades fractales a diferentes escalas, lo que implica que su complejidad se repite al observarlo con distintos niveles de magnificación. Este descubrimiento amplía la comprensión de los atractores caóticos al introducir un nuevo tipo con propiedades únicas y un comportamiento caótico distinto al Atractor de Lorenz [16].

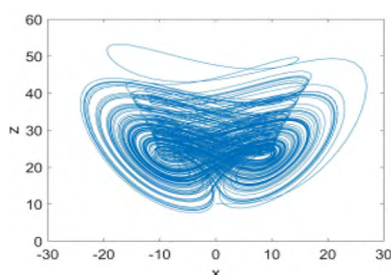


Fig. 3. *Atractor de Chen*

6) *Atractor de Sprott*

El atractor caótico de Sprott, es un fenómeno que muestra un comportamiento caótico a pesar de no tener puntos de equilibrio [17]. Se describe mediante una sola ecuación diferencial ordinaria de tercer orden y carece de parámetros específicos. En lugar de proporcionar condiciones iniciales, se presentan los exponentes de Lyapunov, que permiten obtener estas condiciones a partir de ellos [18]. Se puede observar la representación gráfica del atractor de Sprott en la Figura 4.

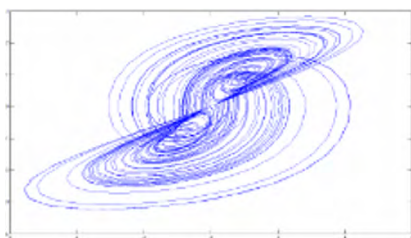


Fig. 4. *Atractor de Sprott*

► III. Marco metodológico

A. *Aplicación de la Metodología SCRUM*

En este apartado se mencionan las fases de desarrollo de la aplicación web para la graficación de atractores caóticos utilizando la metodología ágil SCRUM y la metodología de evaluación de la eficiencia de acuerdo con la norma ISO/IEC 25010.

1) *Product Backlog*

El product backlog registra todos los requisitos definidos por el propietario del producto. Estos requisitos se recopilan a través de entrevistas llevadas a cabo durante sesiones con el investigador Omar Gómez. Este se compone de historias de usuario y técnicas detalladas, fundamentales para la elaboración y desarrollo de la aplicación en cuestión.

2) *Sprint Backlog*

El sprint backlog se emplea para gestionar el progreso del desarrollo de software de manera eficiente. Su finalidad principal radica en garantizar el logro de los objetivos planteados. En el contexto específico de esta aplicación, se han ejecutado cuatro Sprints, cada uno con una duración de dos semanas con 20 puntos de esfuerzo en cada uno. Al finalizar cada sprint el equipo de desarrollo evaluó el cumplimiento de tareas de cada sprint, tomando en cuenta los puntos de estimación designados inicialmente para cada sprint.

3) *Desarrollo de la aplicación web de graficación de atractores*

Previamente a la presentación del Burndown Chart, resulta esencial destacar el desarrollo de la aplicación web dedicada a la graficación de atractores. Desarrollada como parte integral de este trabajo, dicha aplicación se ha diseñado no solo con el propósito de mejorar la eficiencia del proceso actual de graficación de atractores de GrIISof si no para facilitar la visualización y análisis de los atractores en el contexto de la investigación. La aplicación incluye módulos claves para la gestión de usuarios, autenticación,

almacenamiento y consulta de información mejorando potencialmente la experiencia de los investigadores que interactúen con la aplicación

El código fuente de la aplicación está disponible en el siguiente enlace <https://github.com/Thaferzzitha/griisoft-web-project>. Este enlace proporciona acceso al código fuente completo, permitiendo una revisión detallada del proyecto y la posibilidad de una futura contribución al desarrollo de mejoras en esta aplicación.

En la Figura 5. Podemos visualizar la interfaz del módulo de Graficación de atractores de la aplicación web desarrollada.

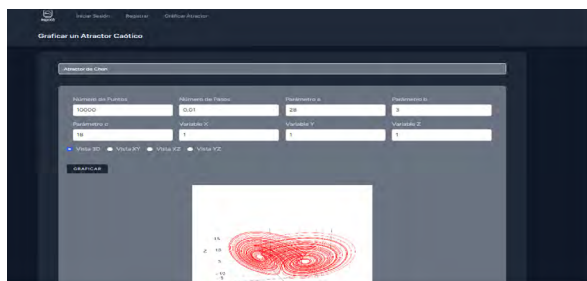


Fig. 5. Interfaz del módulo de graficación de la aplicación web

4) *Burndown Chart*

La metodología ágil SCRUM recomienda el burndown chart como una herramienta gráfica para la gestión del proyecto, en la cual se muestra el progreso del proyecto a lo largo de los sprints, revelando la velocidad con la que se cumplieron. En la Figura 6. se observa el burndown chart resultante del presente proyecto, en el eje X se muestran los 4 sprints, y en el eje Y se muestran los puntos estimados de esfuerzo. Los puntos estimados de esfuerzo se representan en la línea azul y los puntos reales de esfuerzo se representan en la línea naranja.

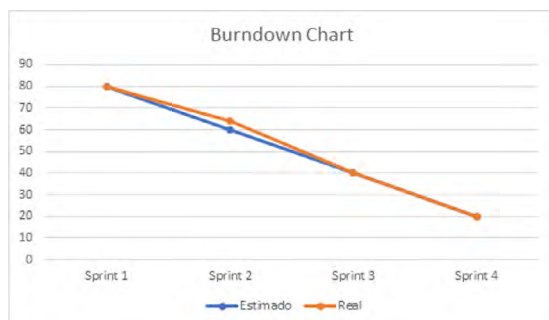


Fig. 6. Burndown Chart del Desarrollo de la aplicación web

Los sprints 1, 3 y 4 se desarrollaron a la par de los puntos estimados, sin embargo, en el sprint 2 existe un desfase respectivamente de los puntos estimados, esto debido a que en este sprint se desarrolló la funcionalidad de graficación de atractores caóticos, considerado por el equipo de desarrollo como una funcionalidad de dificultad alta.

B. Método utilizado para la evaluación de la Eficiencia en función a la norma la ISO/IEC 25010

Para poder evaluar la eficiencia de desempeño según la norma ISO/IEC 25010 se utilizó el método de observación, esto debido a que se observa el comportamiento, las acciones y eventos, en entornos naturales y controlados, de la aplicación web de graficación de atractores caóticos versus el proceso actual de graficación de atractores caóticos, para poder registrar los datos arrojados y analizarlos posteriormente.

1) Población

Se emplearon enfoques específicos para medir las tres subcaracterísticas de la norma ISO/IEC 25010, por lo tanto, cada subcaracterística tiene una población propia descrita a continuación.

- Cinco participantes con experiencia en sistemas de visualización web y ejecución de scripts Python, quienes interactuaron con la aplicación web de graficación de atractores caóticos versus el script de Python de graficación de atractores caóticos de GRIISOFT para evaluar sus Comportamiento Temporales.
- Cuatro navegadores webs comunes (Chrome, Firefox, Edge y Opera) que fueron sometidos a pruebas de rendimiento para evaluar la Utilización de Recursos.
- Trescientos usuarios simulados en una prueba de estrés para evaluar la Capacidad del sistema bajo condiciones de alta demanda.

2) *Recopilación de datos*

La recopilación de datos por cada subcaracterística se describe a continuación.

Comportamiento temporal

Las 5 personas seleccionadas realizaron interacciones con la aplicación y ejecutaron el script de Python tomado del proceso actual de GRIISOFT, generando gráficos del atractor caótico de Rossler. Cada individuo contribuyó con 6 tiempos de respuesta registrados durante estas interacciones, totalizando 60 registros en total.

Utilización de recursos

Los navegadores Chrome, Firefox, Edge y Opera fueron sometidos a pruebas de rendimiento en las cuales se midió el consumo de CPU, RAM y GPU mientras se generaban los gráficos de atractores caóticos. Se realizaron 3 repeticiones de las pruebas para cada navegador, obteniendo un total de 12 registros de utilización de recursos.

Capacidad

La evaluación de la Capacidad del sistema se llevó a cabo mediante una prueba de estrés diseñada en la herramienta JMeter para medir su rendimiento bajo cargas extremas. En esta prueba, se simularon 300 usuarios interactuando con la graficación de atractores caóticos, con un intervalo de 1 segundo entre cada interacción. Esta prueba permitió determinar la capacidad máxima del sistema para manejar usuarios simultáneos sin comprometer significativamente el rendimiento.

► **III. Marco de Resultados**

A. Evaluación de la eficiencia de desempeño según la norma ISO/IEC 25010

En la evaluación de la eficiencia de desempeño se la lleva a cabo con el análisis de sus tres subcaracterísticas: Comportamiento temporal, Utilización de recursos y Capacidad.

1) *Comportamiento Temporal*

Para conocer el Comportamiento Temporal del proceso actual de graficación de atractores caóticos de GRIISOFT y del módulo de graficación de atractores caóticos de la aplicación web se tomaron los tiempos de respuesta que perciben los usuarios al ejecutar manualmente el script Python del proceso actual y utilizar la funcionalidad automatizada de la aplicación web, y una vez obtenidos estos resultados se pudo comparar ambos tiempos promedio y conocer si existe diferencia en los procesos de graficación de atractores caóticos.

a) Tiempo de respuesta

Los tiempos de respuesta se pueden conocer de forma exacta debido a que se se agregaron líneas de código al inicio y fin de las funciones que grafican el atractor caótico en ambos procesos, estas líneas de código nos permiten contar el tiempo exacto que demoran en ejecutarse las funciones y como resultado mostrar el gráfico del atractor caótico. Cabe mencionar que con el fin de obtener el mismo resultado (grafico) se evaluó en base a la graficación del atractor caótico de Rossler con los siguientes datos.

- Número de puntos: 10000
- Número de pasos: 0,01
- Parámetro a: 0,2
- Parámetro b: 0,2
- Parámetro c: 5,7
- Variable x: 1
- Variable y: 1
- Variable z: 1

Dando como resultado resultado por cada uno de los procesos 30 tiempos, 6 por cada persona.

Los datos obtenidos del proceso actual de GRIISOFT se pueden observar en la TABLA II.

Tabla II

TIEMPOS DE RESPUESTA DEL PROCESO ACTUAL DE GRIISOFT

Tiempos (ms)	Persona 1	Persona 2	Persona 3	Persona 4	Persona 5
T1	2600	4750	1700	590	870
T2	2570	4520	1660	540	830
T3	4120	2300	1560	590	860
T4	2100	4150	1800	550	890
T5	3390	5120	1780	550	2860
T6	2150	3320	1690	540	2060
Total	16930	24160	10190	3360	8370
Promedio	2821,67	4026,67	1698,33	560	1395

Los datos obtenidos del proceso en la aplicación web se pueden observar en la TABLA III.

Tabla III

Tiempos de respuesta del proceso en la aplicación web

Tiempos (ms)	Persona 1	Persona 2	Persona 3	Persona 4	Persona 5
T1	51,69	163,89	227,73	102,8	78,34
T2	52,29	160,19	205,68	89,77	59,74
T3	56,34	138,94	234,71	64,01	95,83
T4	58,33	156,61	211,58	70,49	54,49
T5	52,92	162,07	227,1	66,04	53,21
T6	52,08	187,89	220,6	68,09	73,62
Total	323,65	969,59	1327,4	461,2	415,23
Prome-dios	53,94	161,60	221,23	76,87	69,21

Comparación de resultados

En la TABLA IV se presentan y analizan los promedios de los datos obtenidos y descritos previamente de los procesos realizados actualmente por GRIISOFT y realizados por la aplicación web.

Tabla IV

Comparación de tiempos de respuesta entre los dos procesos

	Promedio del proceso actual	Promedio de la aplicación web	Reducción en el tiempo
Tiempos (ms)	10501,67	116,57	10385,10

Se puede notar una disminución de los tiempos de respuesta entre el proceso actual de GRIISOFT y la aplicación web, pues el proceso actual de GRIISOFT tiene un tiempo promedio de 10501,67 ms y el tiempo promedio de la aplicación web es del 116,57 ms, por lo que los investigadores

de GRIISOFT al usar la aplicación web estarían ahorrando hasta 10385,10 ms en la graficación de atractores caóticos, lo que convertido a minutos es 0,17. Al disminuir el tiempo de respuesta en cada iteración durante la graficación de atractores caóticos, se abre un margen significativo para la experimentación. Esto permite a los investigadores probar una variedad más amplia de enfoques, ajustar variables y profundizar en sus investigaciones en el mismo intervalo de tiempo.

2) Utilización de Recursos

Para evaluar la Utilización de Recursos de la aplicación web se monitoreó el uso de memoria RAM, el uso de CPU y el uso de GPU observando los datos obtenidos con el Administrador de Tareas del computador, los cuales fueron tabulados y se obtuvieron los promedios del uso de cada uno de los recursos mencionados.

a) Uso de memoria RAM

El análisis del uso de memoria RAM es esencial para comprender cómo la aplicación web de graficación de atractores caóticos maneja los recursos disponibles. Se llevó a cabo una evaluación del uso de memoria RAM, planteando como escenario, la graficación del atractor caótico de Rossler, el mismo que se lo realizó 3 veces en los navegadores: Chrome, Firefox, Edge y Opera, capturando los datos que se obtiene con el administrador de tareas. Una vez monitoreado el uso de memoria RAM en Chrome, Firefox, Edge y Opera, se procedió a sintetizar los resultados en la TABLA V.

Tabla V

Resultado del uso de memoria RAM

RAM (MB)	Chrome	Firefox	Edge	Opera
Prueba 1	342,6	384,6	121,8	96,2
Prueba 2	331,2	457,1	123	97,4
Prueba 3	398,1	467,9	121,3	76,6
Total	1071,9	1309,6	366,1	270,2
Promedio	357,3	436,5	122,03	90,1

Se puede observar que cada navegador tiene un consumo promedio de memoria RAM distinto,

siendo Firefox el de consumo más alto con 436,5 MB y Opera el de consumo más bajo con 90,1

b) *Uso de CPU*

Es posible identificar patrones de comportamiento mediante el análisis de la utilización de la unidad central de procesamiento (CPU) durante la ejecución de la aplicación web destinada a la graficación de atractores. Por lo tanto, para comprender cómo cada navegador maneja los recursos de CPU, se llevó a cabo una evaluación centrada en la graficación del atractor caótico de Rossler. Varios navegadores, incluidos Chrome, Firefox, Edge y Opera, repitieron este proceso tres veces. Los datos de los administradores de tareas de cada navegador se registraron, lo que da una imagen precisa de la utilización de recursos de CPU en tiempo real.

Una vez monitoreado el uso de CPU en Chrome, Firefox, Edge y Opera, se procedió a sintetizar los resultados en la TABLA VI.

Tabla VI
Resultado del uso de CPU

CPU (%)	Chrome	Firefox	Edge	Opera
Prueba 1	1,7	3,5	2,2	1,6
Prueba 2	1,1	3,9	2,3	2,5
Prueba 3	1,1	3,4	2,1	2,1
Total	3,9	10,8	6,6	6,2
Promedio	1,3	3,6	2,20	2,1

Se puede observar que cada navegador tiene un consumo promedio de uso de CPU distinto durante las pruebas de generación del atractor caótico de Rossler, siendo Firefox el de consumo más alto con 3.6 de recursos de CPU y Chrome el consumo más bajo con 1.3 de recursos de CPU.

c) *Uso de GPU*

El análisis de la utilización de GPU permite tener una visión profunda de cómo se gestionan los recursos disponibles para la renderización gráfica durante la ejecución de la aplicación web de graficación de atractores, para comprender cómo cada navegador distribuye y gestionan los recursos de GPU. Se utilizó la graficación del atractor caótico de Rossler como escenario para realizar

una evaluación del rendimiento de la unidad de procesamiento gráfico (GPU). En los navegadores Chrome, Firefox, Edge y Opera este proceso se repitió tres veces. Los datos proporcionados por el administrador de tareas de cada navegador durante estas pruebas se registraron y analizaron. Este método permitió obtener una comprensión completa de cómo se gestiona la carga gráfica intensiva en cada situación.

Una vez monitoreado el uso de GPU en Chrome, Firefox, Edge y Opera, se procedió a sintetizar los resultados en la TABLA VII.

Tabla VII
Resultado del uso de GPU

GPU (%)	Chrome	Firefox	Edge	Opera
Prueba 1	12	25	29	13
Prueba 2	13	24	27	12
Prueba 3	14	18	31	13
Total	39	67	87	38
Promedio	13	22,3	29	12,7

Se puede observar que cada navegador tiene un consumo promedio de uso de GPU distinto durante las pruebas de generación del atractor caótico de Rossler, siendo Edge el de consumo más alto con 29 de recursos de GPU y Chrome el consumo más bajo con 12.7 de recursos de CPU.

3) *Capacidad*

La evaluación de la capacidad es esencial para comprender los límites operativos del sistema y asegurarse de que esté preparado para afrontar cargas máximas y situaciones de demanda intensa. En esta evaluación se llegó a determinar el límite de usuarios concurrentes que la aplicación web de graficación de atractores caóticos, específicamente del módulo de graficación, puede manejar antes de que se alcancen umbrales críticos de rendimiento, en un ambiente controlado, en un servidor local.

a) *Escenario de carga*

Se crearon tres escenarios de carga en JMeter, cada uno representando una cantidad de 100 usuarios concurrentes. Estos escenarios abarcaron

desde cargas bajas hasta cargas muy altas, con incrementos de 100 usuarios en cada escenario de carga, hasta encontrar en que cantidad de usuarios empieza a dar errores en la carga del módulo de graficación.

b) Monitoreo y registro de datos

Una vez ejecutada las 3 primeras pruebas con un incremento de 100 usuarios en cada prueba, se obtuvieron los datos que se observan en la TABLA VIII.

Tabla VIII
Resultados de las tres primeras pruebas en JMeter.

Con 100 Usuarios						
Label	# Samples	Average	Min	Max	Std. Dev.	Error %
HTTP Request	100	8254	0	16214	4668.06	0.00%
TOTAL	100	8254	0	16214	4668.06	0.00%
Con 200 Usuarios						
HTTP Request	200	17182	0	33904	9657.52	0.00%
TOTAL	200	17182	0	33904	9657.52	0.00%
Con 300 Usuarios						
HTTP Request	300	12471	0	35946	12068.66	32.00%
TOTAL	300	12471	0	35946	12068.66	32.00%

Se puede observar que en las primera dos pruebas no se obtuvieron errores, sin embargo, en la tercera prueba con 300 usuarios se obtuvo un 32% de errores lo que es igual a 96 usuarios que el servidor no permitió el ingreso al módulo de graficación. También, se puede decir que, hasta 204 usuarios concurrentes el sistema no debería mostrar errores, por lo que se procedió a realizar una prueba con 204 usuarios concurrentes. Los resultados de la cuarta prueba se muestran en la TABLA IX.

Tabla IX
Resultados de la cuarta prueba en JMeter

Label	# Samples	Average	Min	Max	Std. Dev.	Error %
HTTP Request	204	24425	0	43502	12594.97	0.00%
TOTAL	204	24425	0	43502	12594.97	0.00%

Se muestran resultados esperados al ejecutar la prueba con 204 usuarios, debido a que no

existieron errores, por lo que se procedió a encontrar cual es el límite de usuarios, para aquello se ejecutaron pruebas con un aumento de un usuario en cada prueba, hasta encontrar cual es el límite de usuarios en la que el servidor responde. En la TABLA X se observa la ejecución de las dos últimas pruebas, que contienen el límite de usuarios sin errores, y el número de usuarios en las que el servidor no responde.

Tabla X
Resultados de las dos últimas pruebas en JMeter

Con 207 Usuarios						
Label	# Samples	Average	Min	Max	Std. Dev.	Error %
HTTP Request	207	17661	0	35057	10296.9	0.00%
TOTAL	207	17661	0	35057	10296.9	0.00%
Con 208 Usuarios						
HTTP Request	208	17288	0	34021	9843.26	0.48%
TOTAL	208	17288	0	34021	9843.26	0.48%

B) Evaluación comparativa de tiempos de respuesta mediante un test estadístico

A través del análisis estadístico, se busca determinar si existen diferencias significativas en los tiempos de respuesta del proceso actual de graficación de atractores de GRIISOFT versus la aplicación web desarrollada.

1) Planteamiento de la hipótesis

Hipótesis nula (H0): Los tiempos de respuesta del proceso actual de graficación de atractores de GRIISOFT y la aplicación web de graficación de atractores son iguales.

Hipótesis alternativa (Ha): Los tiempos de respuesta del proceso actual de graficación de atractores caóticos de GRIISOFT y la aplicación web de graficación de atractores caóticos son diferentes.

2) Recopilación de datos

Los tiempos de respuesta previamente registrados

en el comportamiento temporal se utilizarán como pretest correspondientes a los tiempos del proceso actual de graficación de atractores caóticos de GRIISOFT, que se muestran en la TABLA II, y como postest correspondientes a los tiempos obtenidos a través de la aplicación web de graficación de atractores caóticos, que se muestran en la TABLA III. Para su análisis posterior en R Studio con el lenguaje R, estos datos se han reunido en la TABLA XI. Es importante destacar que los tiempos de respuesta se han redondeado a números enteros para evitar posibles errores de procesamiento de datos en R.

Tabla XI
Tiempos de respuesta agrupados por Pretest y Postest

persona	periodo	respuesta
1	pretest	2600
1	postest	52
2	pretest	4750
2	postest	164
3	pretest	1700
3	postest	228
4	pretest	590
4	postest	103
5	pretest	870
5	postest	78
1	pretest	2570
1	postest	52
2	pretest	4520
2	postest	160
3	pretest	1660
3	postest	206
4	pretest	540
4	postest	90
5	pretest	830
5	postest	60
1	pretest	4120
1	postest	56
t	pretest	2300
2	postest	139
3	pretest	1560
3	postest	235
4	pretest	590
4	postest	64
5	pretest	860
5	postest	96
1	pretest	2100

1	postest	58
2	pretest	4150
2	postest	157
3	pretest	1800
3	postest	212
4	pretest	550
4	postest	70
5	pretest	890
5	postest	54
1	pretest	3390
1	postest	53
2	pretest	5120
2	postest	162
3	pretest	1780
3	postest	227
4	pretest	550
4	postest	66
5	pretest	2860
5	postest	53
1	pretest	2150
1	postest	52
2	pretest	3320
2	postest	188
3	pretest	1690
3	postest	203
4	pretest	540
4	postest	68
5	pretest	2060
5	postest	74

3) Selección del Test estadístico

Se optó por realizar un análisis de varianza (ANOVA) en este contexto específico, donde se trabajó con dos grupos distintos (pretest y postest). El propósito de esta elección estadística es discernir si existen diferencias significativas en las medias de dichos grupos. La aplicación del ANOVA resulta pertinente en situaciones donde se busca determinar si al menos uno de los grupos difiere de manera estadísticamente significativa de los otros en términos de la variable de interés.

4) Aplicación del Test estadístico

El test estadístico se realizó usando la herramienta R Studio, en la Figura 7. y en la Figura 8. se detalla la ejecución:

```

1 library("psych")
2
3 datos = test_thalia_zarate
4
5
6 describeby(datos$respuesta, datos$periodo)
7
8 boxplot(respuesta ~ periodo, data=datos, main="Diagrama de Caja", xlab="Periodo", ylab="Duración(ms)")
9
0 model = aov(respuesta ~ persona + periodo + Error(persona/periodo), data = datos)
1
2 summary(model)
    
```

Fig. 7. Código en lenguaje R del test estadístico a ejecutar usando R Studio

En la Figura 8. se observan las estadísticas descriptivas agrupadas por el factor "periodo". Esto te muestra la media, la desviación estándar, la mediana y otros estadísticos para cada período (pretest y postest).

```

Descriptive statistics by group
group: postest
vars n mean sd median trimmed mad min max range skew kurtosis se
X1 1 30 116 65.89 84 109.75 46.7 52 235 183 0.55 -1.37 12.03
-----
group: pretest
vars n mean sd median trimmed mad min max range skew kurtosis se
X1 1 30 2100.33 1388.29 1790 1957.92 1401.06 540 5120 4580 0.65 -0.76 253.47
    
```

Fig. 8. Estadísticas descriptivas agrupadas por el factor periodo

En la Figura 9. Se puede observar de mejor manera la distribución de los tiempos de respuesta en los dos períodos en un diagrama de caja.

```

Descriptive statistics by group
group: postest
vars n mean sd median trimmed mad min max range skew kurtosis se
X1 1 30 116 65.89 84 109.75 46.7 52 235 183 0.55 -1.37 12.03
-----
group: pretest
vars n mean sd median trimmed mad min max range skew kurtosis se
X1 1 30 2100.33 1388.29 1790 1957.92 1401.06 540 5120 4580 0.65 -0.76 253.47
    
```

Fig. 9. Diagrama de caja con la distribución de los tiempos

5) Resultados del Test estadísticos

En la Figura 10. Se puede observar los resultados del Test estadístico ANOVA.

```

Error: persona
Df Sum Sq Mean Sq
persona 1 12189000 12189000

Error: persona:periodo
Df Sum Sq Mean Sq
periodo 1 30120591 30120591

Error: Within
Df Sum Sq Mean Sq F value Pr(>F)
periodo 1 40721291 40721291 71.15 1.5e-11 ***
Residuals 56 32051604 572350
---
Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
    
```

Fig. 10. Resultados del Test estadístico ANOVA

Se detallan los resultados del Test a continuación.

El análisis compara la variabilidad entre grupos (personas, periodos) con la variabilidad dentro

de los grupos. La hipótesis nula es que no hay diferencias significativas entre los grupos, y la hipótesis alternativa es que los grupos son diferentes entre sí. El estadístico F se utiliza para evaluar si la variabilidad entre grupos es significativamente mayor que la variabilidad dentro de los grupos

Para determinar si las diferencias son significativas, el ANOVA calcula una estadística llamada F-value. Este valor se obtiene al dividir la variabilidad entre grupos por la variabilidad dentro de los grupos. Si el F-value es grande y la probabilidad asociada con él ($Pr(>F)$) es pequeña, entonces se concluye que uno de los grupos es significativamente diferente del otro.

6) Interpretación de los resultados

El resumen del ANOVA proporciona los resultados de la prueba de hipótesis para cada uno de los términos en el modelo:

- El factor "periodo" muestra un valor de F significativo ($Pr(>F) < 0.001$), lo que indica que existe una diferencia significativa entre los períodos (pretest y postest) en términos de tiempos de respuesta. En otras palabras, hay una diferencia estadísticamente significativa entre los tiempos de respuesta antes y después del proceso.
- La interacción "persona:periodo" no se muestra en el resumen, lo que podría indicar que no hay una diferencia significativa en cómo los tiempos de respuesta varían entre las personas en diferentes períodos. Esto no necesariamente significa que la interacción no es relevante, solo que no es significativa en este modelo.
- El valor de F para la variación dentro de "persona:periodo" (Within) también es significativo, lo que indica que hay diferencias significativas entre las respuestas de las personas en diferentes períodos, una vez que se ha tenido en cuenta la variación individual y la variación debida a la interacción.

Conclusión del Test estadístico

Basándonos en los resultados del ANOVA, podemos concluir que existe una diferencia significativa en los tiempos de respuesta entre los períodos (pretest y posttest). Por lo tanto, podríamos rechazar la hipótesis nula (H_0) y aceptar la hipótesis alternativa (H_a). Esto significa que los tiempos de respuesta del proceso actual de graficación de atractores de GRIISOFT y la aplicación web de graficación de atractores son diferentes en términos de los dos períodos evaluados.

» V. Conclusiones

Con base en la observación y revisión documental, se realizó un análisis de los atractores caóticos empleados por GRIISOFT, que abarcan el atractor de Lorenz, Rossler, Chen y Sprott. Estos atractores presentan similitudes, tales como comportamientos no lineales y sensibilidad a condiciones iniciales, siendo todos tridimensionales y compartiendo el mismo conjunto de variables y parámetros. Estos hallazgos resultaron esenciales para el desarrollo del algoritmo destinado a la graficación los atractores en la aplicación web.

En la implementación de los módulos de gestión de usuarios, autenticación, información, creación y consulta de gráficos en la aplicación web, se adoptó la metodología Scrum. Esta metodología facilitó la agilidad y flexibilidad en el desarrollo al gestionar iteraciones, permitiendo así completar el producto dentro de los plazos establecidos de manera efectiva.

La eficiencia de desempeño del proceso actual de GRIISOFT y la aplicación web se evaluó utilizando la norma ISO/IEC 25010, específicamente en sus tres subcaracterísticas: Comportamiento temporal, Utilización de recursos y Capacidad. Se registraron los siguientes resultados: el tiempo de respuesta fue de 10501,67 ms para el proceso actual y 116,57 ms para la aplicación web al graficar un atractor caótico, lo que indica una reducción del 98,89% en el tiempo de respuesta entre ambos procesos. En cuanto al consumo de recursos, se observó que el navegador con menor consumo de memoria

RAM es Opera con 90,1 MB, el menor consumo de CPU se encontró en Chrome con un 1,3%, y el menor consumo de GPU también correspondió a Chrome, con un 13%. Además, se determinó que el módulo de graficación puede soportar hasta 207 usuarios concurrentes.

» V. Referencias

- M. J. Sametband, "ENTRE EL ORDEN Y EL CAOS. La complejidad," 1999.
- [2] E. I. Amaya Barrera, C. A. Suárez Parra, R. E. Huérfano Ortiz, J. D. Moreno Posada, and F. A. Parra Fuentes, "Modelo de encriptación simétrica basada en atractores caóticos," *Ingeniería*, vol. 21, no. 3, 2016, doi: 10.14483/udistrital.jour.reving.2016.3.a08.
- [3] S. H. Strogatz, *Nonlinear Dynamics And Chaos*. 1994. Accessed: Mar. 04, 2023. [Online]. Available: <http://users.uoa.gr/~pjoannou/nonlin/Strogatz,%20S.%20H.%20-%20Nonlinear%20Dynamics%20And%20Chaos.pdf>
- [4] E. N. Lorenz, "Deterministic Nonperiodic Flow," *J Atmos Sci*, vol. 20, no. 2, pp. 130–141, 1963, Accessed: Jan. 21, 2023. [Online]. Available: https://journals.ametsoc.org/view/journals/atsc/20/2/1520-0469_1963_020_0130_dnf_2_0_co_2.xml
- [5] I. F. Rodríguez Rodríguez, E. I. Amaya Barrera, C. A. Suarez Parra, and J. D. Moreno Posada, "Algoritmo de Encriptación de Imágenes Utilizando el Atractor Caótico de Lorenz," *Ingeniería*, vol. 22, no. 3, 2017, doi: 10.14483/23448393.11976.
- [6] J. Ruitter, "Scholarship @ Claremont Practical Chaos: Using Dynamical Systems to Encrypt Audio and Visual Data," 2019. [Online]. Available: https://scholarship.claremont.edu/scripps_theses/1389
- [7] AcademiaLab, "Atractor," <https://academia-lab.com/enciclopedia/attractor/>.
- [8] M. Fuentes, "Dinámica científica y medidas de complejidad." Accessed: Aug. 14, 2023. [Online]. Available: https://books.google.com.ec/s?id=Z8T0DwAAQBAJ&prints_ec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
- [9] C. Andreu, J. Echave, and G. Buela, "Psicothema," *Psicothema* Vol. 10 (no 2). Accessed: Aug. 14, 2023. [Online]. Available:

- <https://www.psicothema.com/pi?pii=168>
- [10] E. Durán Ruiz, “Teoria del Caos_2.” Accessed: Jul. 29, 2023. [Online]. Available: http://recursostic.educacion.es/descartes/web/materiales_didacticos/Teoria_caos/teoria_del_caos_2.html
- [11] M. Á. Medina Torres, “La complejidad de la naturaleza: Fractales, caos y jugando a hacer montones de arena,” 2007.
- [12] S. M. Alwan, A. M. Al-Mahdi, and O. H. Odhah, “Optimal Control and Bifurcation Issues for Lorenz-Rössler Model,” *Open Journal of Optimization*, vol. 09, no. 03, pp. 71–85, 2020, doi: 10.4236/ojop.2020.93006.
- [13] E. Rossler, “AN EQUATION FOR CONTINUOUS CHAOS,” 1976.
- [14] C. Aguilar Ibáñez et al., “Identificación del sistema de Rössler: enfoque algebraico y algoritmos genéticos,” 2005.
- [15] G. Chen, “YET ANOTHER CHAOTIC ATTRACTOR,” 1999. [Online]. Available: www.worldscientific.com
- [16] P. Augustová and Z. Beran, “Characteristics of the Chen Attractor,” *Advances in Intelligent Systems and Computing*, vol. 210, pp. 305–312, 2013, doi: 10.1007/978-3-319-00542-3_31.
- [17] Q. Lai and S. Chen, “Generating multiple chaotic attractors from Sprott B System,” *International Journal of Bifurcation and Chaos*, vol. 26, no. 11, Oct. 2016, doi: 10.1142/S0218127416501777.
- [18] E. León -GAMALIEL, S. Tellez -CANEK, S. Ibarra -YUMA, and N. Pérez -JOSE CRUZ, “Diseño de Sistemas Caóticos de Sprott usando los Exponentes de Lyapunov.”

RECURSOS EDUCATIVOS MULTIMEDIA PARA EL FOMENTO DEL PATRIMONIO CULTURAL INMATERIAL

Subtítulo: Identificación de personajes festivos populares chimboracenses

MULTIMEDIA EDUCATIONAL RESOURCES FOR THE PROMOTION OF INTANGIBLE CULTURAL HERITAGE

Subtopic: Identification of popular chimboracense festive characters

Ángel Xavier Solórzano Costales ¹	angel.solorzano@esPOCH.edu.ec
María Alexandra López Chiriboga ²	ma_lopez@esPOCH.edu.ec
Fausto Vinicio Oviedo Cevallos ³	fausto.oviedo@esPOCH.edu.ec
Raúl Renato López Chiriboga ⁴	correo.renato@gmail.com

^{1,2,3.} Facultad de Informática y Electrónica. Escuela Superior Politécnica de Chimborazo (ESPOCH), Riobamba, Ecuador,

⁴ Investigador independiente, Ambato, Ecuador.

RESUMEN

Ecuador es un país rico en cultura popular tradicional, reflejada en la diversidad de personajes festivos que representan las características demográficas y geográficas identitarias. El mayor grupo étnico presente en el país es el mestizo, seguido por el indígena, montubio y afroecuatorianos sincretizados dando origen a expresiones pagano-religiosas, patrimonio cultural inmaterial. Chimborazo visibiliza estas muestras de cultura escasamente difundidas, pobremente valorizadas, considerando la insuficiente documentación etnohistórica y la influencia de nuevas expresiones en la cotidianidad de los jóvenes, a través de la web. Esta investigación aprovecha la última aparente desventaja mencionada apostando por el uso de material multimedia para la educación patrimonial no formal. La metodología descriptiva cualitativa permitió determinar los personajes festivos representativos de los diez cantones, identificar elementos constituyentes. Entre los principales hallazgos se detectan siete personajes que fusionan herencias y significados, reconociendo rasgos comunes y distintivos en ellos. En tres cantones la presencia del personaje festivo es

poco relevante, prevalece la imagen religiosa católica, no considerada para este estudio. A partir de lo cual se estructura el sistema didáctico compuesto por fichas informativas narrativas-visuales, infografía global, plantillas *paper craft* y multimedia educativo como recurso principal y contenedor de los demás. Estos recursos brindan una opción dinámica y motivadora para el aprendizaje sensitivo patrimonial aceptado por las nuevas generaciones digitales.

Palabras Clave: Recursos educativos, personajes festivos, patrimonio cultural inmaterial, material multimedia, educación no formal.

ABSTRACT

Ecuador is a country rich in traditional popular culture, reflected in the diversity of festive characters that represent demographic and geographic identity characteristics. The largest ethnic group present in the country is the mestizo, followed by the indigenous, montubio and afro-ecuadorian syncretized, giving rise to pagan-religious expressions, intangible cultural

heritage. Chimborazo makes visible these poorly disseminated, poorly valued samples of culture, considering the insufficient ethnohistorical documentation and the influence of new expressions in the daily lives of young people, through the web. This research takes advantage of the last apparent disadvantage mentioned by betting on the use of multimedia material for non-formal heritage education. The qualitative descriptive methodology allowed us to determine the representative festive characters of the ten cantons and identify constituent elements. Among the main findings, seven characters are detected that merge heritages and meanings, recognizing common and distinctive traits in them. In three cantons the presence of the festive character is not very relevant, the Catholic religious image prevails, not considered for this study. From which the didactic system is structured, composed of narrative-visual information sheets, global infographics, paper craft templates and educational multimedia as the main resource and container for the others. These resources provide a dynamic and motivating option for sensitive heritage learning accepted by the new digital generations.

Keywords: Educational resources, festive characters, intangible cultural heritage, multimedia material, non-formal education.

► I. Introducción

El patrimonio cultural inmaterial sigue siendo motivo de preocupación por entidades públicas y organizaciones cuya finalidad es proteger la memoria de los pueblos, más aún en los actuales momentos donde la tecnología ha tomado un rol protagónico, aliado u opositor de la identidad cultural, y en países Sudamericanos tampoco se considera seriamente los recursos digitales como una herramienta de aprendizaje, no solo en la educación formal, sino en la informal, en espacios áulicos y cotidianos, de forma complementaria. Desde su óptica Arango, Según [14], se debe “permitir a las nuevas generaciones el acceso a infraestructura tecnológica y contenidos digitales”, mientras que [4] destacan lo favorable que es el entorno virtual en la participación social, individual y colectiva sobre todo en las nuevas generaciones.

Campaña [3] describen a la educación formal como las actividades que responden a una estructura, niveles y contenidos de aprendizaje regulados por normas de carácter jurídico e impartidos por instituciones cuya competencia educativa es reconocida y, por educación no formal, las acciones educativas estructuradas y reguladas por el ejercicio de competencias en este caso particular culturales, no institucionalizadas.

Los medios digitales y multimedia se han incorporado al aprendizaje formal y no formal patrimonial, cumpliendo un papel mediador durante todo el proceso y a decir de [16], permiten seleccionar el patrimonio a ser observado, su modo de contemplarlo y facilitan la actuación del educador, por sus posibilidades aleatorias, no lineales, flexibles y abiertos, además de ser motivador para una generación conectada a los medios digitales. Por tanto, la relación entre el patrimonio inmaterial, la educación y el uso de la tecnología puede ser una forma de identificar, salvaguardar y revitalizar la herencia cultural.

La realización de un sistema de recursos didácticos donde prevalece el multimedia de los personajes populares de la Provincia de Chimborazo, se enmarca dentro *la construcción de espacios de encuentro común y fortalecimiento de la identidad nacional, las identidades diversas, la plurinacionalidad y la interculturalidad* como dicta el Objetivo 5 del Plan Nacional del Buen Vivir [20] y pretende afianzar la consonancia de los pueblos, sus vivencias cotidianas, por medio del análisis de personajes que están en la memoria colectiva por su aspecto físico, humor, gracia, oficio y habilidades en el entorno festivo.

El patrimonio cultural inmaterial congrega una serie de manifestaciones como las sociales, mágicas, ergológicas utilitarias, ergológicas estéticas, lingüísticas, narrativas y poéticas. Representa los bienes inmateriales de una sociedad, la UNESCO expone:

Se entiende por patrimonio cultural inmaterial, los usos, representaciones, expresiones, conocimientos y técnicas-junto con los instrumentos, objetos, artefactos y espacios

culturales que les son inherentes-que las comunidades, los grupos en algunos casos los individuos reconozcan como parte integrante de su patrimonio cultural. Este patrimonio cultural inmaterial, que se transmite de generación en generación, es recreado constantemente por las comunidades y grupos en función de su entorno, su interacción con la naturaleza y su historia, infundiéndolo un sentimiento de identidad y continuidad y contribuyendo así a promover el respeto de la diversidad cultural y la creatividad humana [20].

Chimborazo es una provincia ubicada en la zona 3 del Ecuador, cuenta con diez cantones, tiene la mayor presencia de población indígena del país, la variedad fisionómica, dialéctica y de costumbres es amplia, ya que su disposición geográfica hace que cantones como Alausí y Chunchi tengan herencia cañari, mientras que Pallatanga y Cumandá tengan costumbres entremezcladas de la región de la Sierra central con el trópico. Este panorama determina la variedad de celebraciones y personajes populares que ayudan a resignificar las memorias colectivas de una provincia rica en elementos culturales.

La afirmación identitaria y el fortalecimiento de las tradiciones en cualquier país o ciudad especialmente en América del Sur, poseedora de una riqueza mestiza es invaluable, “Una dimensión de la identidad cultural corresponde al sentido de pertenencia a un lugar, en el caso de los ecuatorianos a una región”. [12]. El uso de medios tecnológicos y didácticos que están llamados no solo a informar o divertir sino a consolidar el vínculo sociedad - identidad, en una época invadida por nuevos medios que conviven con la niñez y juventud actual, son razones que han permitido en este estudio unir los factores cultural y multimedial.

Díaz, al respecto citan “el uso de Tecnologías de Información y Comunicación (TIC), específicamente a raíz de la cuarta y la quinta revolución tecnológica, constituye una línea de desarrollo en continua evolución en los procesos asociados a la gestión de la educación y en el diseño de herramientas educativas

para la construcción colaborativa de saberes” [7]. Dentro del aprendizaje formal e informal presenta múltiples ventajas para quien las usa, al integrar imágenes, sonidos, texto, etc., motiva su utilización.

El uso de un recurso multimedia sirve de apoyo en la transmisión de contenidos patrimoniales asociados a la construcción de la identidad cultural en adolescentes y jóvenes adultos, pero no es útil como tal, si se mantienen viejos hábitos en el proceso de enseñanza aprendizaje (PEA), metodologías, actividades y evaluaciones de modelos no asociados con la realidad actual del país.

Fontal, [10], afirman que el nuevo contexto en el que se ve inmiscuida la educación patrimonial, debido al vertiginoso avance de las Tecnologías de la Información y Comunicación, da mayor accesibilidad, ampliando el acercamiento de las nuevas generaciones en entornos virtuales. Este espacio virtual permite la facilidad en la adquisición de conocimiento, su comprensión, sensibilización y disfrute.

Como parte del proceso investigativo previo a este estudio, los autores detectaron datos puntuales sobre la existencia de distintas celebraciones, que se realizan en los cantones durante el transcurso del año, la cual se sumó a otras documentaciones para lograr determinar los personajes populares representativos que participan en ellas y de sus características, diferenciados correctamente, para una difusión dinámica, al alcance de todos, que vaya más allá de la identidad puruhá chimboracense. Como afirma [1], los personajes tienen vigencia identitaria en esferas diversas, se encuentran cobijados por “el afecto y reconocimiento del pueblo, asumen el papel de referentes que encarnan añoranzas, logros, imágenes vinculadas a los intereses colectivos...que dinamizan la memoria social”, a lo cual se puede añadir, sean reales, ficticios, fantásticos o de cualquier naturaleza. Desde el descubrimiento de América, la historia cuenta los atropellos a los pueblos aborígenes en la colonización, sin embargo, dentro de lo que significó la decadencia geográfica y social para los indígenas, en la época republicana junto a los

mestizos emprenden la lucha por diferenciar su identidad de la española y criolla.

Como argumenta [13], es muy común encontrar en fiestas indígenas una mezcla de personajes y manifestaciones que responden a la aculturación que fueron objetos de antepasados. Las transiciones sufridas por la sociedad ecuatoriana a lo largo de los siglos han dejado huellas profundas en las tradiciones, presentándose como un país rico en culturas, etnias, expresiones, lleno de colores, olores y sabores, a la espera de ser reconocidos y valorados. En este sentido, el universo digital ocupa un espacio importante en relación con la educación patrimonial [15], pues el entorno virtual genera procesos de conocimiento, puesta en valor, comprensión, sensibilización y disfrute del patrimonio cultural [19].

A pesar de la brecha digital en los países en vías de desarrollo, atravesada la crisis de la pandemia y una vez saboreada la educación virtual, en el campo de la educación patrimonial se observan nuevas lógicas de aprendizaje, como propuestas de recursos multimedia, pieza clave para el aprendizaje en entornos educativos variados, por sus posibilidades de interactividad que implican efectividad y usabilidad, además su estructura cobija contenidos técnicos visuales y estéticos de las disciplinas involucradas, perfectamente aplicables para la educación patrimonial, con amplias posibilidades de conexión con los jóvenes, quienes como especifica Scolari (2018), son elementos clave de esta cultura, que participan en una gran diversidad de situaciones de educación informal.

En este sentido, [11] plantea aspectos de interés que no siempre son considerados como el lenguaje comunicativo, la adecuación funcional del mensaje textual y visual, además enlista las funciones del diseño gráfico tradicionales y desde la retórica: la publicitaria, la estética, la constructiva, la comunicativa y la formativa o didáctica, estas dos últimas son las que en este estudio permiten la conexión triádica del patrimonio cultural inmaterial, la sociedad en el que se presentan las manifestaciones festivas populares y la transformación digital.

Como conciben [8] el uso de recursos interactivos y combinarlos dentro de un contexto socio-cultural específico en el aprendizaje permite que los significados adquieran y transmitan de manera participativa y dinámica. Un producto multimedia se convierte en un recurso didáctico que acopia datos relevantes, que permiten dar a conocer el testimonio silencioso de cada uno de los personajes analizados, democratizando su acceso y difusión.

► II. Metodología

El objetivo general de este trabajo es difundir el patrimonio cultural intangible utilizando el multimedia como recurso didáctico, para el aprendizaje formal e informal cultural de adolescentes y jóvenes universitarios, medio que hace uso de elementos identitarios y tecnológicos, consolidando datos de una investigación generada por el grupo de investigación KARAY laboratorio creativo de la Escuela Superior Politécnica de Chimborazo, así como de la tesis doctoral *Una práctica ar/rtográfica basada en la investigación de personajes ecuatorianos: El diseño de productos visuales como método para la construcción de la identidad cultural preadolescente*.

Bajo una investigación descriptiva cualitativa se determina la existencia de personajes originarios distintivos de los diez cantones para conseguir un listado definitivo descrito en fichas que contienen datos de relevancia como: historia, fechas, procedencia, vestimenta, rasgos característicos y únicos, así como la semiótica de las figuras populares principales.

Cabe especificar que el estudio se concentra en los personajes populares, pudiéndose presentar como seres humanos, animales, seres sobrenaturales, fantásticos o de cualquier tipo, que son protagonistas en una celebración, discriminando otros de índole diferente. Se valió de entrevistas semiestructuradas a fuentes primarias como personeros concedores de los Gobiernos Autónomos Descentralizados Provincial y Municipales, Museo de la Ciudad de Riobamba, Ministerio de Cultura y Patrimonio,

así como a promotores culturales en las ciudades de origen de los personajes. El cuestionario consideró un primer bloque de datos del informante que validen su experticia y sentido de pertenencia al lugar de origen, el segundo bloque constituido por preguntas específicas de las festividades, aspectos estructurantes y vinculantes con la comunidad y el tercer bloque referente a la importancia de difundir el patrimonio cultural festivo.

Tabla 1
ESTRUCTURA DEL CUESTIONARIO

BLOQUE A. Datos identitarios y sociodemográficos
BLOQUE B. Manifestaciones culturales populares de Chimborazo
B1. ¿Cuáles fiestas cívicas son las más representativas del cantón?
B2. ¿Cuáles fiestas religiosas son las más representativas del cantón?
B3. ¿Cuáles fiestas paganas son las más representativas del cantón?
B4. ¿Existe alguna fiesta, que usted considere la más importante?
BLOQUE C. Difusión y aprendizaje del patrimonio cultural inmaterial
C.1 ¿Considera que existe una adecuada difusión de las fiestas y sus personajes desde el punto de vista educativo?
C.2 ¿Actualmente existe recursos didácticos digitales o multimedia de las fiestas y/o sus personajes?

Paralelamente se revisan fuentes secundarias como libros, trabajos de titulación, tesis e inventarios, una muestra de dieciséis documentos fueron la base para determinar los personajes populares originarios chimboracenses, establecer el cantón correspondiente y fijar las características propias. Se señala que se identifica las apariciones reiterativas en dichos documentos.

Tabla 2
MATRIZ DE REVISIÓN DOCUMENTAL

Código	Documento	Autor	Cantón	Fiesta detectada
D01				
D02				
D03				

Se usa una matriz de compilación de la información documentada, hasta el momento de la investigación, respecto a las manifestaciones

festivas populares de la provincia de Chimborazo, a partir de lo cual se seleccionan las de mayor representatividad a criterio de las personas determinadas como fuentes primarias. Posterior a ello se hacen fichas de observación de los personajes culturales populares considerando aspectos formales, comportamentales y semióticos.

Tabla 3
MATRIZ DE REVISIÓN DOCUMENTAL

Cantón	Fiesta
Fotografías (mínimo 3)	
Información general	Nombre Tipo Momento y/o acto
Aspectos formales	Aspecto físico (aspectos corporales, fisonómicos) Etnia Género Indumentaria (estilo, cromática, iconos)
Aspectos comportamentales	Actitud Acciones Comportamiento
Aspectos semióticos	Denotativos connotativos

» III. Resultados

Los resultados que exponen los personajes identificados se aprecian en diferentes tablas y gráficos. En primera instancia se ubican documentadas 26 fiestas en los diez cantones chimboracenses, posteriormente las entrevistas permitieron filtrarlas, obteniendo un listado de las siete más representativas. Es necesario decir que no se tomaron en cuenta las fiestas cívicas. La primera tabla referencia a las fiestas detectadas en las fuentes secundarias, la que da paso a la infografía en la que se identifican los siete personajes populares y originarios, oriundos de los cantones, pero además conocidos y representativos para toda la provincia. Resaltando que en los cantones Guano, Pallatanga, Cumandá no presentaron personajes populares de relevancia para sus pobladores, con las características de sincretismo que se requería. En estos lugares más bien tienen protagonismo las fiestas netamente católicas y su personaje religioso central.

Tabla 4
FIESTAS Y PERSONAJES REPRESENTATIVOS CANTONALES

Cantón	Fiesta	Personaje
Alausí	Carnaval	Rey Carnaval Embajador
Chambo	Fiesta de los Diablitos Semana Santa	Diablito de San Juan Evan- gelista Cucurucho
Chunchi	Carnaval	Rey Carnaval Embajador
Colta	Carnaval	Danzante de Plata de Colta
Cumandá	Virgen de los Dolores*	Virgen*
Guamote	Carnaval	Rey Carnaval Embajador
Guano	Virgen María Inmaculada*	Virgen*
Pallatanga	La Virgen de la Merced*	Virgen*
Penipe	Día de los Difuntos	Animero
Riobamba	Semana Santa Pase del Niño Rey de Reyes	Cucurucho Diablo de Lata

En la Tabla 4 se observan las fiestas detectadas a través de los instrumentos de recolección de datos tanto de las fuentes primarias y de las secundarias. La fiesta del Carnaval aparece en el 75% de los documentos revisados, ya sea en toda la provincia o específicamente de los cantones de Alausí, Chunchi, Colta o Guamote; en el 62,7% se observa el Pase del Niño Rey de Reyes; en el 31,5% aparece la fiesta religiosa de la Semana Santa (Riobamba y Chambo); en el 43,75%, el Día de los Difuntos y en el 18,75%, la fiesta de los Diablitos de Chambo, y en el 18,75% existe más bien una generalización de las festividades provinciales. Por otra parte, los personajes con mayor presencia aparecen en la Tabla 4, siendo en Diablo de Lata mencionado en 62,7%, seguido por el Rey Carnaval (31,5%), el Cucurucho (31,5%), el Animero (43,75%), el Danzante de Plata de Colta (50%), el Diablito de San Juan Evangelista (18,75%) y el Embajador (31,25%). Es importante señalar que la suma total de los porcentajes señalados no ofrece como resultado el 100%, ya que las cinco fiestas detectadas y calificadas como representativas fueron localizadas en varios de los documentos.

FIESTAS DETECTADAS

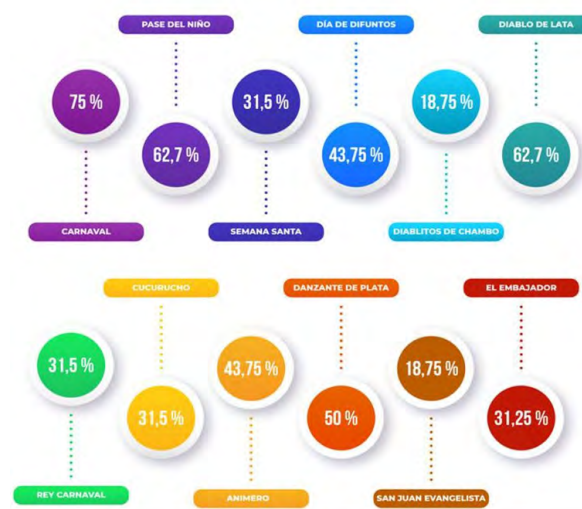


Fig. 1 Fiestas detectadas.



Fig. 2 Infografía de Personajes Chimborazo.

El diseño del multimedia como recurso didáctico pudo congregar una serie de elementos informativos, educativos y significativos de los principales personajes y sus lugares de origen, se estructuró considerando características de simplicidad, usabilidad, fácil navegabilidad, además del aspecto estilístico en una línea gráfica que incluye cromática, tipografía, fotografía, diagramación y composición gráfica con una consecución de línea geométrica y colores cálidos para resaltar no solo a los personajes sino motivar inconscientemente a los públicos del ámbito cultural y social chimboracense y ecuatoriano.

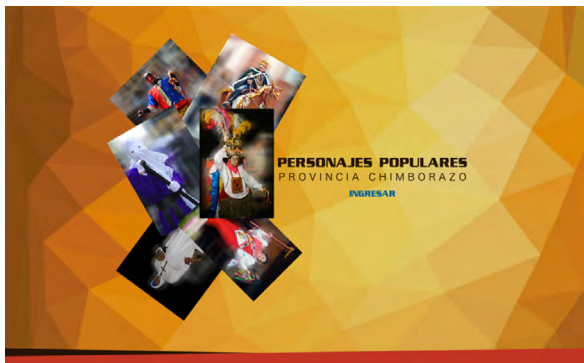


Fig. 3 Multimedia Chimborazo interactivo.



Fig. 6 Fig. 6 Plantillas digitales paper craft personajes.



Fig. 4 Multimedia Chimborazo interactivo.



Fig. 5 Personaje Festivo.

La configuración de los personajes en *paper craft* mantuvo rasgos propios investigados dentro de los cuales se encuentran el mestizaje base intrínseca de los rasgos físicos, vestimentarios y actitudinales de los protagonistas de las manifestaciones festivas populares detectadas.

Posterior a la realización se hace la validación del recurso didáctico multimedia con un grupo de adolescentes, quienes no tienen en su pénsum de estudios educación patrimonial, pero en materias vinculadas al arte e historia ecuatoriana topan brevemente temas vinculados a las manifestaciones culturales. El 90% se muestran interesados, destacan la facilidad de manejo del recurso, la comprensión del contenido, los elementos estéticos y la posibilidad de navegar según el interés particular en los personajes.

IV. Conclusiones

Como los describe Julio García Espinoza (2006): "La idea y reconocimiento de un personaje popular se ha esquematizado; puede ser vulgar, de mal gusto, chusma, pero en el fondo tiene un gran corazón y posee una gran sabiduría" [2]. En siete cantones se detectaron personajes míticos o de otra índole cuya presencia es indispensable en pregones, desfiles, procesiones, etc. los cuales son reconocidos en toda la provincia y poseen características imperecederas, por sus acciones, habilidades, físico o el significado detrás de ellos.

La tecnología afecta no solo a la economía de los países sino también a su cultura, con ello a la comunicación y a la educación, permitiendo al estudiante ser verdaderamente el elemento

Se programó el multimedia educativo con la información organizada y completa, además se incorporaron plantillas *paper craft* de los personajes, demostrando que es posible, el diálogo entre la comunidad y la academia, en la investigación y documentación de la memoria social, el patrimonio cultural y los conocimientos diversos, incentivar y difundir estudios y proyectos interdisciplinarios y transdisciplinarios sobre diversas culturas, identidades y patrimonios, con la finalidad de garantizar el legado a futuras generaciones como lo determinan las políticas del objetivo 5 del Plan del Buen Vivir.

activo en el proceso de enseñanza aprendizaje, teniendo la autonomía de generar por sí solo el conocimiento, en las áreas cognitiva, motriz o afectiva en la que se encuentra el desarrollo de la identidad, incluyendo la cultural.

Inicialmente, para diseñadores y artistas la exploración del uso de recursos vinculados a la tecnología tenía un fin netamente estético. En la actualidad es un recurso que ofrece oportunidades innovadoras, que además son motivantes, facilitando el aprendizaje y a través de quienes captan este aprendizaje la difusión y preservación del patrimonio cultural. El uso de recursos digitales multimedia en el aprendizaje cultural presenta ventajas, puntualmente en adolescentes y jóvenes universitarios. Son productos que conjugan imágenes, videos, sonido, actividades, además resultan fáciles de usar, flexibles al ritmo de cada individuo y por su estructura se adaptan a los diferentes estilos de aprendizaje. Sin embargo, su elaboración requiere “la participación de profesionales procedentes de diversas disciplinas y exige tener en cuenta varios principios de diseño tecnológico y pedagógico para su mejor aprovechamiento” [17].

El recurso multimedia posibilita la inclusión de información textual, imágenes, audio y otros elementos, además de ser un ambiente propicio tanto para la educación patrimonial formal o informal que transmite identidad, tradición y cultura de una forma dinámica para las generaciones digitales de adolescentes y jóvenes universitarios.

A partir de esta investigación se proyecta la realización de productos digitales culturales dentro de la didáctica del diseño, orientado a públicos jóvenes, que sean parte de la experiencia como estudiantes, dentro de la investigación formativa en la Carrera de Diseño Gráfico, cuyo rol complete la triada investigador-diseñador-profesor.

► V. Referencias

- [1] Báez-Jorge, F. (2010). *Personajes populares de Veracruz*. (1° ed.). Comisión Organizadora del Estado de Veracruz de Ignacio de la Llave.
- [2] Caballero, M., Ramos, R. & López, M. (2012). Ilustraciones infantiles de personajes tradicionales contemporáneos de la serranía ecuatoriana aplicada en una línea de soportes gráficos [Tesis de licenciatura, Escuela Superior Politécnica de Chimborazo]. Repositorio institucional-Escuela Superior Politécnica de Chimborazo. <http://dspace.esPOCH.edu.ec/handle/123456789/1960>
- [3] Cambil, I., Díez, M., Gómez, A., Hernández, M., Martos, J., Pedraza, M., Pérez, S., Ruiz, M., Cifuentes, C., Sánchez, S., & Viñas, M. (2022). Educar en patrimonio con perspectiva de género desde la educación no formal: El proyecto “Soleando el río de la vida”. *UNES. Universidad, Escuela y Sociedad*, 13, 49–68. <https://doi.org/10.30827/unes.i13.26161>
- [4] Cepeda, S. & Fontal, O. (2020). La arquitectura del vínculo a través de la web *Personas y Patrimonios*”. *OBETS. Revista de Ciencias Sociales*. 15(1), 137-158. <https://doi.org/10.14198/OBETS20202.15.1.05>
- [5] Chng, K. y Narayanan, S. (2017). Culture and social identity in preserving cultural heritage: an experimental study. *International Journal of Social Economics*, 44(8), 1078-1091. <https://doi.org/10.1108/IJSE-10-2015-0271>
- [6] Díaz, L., Comerci, S., Arias, S. & Piro, J. (2019). Tecnologías disruptivas - Inteligencia artificial aplicable a la gestión de políticas públicas en educación superior en contextos de masividad en M. Morales Editor (Ed.), *Tecnologías digitales - Miradas críticas de la apropiación en América Latina* (1ra. Ed., pp. 175-190). Editorial Consejo Latinoamericano de Ciencias Sociales.
- [7] Díaz, L., García Martínez, R. (2015). *Hacia una Praxis Transformadora de la Comprensión del Estudiante de la educación superior en contextos de masividad en VI Coloquio Internacional: Estado, Política Pública y Acción Colectiva*, Argentina, Córdoba: Editorial UNC.
- [8] Erazo, M., Calderón, F., Murillo, M. & Ávalos, M. (2020). Educación interactiva: estrategia pedagógica para resignificar la identidad cultural y comprensión lectora de leyendas Riobambeñas. *Revista Indexada Ciencia Digital*. 4(4), 44-64. <https://doi.org/10.33262/cienciadigital.v4i4.1421>
- [9] Feldman, J. (2017). Memorylands: Heritage an Identity in Europe Today. *American Ethnologist*, 44 (1), 145-146. <https://doi.org/10.1111/amet.12434>

- [10] Fontal, O., García, S. & Aso, B. (2020) Desarrollo de competencias docentes en educación patrimonial mediante plataformas 2.0 y entornos digitales como herramienta de aprendizaje. *Prácticas y reflexiones en educación patrimonial*. (101), 1-14. <https://doi.org/10.12795/IE.2020.i101.01>
- [11] Gamonal, R. (2004). David Carson Contra Aristóteles: Análisis retórico del diseño gráfico. *Razón y Palabra*. (37). <http://www.razonypalabra.org.mx/anteriores/n37/rgamonal.html>
- [12] López, M., Solórzano, A. & Pomaquero, M. (2021). CGI al servicio de la cultura: características de los personajes ecuatorianos tradicionales andinos. *Revista Internacional de la Imagen*. 6 (2), 43-57. <https://doi.org/10.18848/2474-5197/CGP/v06i02/43-57>
- [13] Ocaña, P. (2015). La danza indígena y su aporte en la conservación de las tradiciones ancestrales de la provincia de Tungurahua. [Tesis de licenciatura, Universidad Técnica de Ambato]. Repositorio institucional-Universidad Técnica de Ambato. <https://repositorio.uta.edu.ec/handle/123456789/12879>
- [14] Martínez, H., Pinzón, J. & Arango, N. (2017). Divulgación y enseñanza del patrimonio: interpretación de contenidos digitales y las nuevas perspectivas educativas. *Designia*, 5(1), 48-66. <https://doi.org/10.24267/22564004.253>
- [15] Piñeiro-Naval, V., Igartua, J. y Rodríguez de Dios, I. (2018). Implicaciones identitarias en la divulgación del patrimonio cultural a través de Internet: un estudio desde la Teoría del Framing. *Communication & Society*, 31 (1), 1-22. <https://doi.org/10.15581/003.31.1.1-21>
- [16] Rico, L. (2004), La difusión del patrimonio a través de las nuevas tecnologías. Nuevos entornos para la educación patrimonial histórico-artística. Formación de la ciudadanía: Formación de la ciudadanía: las TICs y los nuevos problemas. <https://dialnet.unirioja.es/servlet/articulo?codigo=1448458>
- [17] Sampedro, A., Sariago, R., Martínez, Á., Martínez, R. A. & Rodríguez, B. (2005). Procesos implicados en el desarrollo de Materiales Didácticos reutilizables para el fomento de la Cultura Científica y Tecnológica. *RED. Revista de Educación a Distancia*. (3), 1-15. <https://www.redalyc.org/articulo.oa?id=54709610>
- [18] Scolari, C. (2018). Adolescentes, medios de comunicación y culturas colaborativas. Aprovechando las competencias transmedia de los jóvenes en el aula. (1° ed.) Universitat Pompeu Fabra, pp.78-85
- [19] Secretaría Nacional de Planificación y Desarrollo Senplades. (2017). Plan Nacional para el Buen Vivir 2017-2021. <https://www.gobiernoelectronico.gob.ec/wp-content/uploads/downloads/2017/09/Plan-Nacional-para-el-Buen-Vivir-2017-2021.pdf>
- [20] UNESCO. (2003). Convención para la Salvaguardia del Patrimonio Cultural Inmaterial. <https://ich.unesco.org/es/convencion>



REVISTA PERSPECTIVAS

REVISTA TÉCNICA CIENTÍFICA DE LA FIE

- ELECTROMAGNETISMO Y ÓPTICA APLICADA.
 - AUTOMATIZACIÓN Y CONTROL.
 - SOFTWARE Y APLICACIONES.
- REDES Y COMUNICACIÓN DE DATOS.
 - SISTEMAS ELECTRÓNICOS.
 - INFORMÁTICA EDUCATIVA.
 - SISTEMAS DIGITALES.Ç
 - TELECOMUNICACIONES.
 - DISEÑO GRÁFICO.
 - MECÁNICA
 - TIC'S.



Facultad de
Informática y
Electrónica

<http://perspectivas.esPOCH.edu.ec/>