UNIVERSIDAD PRIVADA DEL NORTE

# FACULTAD DE INGENIERÍA

Carrera de Ingeniería de Sistemas Computacionales

## “ANÁLISIS DE ALGORITMOS DE ENCRIPTACIÓN DE DATOS DE TEXTO, UNA REVISIÓN DE LA LITERATURA CIENTÍFICA”

Trabajo de investigación para optar el grado de:

**Bachiller en Ingeniería de Sistemas Computacionales**


**Autores:**

Henry Alexander Cabanillas Urbina

Juan Jose Victor Nizama Ramos

**Asesor:**

Mg. Ing. Neicer Campos Vásquez


Lima - Perú

2019

## DEDICATORIA

*Está presente investigación está dedicada primeramente a Dios, a mi esposa Cintya por darme siempre el apoyo incondicional estando a mi lado creyendo en mi capacidad y a mi hijo Benjamín por ser mi fuente de inspiración y motivación para superarme cada día para que la vida nos depare un próspero futuro.*

**Henry Alexander Cabanillas Urbina**

*Está presente investigación está dedicada primeramente a Dios por bendecir mi vida y fortalecerme en los momentos de dificultad y de debilidad, a mí mama Lala por confiar siempre en mí, por los consejos y valores que me inculco; a mi esposa Jessica y mi hija Fátima por su cariño y apoyo incondicional; a mis hermanas Carmen y Kimberly; mis sobrinos Juan Martín y Gabriela por ser mi apoyo a la largo de mi vida.*

**Juan José Víctor Nizama Ramos**

## AGRADECIMIENTO

*Agradezco el amor recibido de mis padres y ser promotores de mis sueños, gracias a ellos por cada día confiar, creer en mí y en mis expectativas, gracias a mis suegros y a toda mi familia por su apoyo incondicional.*

*Agradezco a la Universidad Privada del Norte, a los docentes por su ayuda y gran enseñanza, a mis compañeros por la amistad que me han otorgado.*

**Henry Alexander Cabanillas Urbina**

*Al finalizar esta tesis quiero agradecer a Dios por todas las bendiciones que derrama sobre mi familia, a mi mamá por ser un ejemplo a seguir de trabajo y honradez, a toda mi familia por su apoyo y paciencia en este trabajo.*

*De igual manera mi agradecimiento a la Universidad Privada del Norte, a la facultad de Ingeniería - Carrera de Sistemas Computacionales, a mis profesores que con su valiosa enseñanza hicieron que pueda crecer como persona y profesional, a mis compañeros por su apoyo y amistad incondicional.*

**Juan José Víctor Nizama Ramos**

# INDICE

# ÍNDICE DE TABLAS

# ÍNDICE DE FIGURAS

## RESUMEN

Actualmente las instituciones están obligadas a mantener seguras la información, existen diversos mecanismos de protección de la información acorde al avance de la tecnología el cual facilita publicar artículos sobre ciberseguridad. El trabajo de investigación tiene como objetivo determinar el efecto de la encriptación de datos en la ciberseguridad, para lo cual se tomó como población de estudio a todos los artículos científicos publicados en EBSCO, SCOPUS, ELSEVIER, PUBMED, SCIELO y otros. Metodología: el diseño de la estrategia de búsqueda, a partir de la pregunta de investigación estructurada, uso de herramientas como los operadores booleanos, palabras clave, uso de comillas, truncamientos, paréntesis y otros, como: ("encriptación" OR "algoritmos") AND "ciberseguridad". Criterios de elegibilidad fueron estudios publicados con 10 años de antigüedad, que incluyan las palabras claves, artículos que cumplen con los criterios de valoración. Las limitaciones durante el desarrollo del trabajo de investigación fueron la falta de accesibilidad a los artículos en forma gratuita. Resultados: se obtuvo como resultado luego de la aplicación de los criterios de elegibilidad, 20 artículos los cuales formaron parte del análisis de la revisión. Conclusiones: Todos los estudios publicados consideran que es necesario aplicar la criptografía la cual consiste en el uso de la matemática para encriptar y desencriptar datos, se demostró que si es efectivo para mantener la seguridad de la información de datos de las instituciones.

**PALABRAS CLAVES:** encriptación, algoritmos, ciberseguridad

## SUMMARY

Currently, institutions are obliged to keep information secure, there are various mechanisms to protect information according to the advancement of technology, which facilitates the publication of articles on cybersecurity. The objective of the research work is to determine the effect of data encryption in cybersecurity, for which all the scientific articles published in EBSCO, SCOPUS, ELSEVIER, PUBMED, SCIELO and others were taken as a study population. Methodology: the design of the search strategy, based on the question of structured research, use of tools such as boolean operators, keywords, use of quotation marks, truncations, parentheses and others, such as: ("encryption" OR "algorithms" ) AND "cybersecurity". Eligibility criteria were studies published 10 years old that include keywords, articles that meet the assessment criteria. The limitations during the development of the research work were the lack of accessibility to the articles for free. Results: 20 items were obtained as a result of the application of the eligibility criteria, which were part of the analysis of the review. Conclusions: All published studies consider that it is necessary to apply cryptography which consists of the use of mathematics to encrypt and decrypt data, it was shown that it is effective to maintain the security of the data information of the institutions.

**KEY WORDS**: encryption, cybersecurity algorithms

# CAPÍTULO I. INTRODUCCIÓN

En la actualidad con el avance de la tecnología como es el internet, que facilita a las instituciones a utilizarlo para el manejo de la información, ha ocasionado la rapidez en sus procesos, mejorando la gestión y atención hacia los usuarios/clientes, favoreciendo el desarrollo y crecimiento institucional en los aspectos de gestión y económico a nivel mundial.

Los datos que conforman la información de una institución, es de suma importancia, por el cual esta debe ser protegida. Las instituciones públicas y privadas hoy en día tienen la obligación de mantener seguras la información, por ello deben establecer diversos mecanismos de protección de la información.

"Sin importar lo robusto que sea un criptosistema, si un intruso puede robar la clave, el sistema no vale." (Tanenbaum, 2003).

"La información es un activo de considerable valor, único en las organizaciones, debido a esto la importancia de emplear mecanismos que garanticen su seguridad, confiabilidad e integridad. Cada vez son más las exigencias en cuanto a seguridad se refiere por lo tanto es necesario establecer el uso de técnicas criptográficas en servicios de mensajería se trata de resolver que la información solo sea accedida y este visible para las partes interesadas mas no para los demás posibles usuarios." (Álvarez Coello, L. / Anzules Navarro, F., 2017).

Basados en la información brinda en los párrafos anteriores, se nos presenta el siguiente problema. ¿De qué manera podemos asegurar una transmisión segura de datos?

Para esta problemática se recomienda usar la metodología de la encriptación de datos. Para poder encriptar datos de textos comparamos tres procesos matemáticos utilizados con mayor frecuencia; estos son los algoritmos HASH, los simétricos y los asimétricos (RSA).

El algoritmo HASH, cuyo significado en inglés es picar y mezclar; efectúa un cálculo matemático sobre los datos que conforman el documento, dicho cálculo genera un número

único conocido como MAC, un mismo documento siempre genera un mismo MAC. Criptografía de Clave Secreta o Simétrica

Los algoritmos simétricos o la criptografía de clave simétrica, también llamada clave secreta, es un método el cual se utiliza una misma clave tanto para cifrar como para descifrar el documento. En este tipo de algoritmo tanto el emisor como el receptor del documento deben establecer previamente que clave van a utilizar. Se debe recalcar que en este procedimiento la clave viaja adjunta a los datos lo que da un alto índice de riesgo en la operación. Actualmente existen dos métodos de cifrado para criptografía de clave secreta, el cifrado de flujo y el cifrado en bloques.

Los algoritmos asimétricos o criptografía de dos claves es un método que utiliza un par de claves para él envió de un documento; ambas claves son de propiedad del receptor del documento una es publica (Puede ser entregada a cualquier persona) y otra privada (Uso exclusivo del propietario). En este tipo de algoritmos destacan: RSA, Diffie-Hellman, DSA, Cifrado El Gamal, Criptografía de curva elíptica, Criptosistema de Merkle-Hellman, entre otros.

En ese sentido, dada la importancia de la información y de la seguridad de esta el objetivo del presente estudio es investigar los principales algoritmos de encriptación de datos de texto, seleccionar las técnicas adecuadas para la protección de los datos de texto y determinar la eficiencia de las técnicas propuestas en la encriptación de datos de texto.

De acuerdo a lo expuesto surge la siguiente interrogante ¿Cuál son los principales algoritmos de encriptación de datos de texto?

Por ello el trabajo de investigación se organiza de la siguiente manera: la sección II presenta la metodología, la sección III presenta los resultados y en la sección IV se discute, analiza e interpreta los resultados de la revisión sistemática y se informa de los resultados en base al modelo de encriptación de datos como medida de ciberseguridad y finalmente se presenta las conclusiones.

# CAPÍTULO II. METODOLOGÍA

La presente investigación ha sido desarrollada en base a una revisión sistemática de la literatura científica sobre los algoritmos de encriptación de datos de texto. La revisión sistemática trabaja sobre realidades de hecho y su característica fundamental es la de presentar una interpretación correcta.

Un ejemplo muy claro es la idea de donde se basaron Adi Shamir y Leonar Adleman que es esta:

> *"Supongamos que Bob quiere enviar a Alicia un mensaje secreto que solo ella pueda leer. Alicia envía a Bob una caja con una cerradura abierta, de la que solo Alicia tiene la llave. Bob recibe la caja, escribe el mensaje, lo pone en la caja y la cierra con su cerradura (ahora Bob no puede leer el mensaje). Bob envía la caja a Alicia y ella la abre con su llave, En este ejemplo, la caja con la cerradura es la* ***clave pública*** *de Alicia, y la llave de la cerradura en su* ***clave privada****".*

El presente trabajo constituye una investigación de tipo Observacional, Descriptivo, Retrospectivo y Transversal. Se realizó una revisión sistemática sobre la eficacia de la encriptación de datos en la ciberseguridad, según las recomendaciones establecidas por Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA)[50].

La revisión sistemática comprendió las siguientes actividades: Identificación del problema a investigar, formulación de la pregunta estructurada de investigación, protocolo de revisión, análisis e interpretación de los resultados y conclusiones.

## 1. Identificación del problema a investigar:

Hoy en día la seguridad de la información es cada vez un tema de mayor importancia en la tecnología, para las grandes, medianas, y pequeñas empresas, también para los usuarios, debido a que existen mecanismos sofisticados no permitiditos, que vulneran la seguridad y acceden a la información poniéndolo en riesgo, para darle otros fines.

La ciberseguridad es la encargada de evitar todo tipo de amenazas, las cuales ponen en riesgo la información que es procesada, transportada y almacenada en cualquier dispositivo. La encriptación de datos o cifrado de archivos es un procedimiento de seguridad mediante el cual la información se mantiene protegida.

## 2. Formulación de la pregunta estructurada de investigación

La información ¿Cuál será la efectividad de la encriptación de datos en la ciberseguridad?, ¿Cuál son los principales algoritmos de encriptación de datos de texto?

**Población:** Está constituida por las publicaciones de artículos científicos resultado de trabajos de investigación sobre el efecto de los principales algoritmos de encriptación de datos de texto en la ciberseguridad.

**Intervención:** El modelo de la encriptación de datos, utilizado para la seguridad de la información.

**Comparación:** Diferentes modelos, utilizados para la seguridad de la información.

**Efecto:** Efectividad en la ciberseguridad.

## 3. Protocolo de Revisión:

- **Identificación de las fuentes de información:** Se estableció las fuentes de información donde se realizaron la búsqueda (EBSCO, SCOPUS, ELSEVIER, PUBMED, SCIELO y otros.

  En las fuentes de información para la búsqueda se tuvo las siguientes consideraciones:

  - ✓ Que incluyan artículos enfocados en modelo de la encriptación de datos en ciberseguridad, sistemas de gestión de seguridad de la información, modelos en ciberseguridad en las organizaciones institucionales.
  - ✓ Fuentes de información que cuenten con mecanismos de búsqueda avanzada, utilizando las palabras claves y sinónimos usados en las preguntas de investigación estructurada.
  - ✓ Artículos disponibles en la Web de forma gratuita.

- ✓ Artículos en idiomas inglés o español.

- **Estrategia de Búsqueda:** Como estrategias de búsqueda, a partir de la pregunta de investigación estructurada, se seleccionó las palabras claves: encriptación de datos, algoritmos de encriptación de datos, ciberseguridad. Efectividad. Los operadores booleanos usados son AND, OR, NOT, conjugados con las palabras clave y uso de comillas, truncamientos, paréntesis y otros.
- Los operadores booleanos usados son AND, OR, NOT, conjugados con las palabras clave y uso de comillas, truncamientos, paréntesis y otros.
  - ✓ "algoritmos de encriptación de datos" AND "ciberseguridad"
  - ✓ ("encriptación" OR "algoritmos") AND "ciberseguridad"
  - ✓ Encriptación AND "ciberseguridad" AND "efectividad"

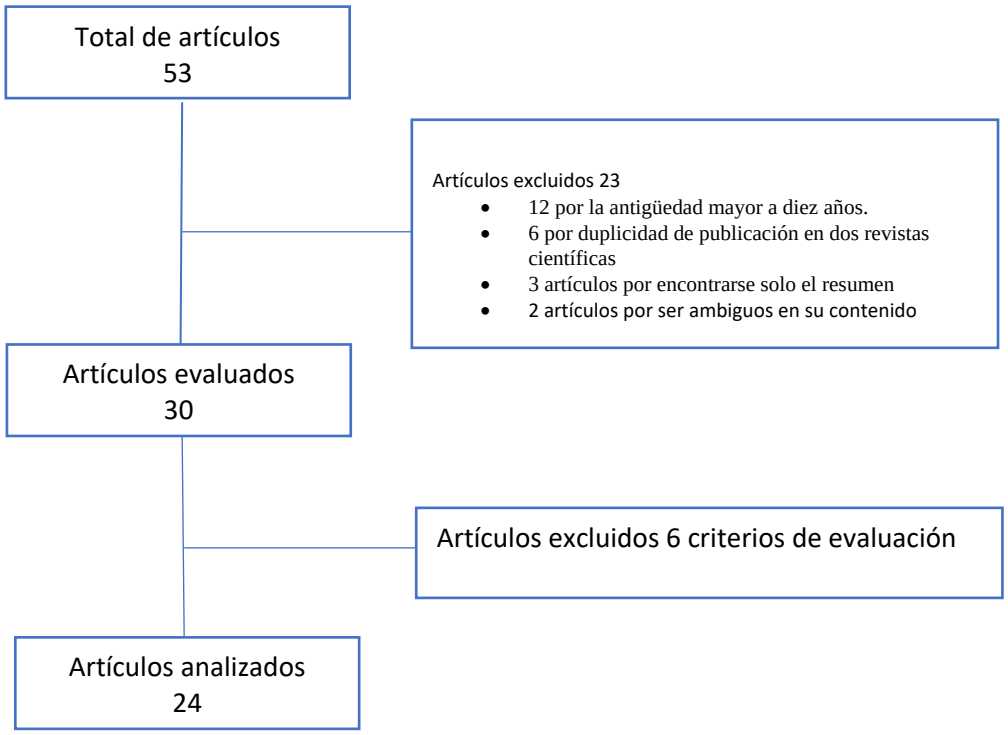
  Además se tuvo en cuenta las palabras claves en el idioma del inglés para la búsqueda, a fin de cubrir la mayor cantidad de artículos como resultados de la búsqueda.

  - ✓ "data encryption" AND "cybersecurity".
  - ✓ "data encryption algorithms" AND "cybersecurity"
  - ✓ ("encryption" OR "algorithms") AND "cybersecurity"
  - ✓ Encryption AND "cybersecurity" AND "effectiveness"
- **Recuperación y Revisión de la información:** Los artículos científicos localizados y recuperados de acuerdo a la estrategia de búsqueda, se revisaron de acuerdo a los criterios de inclusión y exclusión,
- **Criterios de Inclusión:** Estudios publicados con 10 años de antigüedad, que incluyan las palabras claves (Encriptación de datos, algoritmos de encriptación de datos, ciberseguridad, efectividad), Artículos que cumplen con los criterios de valoración.
- **Criterios de Exclusión:** Artículos con más de 10 años de antigüedad, que no contemplan las palabras claves, estudios muy cortos e incompletos que presentan ambigüedad publicaciones duplicadas.

# CAPÍTULO III. RESULTADOS

Al realizar la búsqueda de artículos científicos publicados en las fuentes de información, utilizando las palabras claves, estrategias de búsqueda, se tuvo como resultado una población de 53 artículos científicos relacionados al tema de investigación, de los cuales, aplicando los criterios de inclusión, se excluyeron a 23 artículos: 12 por la antigüedad mayor a diez años, 6 por duplicidad de publicación en dos revistas científicas, 3 artículos por encontrarse solo el resumen, 2 artículos por ser ambiguos en su contenido, y 6 por criterios de evaluación.

**Figura N° 1**. *Total de Estudios obtenidos con las palabras claves*




**Fuente:** propia del investigador

En la siguiente fase, después de revisar cada uno de los estudios tomando en consideración los criterios de inclusión y exclusión citados, obteniendo un total de 30 estudios relevantes. Para seleccionar los estudios relevantes, se siguieron los siguientes pasos:

- **Lectura del título.** Si el articulo proporciona suficiente información del tema, el estudio fue seleccionado y guardado. Si no se le excluyó

- **Lectura del resumen del artículo**. Si el articulo proporciona suficiente información del tema, el estudio fue seleccionado y guardado. Si no se le excluyó
- **Lectura de las conclusiones**. Si el articulo proporciona suficiente información del tema, el estudio fue seleccionado y guardado. Si no se le excluyó, se obtuvieron 24 artículos científicos que respondían a las preguntas de investigación formulad. Ver la Tabla N°1.

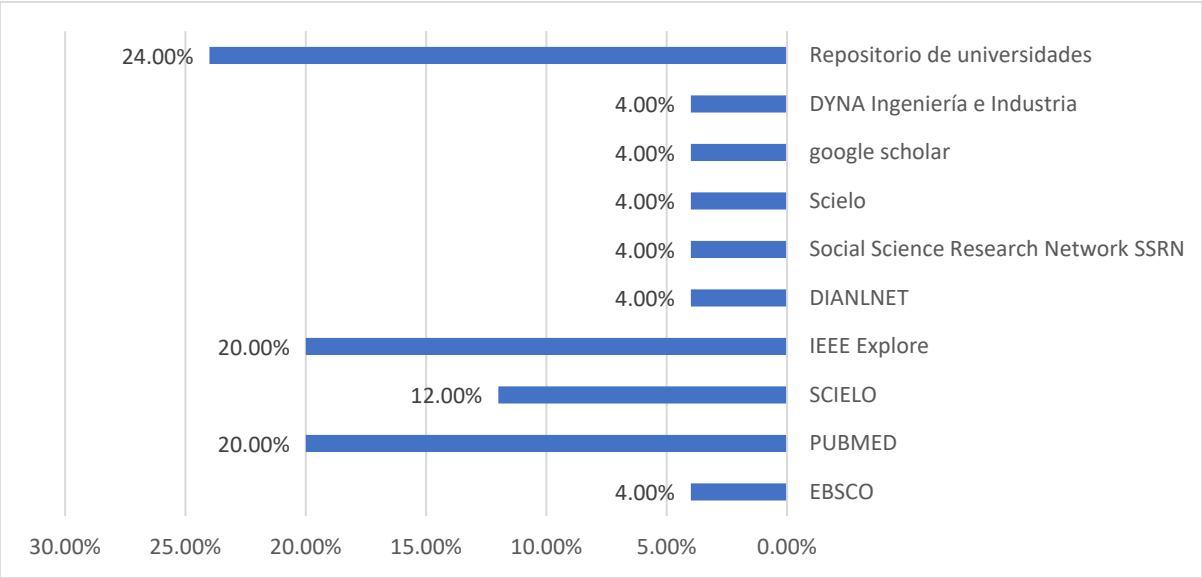
**Tabla N° 1.** *Distribución de los Estudios por Fuente de Información*

| FUENTE DE INFORMACIÓN | INFORMACIÓN SELECCIONADA | PORCENTAJE |
|---|---|---|
| EBSCO | 1 | 4.00% |
| PUBMED | 5 | 20.00% |
| SCIELO | 3 | 12.00% |
| IEEE Explore | 5 | 20.00% |
| DIANLNET | 1 | 4.00% |
| Social Science Research Network SSRN | 1 | 4.00% |
| Scielo | 1 | 4.00% |
| Google scholar | 1 | 4.00% |
| DYNA Ingeniería e Industria | 1 | 4.00% |
| Repositorio de universidades | 6 | 24.00% |
| **TOTAL** | **25** | **100%** |

**Fuente:** propia del investigador

De la tabla 1 se observa que los estudios publicados fueron el de mayor porcentaje (25%) en los repositorios institucionales de las universidades, seguidos de la fuente de búsqueda en Pubmed con el 20.83 % seguido del IEE explore (16.67%).

**Figura 2.** *Distribución de los estudios por fuente de información.*




**Fuente:** propia del investigador

De la tabla N°1 y Figura 2 se observa que los estudios publicados fueron el de mayor porcentaje (24%) en los repositorios institucionales de las universidades, seguidos de la fuente de búsqueda en Pubmed y IEE explore con el 20 %.

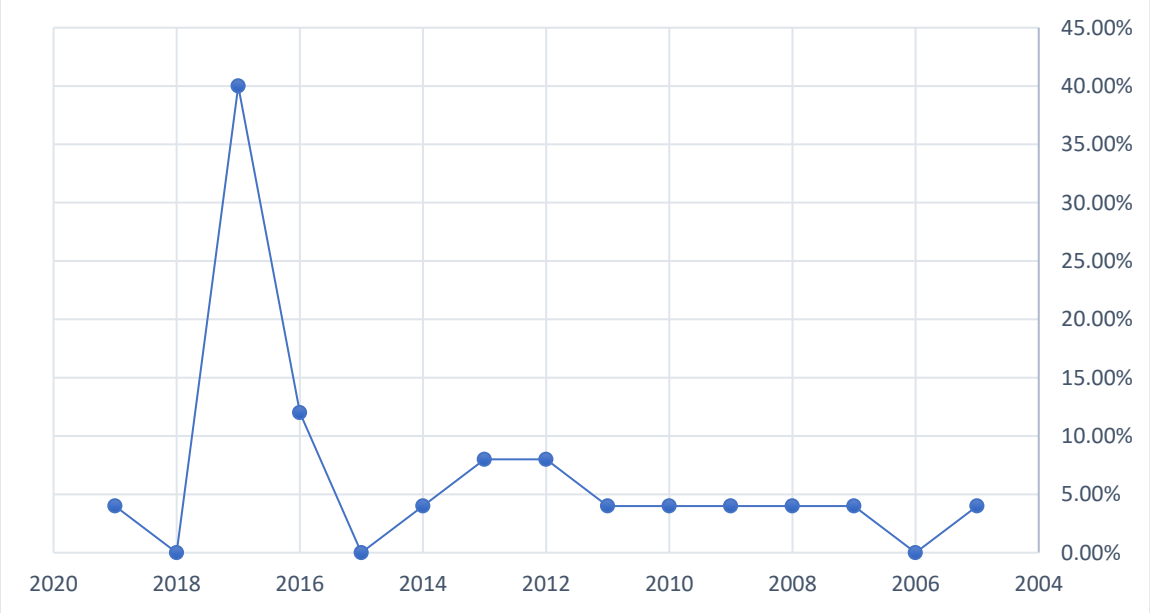
**Tabla N° 2.** *Distribución de los Estudios por Año de Publicación*

| AÑO DE PUBLICACIÓN | CANTIDAD | PORCENTAJE |
|---|---|---|
| 2005 | 1 | 4.00% |
| 2006 | 0 | 0.00% |
| 2007 | 1 | 4.00% |
| 2008 | 1 | 4.00% |
| 2009 | 1 | 4.00% |
| 2010 | 1 | 4.00% |
| 2011 | 1 | 4.00% |
| 2012 | 2 | 8.00% |
| 2013 | 2 | 8.00% |
| 2014 | 1 | 4.00% |
| 2015 | 0 | 0.00% |
| 2016 | 3 | 12.00% |
| 2017 | 10 | 40.00% |
| 2018 | 0 | 0.00% |
| 2019 | 1 | 4.00% |
| **TOTAL** | **25** | **100%** |

**Fuente:** propia del investigador

De la tabla N°2 y Figura 3 se observa que los estudios publicados por año fueron de mayor porcentaje en el 2017 con 40% seguido del 2016 con 12%. Siendo 0% en los años 2006, 2015 y 2018.

**Figura N° 3.** *Distribución de los Estudios por Año de Publicación*



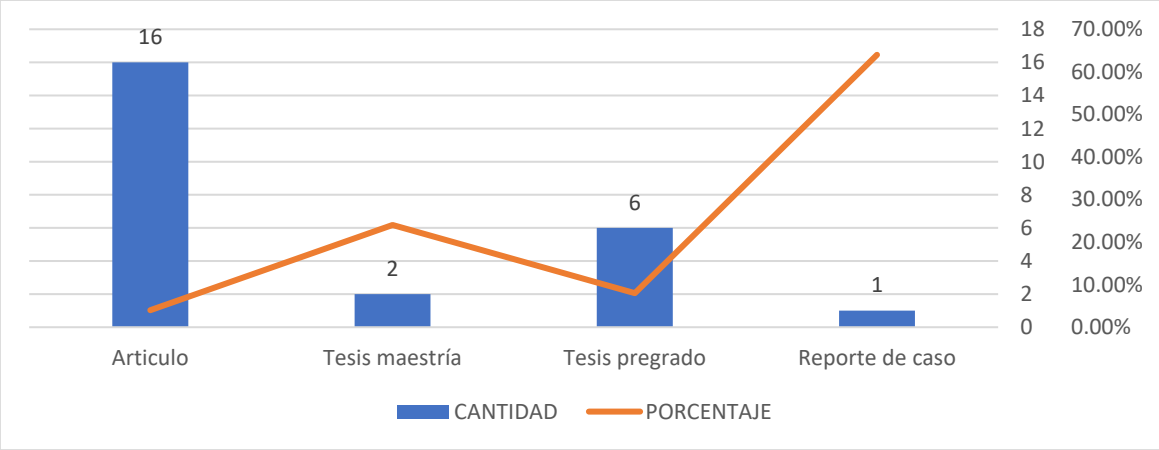

**Fuente:** propia del investigador

**Tabla N° 3.** *Distribución de los Estudios por tipo*

| TIPO DE ESTUDIO | CANTIDAD | PORCENTAJE |
|---|---|---|
| Reporte de caso | 1 | 4.00% |
| Tesis pregrado | 6 | 24.00% |
| Tesis maestría | 2 | 8.00% |
| Articulo | 16 | 64.00% |
| **TOTAL** | **25** | **100%** |

**Fuente**: propia del investigador

**Figura N°4.** Distribución de los Estudios por tipo




**Fuente:** propia del investigador

De la tabla N°3 y Figura 4 se observa que los estudios publicados según el tipo fueron el de mayor porcentaje los artículos con el 64%, seguido de las tesis de pregrado.

**Extracción de datos y síntesis**

En la presente revisión sistemática se realizó, la lectura de cada artículo encontrado y se extrajo la información importante sobre el tema, se diseñó un formulario. El formato contiene los siguientes campos: Autores, Titulo, Año, link, Abstract.

Por cada artículo seleccionado, después de leerse el texto completo, se procedió a registrar la información en el formato, el cual permitió realizar el análisis posterior de los resultados.

(Ver tabla N° 4)

**Tabla N° 4.** *Estudios Clasificados para la Revisión Sistemática*

| N° | AUTORES | TÍTULO | AÑO | DISEÑO DEL ESTUDIO | FUENTE |
|---|---|---|---|---|---|
| **1** | Álvarez Coello Lidia Alejandrina Anzules Navarro Félix Samuel | Diseño de una aplicación segura de mensajería web interna utilizando el algoritmo de encriptación RSA para la Carrera De Ingeniería en Networking & Telecomunicaciones, año 2017. | 2017 | Tesis Pregrado | Repositorio Universidad de Guayaquil |
| **2** | Guillermo Mejía Díaz, Edwin Enrique Viche Rivas | Algoritmo para mostrar el proceso de encriptación y desencriptación de datos en PHP. Una aplicación de seguridad informática. | 2017 | Artículo | Scielo |
| **3** | Sheilla Etty Gomez Fernandez | Criptografía y Seguridad en Computadores | 2007 | Tesis pregrado | Repositorio de la Universidad Nacional de Ingeniería |
| **4** | Julio César Mendoza T. Ingeniería de Sistemas – Quito | Demostración de cifrado simétrico y asimétrico | 2008 | Artículo | Red de repositorios de acceso abierto del Ecuador |
| **5** | Ian Carlo Guzmán, Rubén Darío Nieto & Álvaro Bernal | Implementación en FPGA del algoritmo AES-128 en modos de operación no realimentados | 2016 | Artículo | DYNA SCIELO |
| **6** | José Moreno, Fabio Parra, Rafael Huérfano, Cesar Suarez, Isabel Amaya | Modelo de Encriptación Simétrica Basada en Atractores Caóticos | 2016 | Reporte de caso | SCIELO |
| **7** | Katia Regina León Lomparte | Rencriptacion RSA de archivos de texto | 2005 | Tesis Maestría | Repositorio PUCP |

| | | | | | |
|---|---|---|---|---|---|
| **8** | Álvarez Coello Lidia Alejandrina. Anzules Navarro Félix Samuel. | Diseño De Una Aplicación Segura De Mensajería Web Interna Utilizando El Algoritmo De Encriptación Rsa Para La Carrera De Ingeniería En Networking & Telecomunicaciones, Año 2017 | 2017 | Tesis pregrado | GOOGLE SCHOLAR |
| **9** | López Mendoza Roxana Mercedes Mesías Meza Luis Enrique | Simulación De Un Sistema Transaccional Mediante. Un Canal Seguro, Usando Criptografía | 2017 | Tesis pregrado | Repositorio de la Universidad De Guayaquil |
| **10** | Jhonny Antonio Pabón Cadavid | The cryptography and the protection of digital information | 2012 | Artículo | Social Science Research Network SSRN |
| **11** | Lil María Xibai Rodríguez Henríquez | Esquema de cifrado para la ejecución de consultas en bases de datos cifradas | 2009 | tesis maestría | Repositorio del instituto politécnico nacional |
| **12** | Iv´anFelipeRodr´ıguez1, EdilmaIsabel Amaya∗1,C´esarAugustoSu´arez1, Jos´eDavidMoreno1 | Algoritmo de Encriptación de Imágenes Utilizando el Atractor Caótico de Lorenz | 2017 | Artículo | Revista de ingeniería. DIALNET |
| **13** | Chun Kiat Tan,1 Jason Changwei Ng,1 Xiaotian Xu,1 Chueh Loo Poh,2 Yong Liang Guan,1 and Kenneth Sheah3 | Security Protection of DICOM Medical Images Using Dual-Layer Reversible Watermarking with Tamper Detection Capability | 2010 | Artículo | Pubmed |
| **14** | Whye Kit Tan 1, Sang-Gon Lee 1,*, Jun Huy Lam 1 and Seong-Moo Yoo 2 | A Security Analysis of the 802.11s Wireless Mesh Network Routing Protocol and Its Secure Routing Protocols | 2013 | Artículo | Pubmed |
| **15** | Mantos PL[1], Maglogiannis I[2]. | Sensitive Patient Data Hiding using a ROI Reversible Steganography Scheme for DICOM Images. | 2016 | Artículo | Pubmed |

| | | | | | |
|---|---|---|---|---|---|
| **16** | Danielle Kriz | Cybersecurity Principles for Industry and Government A Useful Framework for Efforts Globally to Improve Cybersecurity | 2012 | Artículo | Pubmed |
| **17** | Regner Sabillon ; Jordi Serra-Ruiz ; Victor Cavaller ; Jeimy Cano | A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM) | 2017 | Artículo | IEEE xplore |
| **18** | Danielle Kriz | Cybersecurity principles for industry and government: A useful framework for efforts globally to improve cybersecurity | 2011 | Artículo | IEEE xplore |
| **19** | Paresh Rathod ; Timo Hämäläinen | A Novel Model for Cybersecurity Economics and Analysis | 2017 | Artículo | IEEE xplore |
| **20** | Gloria D'Anna | CHAPTER 5 Engineering for Vehicle Cybersecurity by Daniel DiMase, Zachary A. Collier, John A. Chandy, Bronn Pav, Kenneth Heffner, and Steve Walters | 2019 | Artículo | IEEE xplore |
| **21** | Tan WK1, Lee SG, Lam JH, Yoo SM. | A security analysis of the 802.11s wireless mesh network routing protocol and its secure routing protocols | 2013 | Artículo | Pubmed |
| **22** | Walker, Alastair | Cybersecurity in safety-critical systems DOI: 10.1002/smr.1956 | 2017 | Artículo | EBSCO |
| **23** | Kiminao Kogiso ; Takahiro Fujita | Cyber-Security Enhancement of Networked Control Systems Using Homomorphic Encryption DOI: 10.1109/CDC.2015.7403296 | 2017 | Artículo | IEEE xplore |
| **24** | Ríos Taipe, Josue Wenceslao | Sistema de encriptación para optimizar el proceso de Desarrollo de software de una empresa de lima | 2017 | Tesis pregrado | alicia.concytec.gob.pe |
| **25** | María De Los Ángeles Valle C | Análisis de métodos criptográficos para la gestión de firmas y Certificados digitales dentro de un contexto de supervisión (SBS) Para enfrentar los nuevos requerimientos de seguridad Informática | 2014 | Tesis Pregrado | Repositorio de tesis de grado y posgrado Pontificia Universidad católica ecuador. |

**Fuente:** propia del investigador

El resultado de la revisión sistemática de los estudios:

1. **Algoritmo para mostrar el proceso de encriptación y desencriptación de datos en PHP. Una aplicación de seguridad informática:**

   En este artículo, Se muestra el proceso de encriptamiento a través de la elaboración de un algoritmo para exponer el funcionamiento básico encriptar y desencriptar. Y como aporte adicional se presenta la historia de los algoritmos y una comparación de los más usados en la actualidad. También se presentan las técnicas usadas en criptografía para garantizar la seguridad informática se incluye el uso de CryptoForge para el sistema operativo Windows que cumple este propósito de encriptar y desencriptar.

2. **Análisis de la Seguridad de la Información**: Los autores concluyen que la seguridad de las redes de comunicaciones, y concretamente de Internet, evoluciona a pasos agigantados cada minuto que transcurre. Nuevas vulnerabilidades y utilidades, tanto para explotarlas como para combatirlas, son distribuidas públicamente en la red. La información disponible al respecto es inmanejable, por lo que el diseño de un sistema de seguridad debe basarse en la fortaleza de las tecnologías empleadas, y no en la ocultación de las mismas: "security through obscurity".

   El protocolo TCP/IP sufre algunos problemas de seguridad por las características intrínsecas de su diseño, los cuales han sido ampliamente analizados a lo largo de los últimos años. La nueva versión de IP, versión 6, se diseñó con la seguridad en mente, de ahí la aparición del estándar IPSec, que junto a otras tecnologías, como las infraestructuras de clave pública, PKls, permiten controlan y disolver muchas de las vulnerabilidades presentadas a lo largo del presente trabajo.

   Algoritmos más utilizados

   Asimismo, concluyen que la seguridad de una red no se basa en una única técnica. exclusivamente, como promulga la idea errónea de securizar una red mediante un firewall, sino que viene reforzada por la utilización de multitud de tecnologías que permiten monitorizar y gestionar cada uno de los aspectos críticos de la red: encriptación, IDSs, firewalls, software específico de seguridad, protocolos seguros (SSL, SSH, IPSec), PKls

Finalmente, concluye con una reflexión al respecto de la seguridad: el esfuerzo dedicado a la protección de un entorno debe ser directamente proporcional al valor de su contenido. Debido a que toda vulnerabilidad posee, más tarde o más temprano, su correspondiente protección, la vertiginosa carrera en la que la seguridad de las redes se debate actualmente, se centra en el mantenimiento constante y actualizado de las protecciones necesarias para evitar las vulnerabilidades existentes y ya conocidas.

Resguardar la información siempre ha sido uno de los elementos de estudio más importantes a través de los años, con los sistemas de información actuales hoy en día se vuelve parte esencial de los sistemas informáticos de empresas u organizaciones a nivel mundial. Siendo los elementos la confidencialidad, la disponibilidad e integridad y no repudio las que hacen el estado de seguro a la información. La criptografía se ha encargado de encontrar de formular el algoritmo criptográfico más seguro desde sus inicios comenzando por simples desplazamientos de letras del alfabeto hasta la actualidad siendo los algoritmos simétricos y asimétricos la clasificación actual teniéndose métodos con posibilidades de proporcionar claves de hasta 256 bits y múltiples iteraciones para encriptar información siendo la combinación de múltiples algoritmos criptográficos la mejor opción en cuanto al resguardo de información. La construcción de un algoritmo criptográfico propio para encriptar mensajes es una alternativa a los métodos sofisticados dando a la creatividad del autor del algoritmo las pautas a la creación de métodos básicos pero que mantienen la esencia de resguardar información con una clave, como el que se presentó en este artículo que toma el código ASCII para encriptar mensajes siendo un algoritmo sencillo que se puede mejorar incluyéndose un canal de transmisión de la clave al receptor así como el mensaje encriptado sea una sola cadena y no segmentado se puede incluir además una característica de los algoritmos criptográficos actuales que es el número de iteraciones para encriptar mensajes, así también se puede hacer una mejora sustancial para que además del código ASCII se convine con otros conjuntos de codificadores de caracteres como ISO/IEC 8859 que es un estándar para caracteres de 8 bits en computadoras. Logrando así una mayor eficiencia en el texto encriptado.

3. **Diseño de una aplicación segura de mensajería web interna utilizando el algoritmo de encriptación RSA para la Carrera De Ingeniería en Networking & Telecomunicaciones, año 2017:** El proyecto basa su importancia del diseño de una mensajería web segura que permitirá que los docentes y administrativos de la carrera de Ingeniería en Sistemas Computacionales y la carrera de Ingeniería en Networking y Telecomunicaciones de la Universidad de Guayaquil puedan contar con una herramienta que facilite la oportuna toma de decisiones. Se realizó una investigación sobre los servicios, funcionamiento, requerimientos y beneficios de tener una aplicación de mensajería web interna utilizando el algoritmo de encriptación RSA que puedan prevenir y contrarrestar posibles ataques, proporcionando la confidencialidad e integridad de los datos. La modalidad de investigación es descriptiva y exploratoria por cuándo permitió una mejor compresión del problema, así mismo la población establecida fue de 183 personas entre docentes y administrativos que reflejó una muestra estadística de 111 profesionales de los cuales se pudo obtener información mediante la utilización de un cuestionario de 10 preguntas. Las variables determinadas fueron control de envío, recepción y seguridad de la información y baja adaptabilidad de la mensajería web que ayudarán a un mejor desenvolviendo de los tramites y procesos institucionales además de brindar seguridad y confidencialidad. Se concluye proponiendo una mensajería web que ofrezca confianza a los docentes y administrativos de la institución al momento de enviar y recibir cualquier tipo de información, así como contar con opciones que faciliten la comunicación.

4. **Demostración de cifrado simétrico y asimétrico:** En el presente artículo se presenta una breve introducción a la criptografía sin profundizar en las matemáticas que soportan los algoritmos criptográficos; simplemente se abordará al cifrado a un nivel muy básico, para mostrar una visión de los distintos tipos (simétricos y asimétricos) y realizar una demostración de cifrado aplicando ambas técnicas mediante la aplicación del algoritmo RSA y 3DES en Visual Basic.NET. El propósito de éste artículo es mostrar técnicas sencillas, fáciles de integrar en aplicaciones y que tengan un impacto mínimo en la facilidad de empleo. concluye

   El cifrado simétrico es una eficaz táctica de almacenamiento de información sensible en una base de datos, un registro o archivo El cifrado asimétrico se lo emplea muy

frecuente para pasar con seguridad una clave privada, que posteriormente, será la que se utilice para cifrar y/o descifrar otra información.

"Suele ser un error muy frecuente pensar que los algoritmos de cifrado deben ser secretos para resultar seguros. Los algoritmos de cifrados utilizados son de dominio público y el código fuente asociado también. Sin embargo, siguen siendo seguros porque requieren que el usuario proporcione la clave secreta.

5. **Symmetric Encryption Model Based on Chaotic Attractors:** El aumento en la capacidad de procesamiento de las máquinas y los desarrollos en los algoritmos de búsqueda combinatoria disminuyen el tiempo necesario para descifrar fraudulentamente la información; por esta razón se plantea la necesidad de generar nuevas formas de codificar la información para su transmisión segura.

   Método: En este artículo se presenta un modelo de encriptación simétrico extensible para comunicaciones digitales, aprovechando el caos generado por sistemas dinámicos no lineales. Resultados: El modelo desarrollado demostró estar en la capacidad de encriptar mensajes en tiempos de sincronización, encriptación y desencriptación inferiores a 1 ms con una entropía superior a 6 usando el atractor de Rossler para su implementación. Conclusiones: El algoritmo se presenta como una alternativa a los algoritmos tradicionales de combinatoria demostrando una mayor eficiencia en la gestión de recursos computacionales y plantea las bases para su continuar con su estudio en la comunidad académica interesada, debido a la variedad de los sistemas dinámicos no lineales.

6. **Simulación de un Sistema Transaccional Mediante. Un Canal Seguro, Usando Criptografía RSA.** Mejorar la seguridad en las transacciones electrónicas es una temática que cada vez interesa más a los usuarios, ya que durante el proceso de este tipo de transacciones desean estar protegidos en todo momento, en especial cuando el pago se lo realiza a través de tarjeta de crédito o débito ya que desean tener la seguridad de que estos no se vean comprometidos por posibles malos manejos como lo son las compras no autorizadas. En este sentido reforzar la seguridad con técnicas de encriptación avanzada es vital para las empresas que ofrecen sus productos online, por lo que el presente trabajo hace un estudio de la encriptación RSA y una simulación de su funcionamiento en el ámbito de las compras online.

7. **FPGA implementation of the AES-128 algorithm in non-feedback modes of operation:** En este artículo, presentamos una implementación hardware segmentada del algoritmo AES-128 en modos de operación no realimentados (ECB, CTR). La arquitectura fue implementada en la FPGA Virtex 5 de Xilinx. Dos modos de operación (ECB, CTR) para encriptación y desencriptación de acuerdo a uso de recursos, rendimiento y seguridad fueron comparados. Una frecuencia de reloj de 272.59Mhz para el proceso de encriptación ECB fue obtenida, la cual es equivalente a un rendimiento de 34.89 Gb/s. Además, una frecuencia de reloj de 199.48Mhz para el proceso de desencriptación, equivalente a un rendimiento de 25.5Gb/s fue obtenido. En el modo CTR, una frecuencia de reloj de 272.59Mhz. equivalente a un rendimiento de 34.89Gb/s fue obtenido.

8. **Parallelizing fully homomorphic encryption for a cloud environment:** La computación en la nube es una bendición para el uso comercial y privado, pero los problemas de seguridad de los datos retrasan su adopción. El cifrado totalmente homomórfico (FHE, por sus siglas en inglés) ofrece los medios por los cuales la computación en la nube se puede realizar con datos encriptados, obviando los problemas de seguridad de los datos. FHE no está exento de costos, ya que las operaciones de FHE requieren órdenes de magnitud más tiempo de procesamiento y memoria que las mismas operaciones en datos sin cifrar. La computación en la nube se puede aprovechar para reducir el tiempo que lleva llevar a cabo el procesamiento paralelo. Este documento presenta una implementación de un despachador de procesamiento que toma un conjunto iterativo de operaciones en datos cifrados FHE y los divide entre varios motores de procesamiento. Se implementó una nube privada para soportar los motores de procesamiento. El tiempo de procesamiento se midió con 1, 2, 4 y 8 motores de procesamiento. Se presenta el tiempo necesario para realizar los cálculos con los cuatro niveles de paralelización, así como la cantidad de tiempo utilizado en las transferencias de datos. Además, se presenta el tiempo que los servidores de computación dedicaron a cada suma, resta, multiplicación y división. Se presenta un análisis del tiempo ganado por el procesamiento paralelo. Los resultados experimentales muestran que el procesamiento paralelo propuesto del cifrado de Gentry mejora el rendimiento mejor que los cálculos en un solo nodo. Esta investigación proporciona las siguientes contribuciones. Se construyó una nube

privada para admitir el procesamiento paralelo de cifrado homomórfico en la nube. Se creó un modelo cliente-servidor para evaluar la computación en la nube del algoritmo de cifrado de Gentry. Se desarrolló un algoritmo distribuido para admitir el procesamiento paralelo del algoritmo de Gentry para la evaluación en la nube. Se configuró un experimento para la evaluación del algoritmo de Gentry, y los resultados de la evaluación muestran que el algoritmo distribuido se puede utilizar para acelerar el procesamiento del algoritmo de Gentry con la computación en la nube.

9. **The cryptography and the protection of digital information**. En este artículo el autor presenta un interesante estudio, desde un enfoque técnico-legal, sobre la criptografía, técnica utilizada para cifrar mensajes que contienen información, comenzando por su evolución a lo largo de la historia, y planteando las funciones de la criptografía en el ambiente digital, dentro del cual tiene una utilidad sumamente importante en el contexto de la evidencia digital. Luego de exponer las restricciones al uso de la criptografía y los fuertes controles que varios países han impuesto a la exportación, importación y uso doméstico de herramientas criptográficas, el autor resalta la ausencia de regulación sobre la criptografía en Colombia y plantea la necesidad de que se establezca una política estatal sobre esta disciplina, formulando los asuntos que deben ser considerados como prioridad dentro de esta política pública. La implementación de algoritmos criptográficos en el desarrollo de software es vital, y definitivamente se debe buscar la implementación de algoritmos fuertes, si se desea crear y consolidar una industria de creación de software fuerte, tal como ha sucedido en economías emergentes en este sector, como India o Corea: es necesario contar con tales algoritmos, además de realizar una discusión política sobre la conveniencia o no de la protección legal de los mismos**.**

10. **Esquema de cifrado para la ejecución de consultas en bases de datos cifradas:** Este trabajo propone un esquema de cifrado que permite realizar consulta en bases de datos cifradas de forma eficiente; estas consultas pueden involucrar funciones de agregación, evaluación de rangos y condiciones alfanuméricas. La principal aportación de esta investigación es proporcionar un esquema de cifrado lo suficientemente robusto como para mantener la funcionalidad de una base de datos relacional en claro; cubriendo el servicio de confidencialidad y haciéndolo ideal para ser utilizado en el contexto de bases de datos

subcontratadas. Esta aseveración tiene fundamento en el levantamiento de las operaciones que es posible realizar en una base de datos, para lo cual tomamos de referencia la documentación de Postgresql [33]. Con esta información se construyó la tabla 7.1 donde se muestran las diferentes operaciones y cuáles de ellas son soportadas por el esquema. Para mayor comprensión de las operaciones mostradas en la tabla, consulte el apéndice C. Ésta es una aportación importante debido a que aun cuando existen múltiples propuestas para la ejecución de consultas en bases de datos cifradas, la mayoría únicamente se concentra en un tipo específico de consulta. Para evaluar el esquema se realizó una implementación de los algoritmos que lo cons tituyen: el cifrado basado en homomorfismos de Paillier con lo que se resuelve la operación de agregación SUM, el cifrado de preservación de orden que hace posible la evaluación de rangos y otras operaciones como MIN, MAX (también de agregación); el cifrado de AES-128 para restricciones alfanuméricas y el poder mantener la cualidad de que la base sea relacional. Todas estas primitivas criptograficas se implementaron en C, permitiendo que la multiprecisión requerida por algunas variables y ciertas operaciones de la aritmética fueran resueltas utilizando las funciones que incluye la biblioteca gmp.

11. **A security analysis of the 802.11s wireless mesh network routing protocol and its secure routing protocols.** Las redes de malla inalámbricas (WMN) pueden actuar como una red troncal escalable conectando redes de sensores independientes e incluso conectando WMN a una red cableada. El Protocolo de malla inalámbrico híbrido (HWMP) es el protocolo de enrutamiento predeterminado para el WMN 802.11s. El protocolo de enrutamiento es una de las partes más importantes de la red y requiere protección, especialmente en el entorno inalámbrico. Los protocolos de seguridad existentes, como el Protocolo de Integridad de Transmisión (BIP), el Contador con cifrado de bloque de encadenamiento del mensaje, el Código de autenticación del Protocolo (CCMP), el Protocolo de malla inalámbrico híbrido seguro (SHWMP), la Criptografía basada en la identidad HWMP (IBC-HWMP), la curva elíptica digitalEl algoritmo de firma HWMP (ECDSA-HWMP) y Watchdog-HWMP tienen como objetivo proteger las tramas HWMP. En este documento, hemos analizado las vulnerabilidades del HWMP y hemos desarrollado requisitos de seguridad para proteger estas vulnerabilidades identificadas. Aplicamos los requisitos de seguridad para analizar los esquemas de seguridad existentes para HWMP. Los resultados de nuestro análisis indican que ninguno de estos protocolos es capaz de satisfacer todos los requisitos de seguridad. También presentamos una comparación de complejidad cuantitativa entre los protocolos y un ejemplo de un esquema de seguridad para HWMP para demostrar cómo se puede utilizar

el resultado de nuestra investigación. Nuestros resultados de investigación proporcionan una herramienta para diseñar esquemas seguros para el HWMP.

12. **Sensitive Patient Data Hiding using a ROI Reversible Steganography Scheme for DICOM Images**: El intercambio de imágenes médicas a través de Internet ha suscitado un gran interés en los últimos años debido a la introducción de sistemas de información médica basados en la web y en la nube. La protección de datos confidenciales siempre ha sido un indicador clave en el rendimiento de dichos sistemas. En este contexto, este trabajo presenta un algoritmo desarrollado para imágenes médicas de imágenes digitales y comunicaciones en medicina (DICOM), que aplica métodos de esteganografía de intercambio secreto para garantizar la integridad de los datos confidenciales del paciente y las partes importantes de la imagen. En el algoritmo propuesto, las imágenes se dividen en dos partes: la región de interés (ROI) y la región de no interés (RONI). Los datos del paciente y los hashes de integridad se colocan dentro del ROI, mientras que la información (mapa) necesaria para recuperar el ROI antes de la inserción se coloca en el RONI. La seguridad del proceso de extracción está asegurada a través del uso de la criptografía. Los resultados experimentales demuestran que las imágenes originales (de portada) y las imágenes de stego proporcionan un excelente resultado de igualdad visual en términos de PSNR. Además, demuestran que el esquema propuesto se puede usar de manera eficiente como un esquema de esteganografía en imágenes DICOM con áreas suaves limitadas.

13. **Masking the energy behaviour of encryption algorithms:** Las tarjetas inteligentes son vulnerables a los ataques no invasivos que usan las mediciones de potencia y tiempo para extraer la clave criptográfica. Las técnicas de medición de potencia se basan en el comportamiento energético dependiente de los datos del sistema subyacente. Además, el análisis de potencia se puede usar para identificar las partes específicas del programa que se está ejecutando para inducir problemas de sincronización que, a su vez, pueden ayudar a evitar la verificación de claves. Por lo tanto, es importante enmascarar el consumo de energía al ejecutar los algoritmos de cifrado. La arquitectura de conjunto de instrucciones de un simple procesador de tarjeta inteligente canalizada de cinco etapas con instrucciones seguras para enmascarar las diferencias de energía debidas a los cálculos de datos relacionados con la clave en DES y encriptaciones de Rijndael se aumenta. Las versiones seguras operan en las versiones normales y complementarias de los operandos simultáneamente para enmascarar las variaciones de energía debidas a operaciones dependientes del valor. Sin embargo, esto conlleva la penalización de un mayor consumo total de energía en los componentes de la ruta de datos. En consecuencia, empleamos versiones seguras de

instrucciones solo para operaciones críticas; es decir, utilizamos instrucciones seguras de forma selectiva, tal como lo indica un compilador de optimización. Usando un simulador de energía de ciclo preciso, se demuestra la efectividad de esta mejora. El enfoque logra enmascarar la energía de las operaciones críticas, consumiendo un 83% menos de energía en comparación con los enfoques existentes que emplean circuitos de doble carril. Empleamos versiones seguras de instrucciones solo para operaciones críticas; es decir, utilizamos instrucciones seguras de forma selectiva, tal como lo indica un compilador de optimización. Usando un simulador de energía de ciclo preciso, se demuestra la efectividad de esta mejora. El enfoque logra enmascarar la energía de las operaciones críticas, consumiendo un 83% menos de energía en comparación con los enfoques existentes que emplean circuitos de doble carril. Empleamos versiones seguras de instrucciones solo para operaciones críticas; es decir, utilizamos instrucciones seguras de forma selectiva, tal como lo indica un compilador de optimización. Usando un simulador de energía de ciclo preciso, se demuestra la efectividad de esta mejora. El enfoque logra enmascarar la energía de las operaciones críticas, consumiendo un 83% menos de energía en comparación con los enfoques existentes que emplean circuitos de doble carril.

14. **A Hybrid Scheme of Public-Key Encryption and Somewhat Homomorphic Encryption:** Presentamos un cifrado homomórfico híbrido que combina el cifrado de clave pública (PKE) y el cifrado algo homomórfico (SHE) para reducir los requisitos de almacenamiento de la mayoría de las aplicaciones de cifrado homomórfico (FHE). En este modelo, los mensajes se cifran con un PKE y los cálculos sobre datos cifrados se realizan mediante SHE o FHE después del descifrado homomorfo. Para obtener un descifrado homomorfo eficiente, nuestro esquema híbrido combina IND-CPA PKE sin un relleno de mensajes complicado con SHE con un gran espacio de mensajes de enteros. Además, si el PKE subyacente es multiplicativo, el esquema propuesto tiene la ventaja de que los polinomios de grado arbitrario pueden evaluarse sin arranque. Construimos este esquema mediante la concatenación de los esquemas de ElGamal y Goldwasser-Micali en un anillo $\mathbb{Z}_N$ para un entero compuesto N cuyo espacio de mensaje es $\mathbb{Z}_N^\times$. Para acelerar la evaluación homomórfica del descifrado PKE, introducimos un método para reducir el grado del circuito de exponenciación al costo de claves públicas adicionales. Usando la misma técnica, presentamos una solución parcial eficiente a un problema abierto que consiste en evaluar la aritmética mod q mod p homomorfamente para p grande. Como interés independiente, también obtenemos un método genérico para convertir de SHE de clave privada a SHE de clave pública. A

diferencia del método descrito por Rothblum, somos libres de elegir el espacio de mensajes SHE.

15. **The Application of Hybrid Encryption Algorithm in Software Security:** Debido al defecto de solo el cifrado de datos único y el uso del famoso algoritmo de cifrado, que no se mejoró en los métodos tradicionales del proceso de registro, en esta tesis se propone un algoritmo de cifrado combinado. Es decir, la seguridad del algoritmo se mejora en gran medida, investigando varios algoritmos de cifrado de datos famosos, y mejorando algunos algoritmos de cifrado de datos, y organizando los algoritmos de cifrado en algún orden. Finalmente, el algoritmo de cifrado combinado se realiza con éxito utilizando el algoritmo de cifrado inicial, el algoritmo de cifrado Micro Genard y el famoso algoritmo de cifrado Base64. Es decir, de acuerdo con el orden del algoritmo de cifrado inicial, el algoritmo de cifrado Micro Genard mejorado y el famoso algoritmo de cifrado Base64, la información del usuario se cifra gradualmente. y la seguridad del algoritmo es mucho mayor. Además, al sistema de software de videovigilancia, por ejemplo, que se utiliza ampliamente en el campo de la gestión de la seguridad del tráfico, el algoritmo de cifrado combinado está completamente validado y su seguridad es muy alta.

16. **White-Box cryptography based data encryption-decryption scheme for IoT environment.** El progreso económico de la Internet de las cosas. (IoT) es fenomenal. Las aplicaciones van desde la comprobación de la Alineación de algunos componentes durante un proceso de fabricación. Seguimiento de los niveles de transporte y peatones para mejorar. Conducción y camino a pie, observando a distancia enfermos terminales. Pacientes mediante dispositivos médicos como dispositivos implantados. y bombas de infusión, y así sucesivamente. Para proporcionar seguridad, encriptando el Los datos se convierten en un requisito indispensable, y simétrico. Los algoritmos de encriptación se están convirtiendo en una implementación crucial en Los entornos de recursos limitados. Simetrico típico algoritmos de encriptación como Advanced Encryption Standard (AES) muestra un supuesto de que los puntos finales de las comunicaciones son seguro y que la clave de cifrado se almacena de forma segura. Sin embargo, los dispositivos pueden estar físicamente desprotegidos, y los atacantes puede tener acceso a la memoria mientras los datos aún están encriptados. Eso Es esencial reservar la clave de tal manera que un atacante encuentre Es difícil extraerlo. En la actualidad, técnicas como la caja blanca. La criptografía ha sido utilizada en estas circunstancias. Pero tiene Se ha informado que la aplicación de la criptografía de caja blanca en IoT Los dispositivos han provocado otros problemas de seguridad como el adversario. Tener acceso a los valores intermedios, y la práctica.

Implementaciones que conducen a código de ataques de elevación y diferencial los ataques. En este trabajo, se presenta una solución para superar estos problemas al demostrar la necesidad de la criptografía de caja blanca para mejorar la seguridad utilizando el encadenamiento de bloques de cifrado Modo (CBC).

17. **Cybersecurity in safety-critical systems.** El año 2016 vio estándares de ciberseguridad en las industrias de dispositivos médicos y automotrices. Ambos estándares están comprensiblemente basados en procesos que ya existen en las industrias respectivas. El estándar J3061[1] automotriz está muy centrado en las categorías existentes para definir las amenazas de ciberseguridad, es decir, sistemas, hardware y software. La ciberseguridad es un tema muy multifacético, y al restringir el alcance a estas 3 áreas temáticas, existe el riesgo de que se pasen por alto muchas amenazas importantes, en particular los actos maliciosos de los empleados dentro de una organización. La ciberseguridad médica informe AAMI TIR 57[2] adopta el enfoque basado en la norma ISO 14971[3], el estándar de gestión de riesgos de dispositivos médicos, que fomenta un enfoque más abierto para evaluar las amenazas de ciberseguridad . Ambos documentos, que se discuten en este documento, carecen de ejemplos prácticos o técnicas para evaluar y mitigar las amenazas; El tema se trata de una manera más teórica. Los problemas clave, como los circuitos de troyanos en microcontroladores, no están bien representados en ninguno de los dos documentos. En general, los temas de software, como la autenticación y el cifrado, reciben una buena cobertura en los estándares internacionales; Sin embargo, este no es el caso cuando se revisan problemas de hardware. Tanto TIR 57 como J3061 son buenos documentos de inicio para el tema de la ciberseguridad., pero ambos podrían beneficiarse de la expansión para cubrir los temas más amplios que afectan a la ciberseguridad.

18. **Cyber-Security Enhancement of Networked Control Systems Using Homomorphic Encryption.** Este artículo propone un nuevo concepto de controlador. Cifrado para la mejora de la ciberseguridad de la red. controle los sistemas y presenta cómo cifrar un controlador lineal utilizando nuestros esquemas de cifrado homomórficos modificados basado en sistemas de encriptación RSA y El Gamal de clave pública. Una ventaja notable del cifrado del controlador es ser capaz de ocultar varias informaciones procesadas dentro de la Dispositivo controlador, como parámetros del controlador, referencias (Recetas), medidas, comandos de control, y parámetros. de modelos de plantas en el modelo interno principal, manteniendo un Función original del controlador. Por lo tanto, incluso si malicioso los usuarios piratearon el dispositivo controlador por accesos no autorizados,

Tomaría mucho tiempo y costo descifrar y robar el control información del sistema. Finalmente, los ejemplos numéricos confirman que solo los parámetros y señales codificados se pueden ver en el dispositivo controlador del control en red del sistema de seguridad mejorada.

## ANALISIS DE LOS RESULTADOS.

Encriptación es el proceso mediante el cual cierta información o texto sin formato es cifrado de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación. Es una medida de seguridad utilizada para que al momento de almacenar o transmitir información sensible ésta no pueda ser obtenida con facilidad por terceros. Opcionalmente puede existir además un proceso de desencriptación a través del cual la información puede ser interpretada de nuevo a su estado original, aunque existen métodos de encriptación que no pueden ser revertidos. El término encriptación es traducción literal del inglés y no existe en el idioma español. La forma más correcta de utilizar este término sería cifrado.

Cuando hablamos de criptografía se tienen en cuenta ciertos elementos:

- ✓ Un mensaje que se desea transmitir.
- ✓ Un sistema de comunicación por el cual se va a transmitir el mensaje.
- ✓ Un protocolo o sistema que va a permitir el cifrado y descifrado del mensaje.

Para hablar de un sistema criptográfico o criptosistema tenemos que tener en cuenta los siguientes elementos:

- ✓ Alfabeto.
- ✓ Un conjunto de transformaciones de cifrado.
- ✓ Conjunto de transformación de descifrado.
- ✓ Conjunto de claves.

Las condiciones básicas de un criptosistema informático son cinco:

- ✓ Conjunto finito de textos claros, es decir de unidades de mensaje que se deseen transmitir.
- ✓ Conjunto finito de textos cifrados, unidades de mensaje que se reciban por parte del receptor.

- ✓ Conjunto finito de claves: se busca que este conjunto sea lo más grande posible para que se demore la mayor cantidad de tiempo posible en hallar claves para cifrar o descifrar los textos.

Conjunto de funciones de cifrado: a cada texto claro se asigna una función de texto cifrado.

Conjunto de funciones de descifrado: a cada texto cifrado corresponde un texto claro

**La encriptación de datos funciona utilizando la criptografía**. La criptografía es la ciencia de usar las matemáticas para encriptar y desencriptar datos. Una vez que la información ha sido encriptada, puede ser almacenada en un medio inseguro o enviada a través de una red insegura (como Internet) y aun así permanecer secreta.

Luego, los datos pueden desencriptarse a su formato original.

**Algoritmo criptográfico:** Un algoritmo criptográfico, o cifrador, es una función matemática usada en los procesos de encriptación y desencriptación. Un algoritmo criptográfico trabaja en combinación con una llave (un número, palabra, frase, o contraseña) para encriptar y desencriptar datos. Para encriptar, el algoritmo combina matemáticamente la información a proteger con una llave provista.

El objetivo de un algoritmo criptográfico es hacer tan difícil como sea posible desencriptar los datos sin utilizar la llave. Si se usa un algoritmo de encriptación realmente bueno, entonces no hay ninguna técnica significativamente mejor que intentar metódicamente con cada llave posible.

El resultado de este cálculo son los datos encriptados. Para desencriptar, el algoritmo hace un cálculo combinando los datos encriptados con una llave provista, siendo el resultado de esta combinación los datos desencriptados.

La mayoría de los algoritmos modernos del cifrado se basan en una de las siguientes dos categorías de procesos:

- ✓ Problemas matemáticos que son simples pero que tienen una inversa que se cree (pero no se prueba) que es complicada.
- ✓ Secuencias o permutaciones que son en parte definidos por los datos de entradas.

**Diferencias entre el proceso de encriptación y desencriptación**

La encriptación es el proceso en el cual los datos a proteger son traducidos a algo que parece aleatorio y que no tiene ningún significado (los datos encriptados). La desencriptación es el proceso en el cual los datos encriptados son convertidos nuevamente a su forma original.

**Funcionamiento**

Para la encriptación de datos se utiliza comúnmente un sistema de clave pública que permite conjuntamente con la firma digital, el aseguramiento de la integridad de los datos transmitidos o almacenados.
La encriptación con algoritmos de clave pública, funciona con un par de llaves, una publica y una privada.
Estas claves permiten que el receptor y emisor mantengan una comunicación confiable permitiendo que los datos viajen a través de la red encriptados y que al llegar al receptor, pueda el mismo recomponer la información fácilmente.

***La encriptación de datos se basa en métodos llamados Métodos de encriptación:***
Para poder Encriptar un dato, se pueden utilizar procesos matemáticos diferentes:

1. ***Algoritmo HASH:*** Este algoritmo efectúa un cálculo matemático sobre los datos que constituyen el documento y da como resultado un número único llamado MAC. Un mismo documento dará siempre un mismo MAC. es una **función** para resumir o identificar probabilísticamente un gran **conjunto** de información, dando como resultado un conjunto imagen finito generalmente menor. se refiere a una **función** o método para generar **claves** o llaves que representen de manera casi unívoca a un **documento**, **registro**, **archivo**, etc., resumir o identificar un **dato** a través de la **probabilidad**, utilizando una función hash o algoritmo hash. Un hash es el resultado de dicha **función** o **algoritmo**. Entre los algoritmos de hash más comunes están: *SHA-1:* algoritmo de hash seguro. *Algoritmo de síntesis* que genera un hash de 60 bits. Se utiliza, por ejemplo, como algoritmo para la firma digital. *MD2* está optimizado para computadoras de 8 bits. El valor hash de cualquier mensaje se forma haciendo que el mensaje sea múltiplo de la longitud de bloque en el ordenador (128 bits o 16 bytes) y añadiéndole un checksum. Para el cálculo real, se utiliza un bloque auxiliar 48 bytes y una tabla de 256 bytes que contiene dígitos al azar del número pi. *MD4* es un algoritmo de resumen del mensaje (el cuarto en la serie) diseñado por el profesor **Ronald Rivest** del **MIT**. Implementa una función criptográfica de **hash** para el uso en comprobaciones de integridad de mensajes. La longitud del resumen es de 128 bits.
*MD5* Esquema de hash de hash de 128 bits muy utilizado para autenticación cifrada.

Gracias al MD5 se consigue, por ejemplo, que un usuario demuestre que conoce una contraseña sin necesidad de enviar la contraseña a través de la red.

2. ***Algoritmos Simétricos:*** Utilizan una clave con la cual se encripta y desencripta el documento. Todo documento encriptado con una clave, deberá desencriptarse, en el proceso inverso, con la misma clave. En este modelo, el mensaje original es convertido en un mensaje cifrado que aparentemente es aleatorio y sin sentido. El proceso de encriptación está formado por dos componentes, un algoritmo y una clave. La clave es un valor que es independiente del texto o mensaje a cifrar. El algoritmo va a producir una salida diferente para el mismo texto de entrada dependiendo de la clave utilizada. Una vez cifrado, el mensaje puede ser transmitido. El mensaje original puede ser recuperado a través de un algoritmo de desencriptación y la clave usada para la encriptación.
3. **Algoritmos Asimétricos (RSA):** Requieren dos Claves, una Privada (única y personal, solo conocida por su dueño) y la otra llamada Pública, ambas relacionadas por una fórmula matemática compleja imposible de reproducir.
   Los pasos del proceso de encriptación con clave pública son los siguientes:
   o Cada sistema genera un par de claves para ser usadas en la encriptación y desencriptación de los mensajes que envíen y reciban.
   o Cada sistema publica su clave de encriptación (clave pública). La clave de desencriptación relacionada (clave privada) se mantiene en privado.
   o Si Alice desea enviar un mensaje a Bob, encripta el mensaje utilizando la clave pública de Bob o Cuando Bob recibe un mensaje lo desencripta usando su clave privada. Nadie puede desencriptar el mensaje porque solo Bob conoce su clave privada.
4. **Algoritmo de encriptación RC4:** Es un algoritmo de Cifrador de flujo (no de bloques), creado en 1987 por Ronald Rivest (la R de RSA - Secreto Comercial de RSA Data Security). Fue publicado el 13 de Septiembre de 1994 usando remailers anónimos en un **grupo** de news: sci.crypt. Es usado por diversos **programas** comerciales como Netscape y Lotus Notes.

## Firma Digital:

La **firma digital** permite garantizar algunos conceptos de seguridad que son importantes al utilizar documentos en formato digital, tales como Identidad o autenticidad, integridad y no repudio. El modo de funcionamiento es similar a lo explicado para los algoritmos de encriptación, se utilizan también algoritmos de clave pública, aplicados en dos etapas.

### *Ventajas Ofrecidas por la Firma Digital*

- *Integridad de la información:* la integridad del documento es una protección contra la modificación de los datos en forma intencional o accidental. El emisor protege el documento, incorporándole a ese un valor de control de integridad, el receptor deberá efectuar el mismo cálculo sobre el documento recibido y comparar el valor calculado con el enviado por el emisor.

- *Autenticidad del origen del mensaje:* este aspecto de seguridad protege al receptor del documento, garantizándole que dicho mensaje ha sido generado por la parte identificada en el documento como emisor del mismo, no pudiendo alguna otra entidad suplantar a un usuario del sistema.
- *No repudio del origen:* el no repudio de origen protege al receptor del documento de la negación del emisor de haberlo enviado. Este aspecto de seguridad es más fuerte que los anteriores ya que el emisor no puede negar bajo ninguna circunstancia que ha generado dicho mensaje, transformándose en un medio de prueba inequívoco respecto de la responsabilidad del usuario del sistema.

***Diferencias hay entre los algoritmos simétricos y los asimétricos***

Los algoritmos simétricos encriptan y desencriptan con la misma llave. Las principales ventajas de los algoritmos simétricos son su seguridad y su velocidad. Los algoritmos asimétricos encriptan y desencriptan con diferentes llaves. Los datos se encriptan con una llave pública y se desencriptan con una privada, siendo ésta su principal ventaja. Los algoritmos asimétricos, también conocidos como algoritmos de llave pública, necesitan al menos una llave de 3.000 bits para alcanzar un nivel de seguridad similar al de uno simétrico de 128 bits. Y son increíblemente lentos, tanto que no pueden ser utilizados para encriptar grandes cantidades de información.

Los algoritmos simétricos son aproximadamente 1.000 veces más rápidos que los asimétricos.

***Encriptar datos en un PDA.***

La importancia de tener nuestros datos a salvo de miradas extrañas o tener un mínimo de privacidad se ha convertido en un tema muy importante. Los PDAs son muchas veces usados como pequeñas oficinas portátiles donde se guardan datos de gran valor y donde es de gran importancia tener estos datos protegidos.

Muchos usuarios de PDAs por comodidad no protegen el acceso de inicio con una clave, imagínense en caso de pérdida del aparato o descuido poder dejar estos datos confidenciales en manos ajenas a las nuestras. Para solucionar este problema o tener un cierto grado de seguridad, es muy importante poder encriptar nuestros datos.

***Encriptación de ficheros***

Windows XP Profesional nos da una alternativa para poder proteger estos datos y prevenir su pérdida. El "Encripting File System" (EFS) es el encargado de codificar los ficheros. Estos

ficheros sólo se pueden leer cuando el usuario que los ha creado hace "logon" en su máquina (con lo cual, presumiblemente, nuestra password será una password robusta). De hecho, cualquiera que acceda a nuestra máquina, no tendrá nunca acceso a nuestros ficheros encriptados aunque sea un Administrador del equipo.

La encriptación es el proceso de codificar datos sensibles usando un algoritmo. Sin la clave del algoritmo correcta los datos no pueden ser desencriptados. Windows XP usa encriptación para varios propósitos:

- Ficheros encriptados en un volumen NTFS.
- Datos encriptados enviados entre un cliente web y un servidor usando Security Socket Layer (SSL).

En la revisión de los artículos publicados consideran:

- **DES:** Las siglas DES corresponden a las iniciales de Data Encryption Standard. Este algoritmo se convirtió en un estándar y se utiliza en gran parte de los sistemas informáticos que precisan de un cierto grado de protección, a pesar de las restricciones que el gobierno de los Estados Unidos impuso para su comercialización fuera del país. El algoritmo consiste en un complejo sistema de operaciones matemáticas basado en sustituciones y permutaciones de bits en función de una clave. El conocimiento del algoritmo no permite descifrar la información cifrada; de hecho éste es de dominio público.

  **Seguridad del algoritmo**

  Cuando el algoritmo DES se presentó existían numerosas dudas sobre si contendría "puertas traseras" que permitiesen al gobierno de los Estados Unidos descifrar todo tipo de comunicaciones. Más tarde se demostró que estas dudas no tenían fundamento; sin embargo, el tamaño de la clave utilizada hace que el algoritmo sea vulnerable y esta situación se agrave más según vaya incrementándose la potencia de los ordenadores y disminuyendo su precio. La única forma conocida de violar el algoritmo es probar a descifrar la información con todas las posibles claves. Puesto que constan de 56 bits habría que probar con 2E56, es decir, 72.057.594.037.927.936 claves distintas. Suponiendo que se dispone de un ordenador de gran potencia capaz de generar y probar un millón de claves por segundo, se requerirían unos 72.000 millones de segundos lo que, traducido a años, serian 2.285. Sin embargo, utilizando un superordenador con multitud de procesadores en paralelo se podrían generar todas las claves en tan sólo unas horas, aunque este tipo de ordenadores no está al alcance de cualquiera

- **RSA:** El algoritmo RSA fue desarrollado en los años setenta por Rivest, Shamir y Adleman, de cuyas iniciales toma su nombre, y está basado en el problema de hallar los factores primos de grandes números. Frente a sus diversas ventajas sobre los sistemas de clave privada presenta el inconveniente de la carga que supone al sistema, puesto que se basa en operaciones que consumen mucho tiempo de proceso.
  **La seguridad del algoritmo** radica en el tamaño de un número n, que es el producto de los números primos. No es aconsejable trabajar con valores inferiores a 154 dígitos o lo que es lo mismo 512 bits y para aplicaciones que requieran un alto grado de seguridad 1024 bits (308 dígitos) ó incluso 2048. El algoritmo más rápido conocido para factorizar un número se debe a R. Shroeppel, que permite hacerlo con un número de operaciones definido por la expresión: ev(ln (In n))ln n Por ejemplo con un número de 300 dígitos. Suponiendo que se dispone de un ordenador de gran potencia capaz de realizar un millón de operaciones por segundo, se requerirían 4800 billones de años para factorizar el número. Aun dividiendo el problema en partes y utilizando múltiples sistemas o un superordenador con multitud de procesadores en paralelo, con 300 dígitos la seguridad está garantizada.
- **Aplicaciones** La Criptología se utiliza también para la autentificación de mensaJes y para firmas digitales. El método de la autentificación consiste en incorporar al mensaje un código llamado MAC (Modification Autentification Code ), que se calcula aplicando un algoritmo de cifrado al texto entero. El receptor hace lo mismo y compara el valor que le da con el que lleva el mensaje, si es igual, el mensaje se considera autentico.
  - ✓ **Firma Digital:** El mecanismo de firma digital soporta los servicios de integridad de datos, autenticación de origen y no repudio con prueba de origen. Para proporcionar el servicio de no repudio con prueba de entrega es necesario forzar al receptor a enviar al emisor un recibo firmado digitalmente.
  - ✓ **Firewalls:** Un firewall es un sistema o un grupo de sistemas que decide que servicios pueden ser accesados desde el exterior (Internet, en este caso) de un red privada, por quienes pueden ser ejecutados estos servicios y también que servicios pueden correr los usuarios de la intranet hacia el exterior (Internet). Para realiz.ar esta tarea todo el tráfico entre las dos redes tiene que pasar a través de él.

Los algoritmos de cifrado basados en homomorfismo pueden ser determinísticos o probabilísticos. Cuando el algoritmo es probabilístico, se obtienen diferentes textos cifrados para un mismo texto en claro, dependiendo de una variable aleatoria. A continuación se describen algunos criptosistemas que son homomórficos.

- **RSA:** El esquema de RSA es un ejemplo de un algoritmo homomórfico determinista bajo la multiplicación. Éste realiza los cálculos en Zn donde n = p·q y p, q son primos distintos. Para ese entero n se sabe que φ(n) = (p − 1)(q

− 1), donde φ es la función tociente de Euler. El espacio de los textos en claro T es igual que el de los textos cifrados T 0 y queda expresado como: T = T 0 = Zn.

- **El Gamal:** El Gamal es un criptosistema que basa su seguridad en el problema del logaritmo discreto. Este problema puede ser descrito en un grupo multiplicativo (G, ·), para un elemento α ∈ G de orden n se define el subgrupo generado por α como: hαi = {α i : 0 ≤ i ≤ n − 1} hαi es un subgrupo ciclico de G, que tiene orden n. En este contexto el problema del logaritmo discreto en un subgrupo hαi de un grupo (G, ·) se enuncia como: encontrar un entero a donde 0 ≤ a ≤ n − 1 tal que α a = β. Este entero a es equivalente a la expresión logα β.

# CAPÍTULO IV. CONCLUSIONES

En todos los estudios publicados se obtuvieron que fueron el de mayor porcentaje en los repositorios institucionales de las universidades, seguidos de la fuente de búsqueda en Pubmed y en el IEE explore.

En todos los estudios publicados se obtuvieron que por año fueron de mayor porcentaje en el 2017 seguido del 2016, siendo 0% en los años 2006, 2015 y 2018.

En todos los estudios publicados se obtuvieron que según el tipo fueron el de mayor porcentaje los artículos científicos seguido de las tesis de pregrado.

Se concluye que reforzar la seguridad con técnicas de encriptación avanzada es vital para las empresas que ofrecen sus productos, el algoritmo se presenta como una alternativa a los algoritmos tradicionales de combinatoria demostrando una mayor eficiencia en la gestión de recursos computacionales y plantea las bases para su continuar con su estudio en la comunidad académica interesada, debido a la variedad de los sistemas dinámicos no lineales. Por lo que evidencia que el efecto de la encriptación de datos en la ciberseguridad es efectiva.

# REFERENCIAS

1. Repositorio.ug.edu.ec/.../B-CINT-PTG N.223.Álvarez%20Coello%20Lidia%20Alejand.
2. https://www.academia.edu/34307828/Algoritmo_para_mostrar_el_proceso_de_encriptaci%C3%B3n_y_desencriptaci%C3%B3n_de_datos_en_PHP._Una_aplicaci%C3%B3n_de_seguridad_inform%C3%A1tica
3. http://dspace.ups.edu.ec/handle/123456789/8185
4. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0012-73532016000400004&lng=es&nrm=iso&tlng=en
5. www.scielo.org.co/pdf/inge/v21n3/v21n3a08.pdf
6. http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/131?show=full
7. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1705507
8. https://www.cs.cinvestav.mx/TesisGraduados/2009/tesisLilRodriguez.pdf
9. https://dialnet.unirioja.es/servlet/articulo?codigo=6114397
10. http://repositorio.ucv.edu.pe/handle/UCV/13324
11. http://repositorio.puce.edu.ec/handle/22000/12017

## ANEXOS

| N° | AUTORES | TÍTULO | AÑO | DISEÑO DEL ESTUDIO | FUENTE |
|---|---|---|---|---|---|
| **1** | Álvarez Coello Lidia Alejandrina Anzules Navarro Félix Samuel | Diseño de una aplicación segura de mensajería web interna utilizando el algoritmo de encriptación RSA para la Carrera De Ingeniería en Networking & Telecomunicaciones, año 2017. | 2017 | Tesis Pregrado | Repositorio Universidad de Guayaquil |
| **2** | Guillermo Mejía Díaz, Edwin Enrique Viche Rivas | Algoritmo para mostrar el proceso de encriptación y desencriptación de datos en PHP. Una aplicación de seguridad informática. | 2017 | Artículo | Scielo |
| **3** | Sheilla Etty Gómez Fernandez | Criptografía y Seguridad en Computadores | 2007 | Tesis pregrado | Repositorio de la Universidad Nacional de Ingeniería |
| **4** | Julio César Mendoza T. Ingeniería de Sistemas – Quito | Demostración de cifrado simétrico y asimétrico | 2008 | Artículo | Red de repositorios de acceso abierto del Ecuador |
| **5** | Ian Carlo Guzmán, Rubén Darío Nieto & Álvaro Bernal | Implementación en FPGA del algoritmo AES-128 en modos de operación no realimentados | 2016 | Artículo | DYNA SCIELO |
| **6** | José Moreno, Fabio Parra, Rafael Huérfano, Cesar Suarez, Isabel Amaya | Modelo de Encriptación Simétrica Basada en Atractores Caóticos | 2016 | Reporte de caso | SCIELO |
| **7** | Katia Regina León Lomparte | Rencriptacion RSA de archivos de texto | 2005 | Tesis Maestría | Repositorio PUCP |

| | | | | | |
|---|---|---|---|---|---|
| **8** | Álvarez Coello Lidia Alejandrina. Anzules Navarro Félix Samuel. | Diseño De Una Aplicación Segura De Mensajería Web Interna Utilizando El Algoritmo De Encriptación RSA Para La Carrera De Ingeniería En Networking & Telecomunicaciones, Año 2017 | 2017 | Tesis pregrado | GOOGLE SCHOLAR |
| **9** | López Mendoza Roxana Mercedes Mesias Meza Luis Enrique | Simulación De Un Sistema Transaccional Mediante. Un Canal Seguro, Usando Criptografía | 2017 | Tesis pregrado | Repositorio de la Universidad De Guayaquil |
| **10** | Jhonny Antonio Pabón Cadavid | The cryptography and the protection of digital information | 2012 | Artículo | Social Science Research Network SSRN |
| **11** | Lil María Xibai Rodríguez Henríquez | Esquema de cifrado para la ejecución de consultas en bases de datos cifradas | 2009 | tesis maestría | Repositorio del instituto politécnico nacional |
| **12** | Iv´anFelipeRodr´ıguez1, EdilmaIsabel Amaya∗1,C´esarAugustoSu´arez1, Jos´eDavidMoreno1 | Algoritmo de Encriptación de Imágenes Utilizando el Atractor Caótico de Lorenz | 2017 | Artículo | Revista de ingeniería. DIALNET |
| **13** | Chun Kiat Tan,1 Jason Changwei Ng,1 Xiaotian Xu,1 Chueh Loo Poh,2 Yong Liang Guan,1 and Kenneth Sheah3 | Security Protection of DICOM Medical Images Using Dual-Layer Reversible Watermarking with Tamper Detection Capability | 2010 | Artículo | Pubmed |
| **14** | Whye Kit Tan 1, Sang-Gon Lee 1,*, Jun Huy Lam 1 and Seong-Moo Yoo 2 | A Security Analysis of the 802.11s Wireless Mesh Network Routing Protocol and Its Secure Routing Protocols | 2013 | Artículo | Pubmed |
| **15** | Mantos PL[1], Maglogiannis I[2]. | Sensitive Patient Data Hiding using a ROI Reversible Steganography Scheme for DICOM Images. | 2016 | Artículo | Pubmed |

| | | | | | |
|---|---|---|---|---|---|
| **16** | Danielle Kriz | Cybersecurity Principles for Industry and Government A Useful Framework for Efforts Globally to Improve Cybersecurity | 2012 | Artículo | Pubmed |
| **17** | Regner Sabillon ; Jordi Serra-Ruiz ; Victor Cavaller ; Jeimy Cano | A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM) | 2017 | Artículo | IEEE xplore |
| **18** | Danielle Kriz | Cybersecurity principles for industry and government: A useful framework for efforts globally to improve cybersecurity | 2011 | Artículo | IEEE xplore |
| **19** | Paresh Rathod ; Timo Hämäläinen | A Novel Model for Cybersecurity Economics and Analysis | 2017 | Artículo | IEEE xplore |
| **20** | Gloria D'Anna | CHAPTER 5 Engineering for Vehicle Cybersecurity by Daniel DiMase, Zachary A. Collier, John A. Chandy, Bronn Pav, Kenneth Heffner, and Steve Walters | 2019 | Artículo | IEEE xplore |
| **21** | Tan WK1, Lee SG, Lam JH, Yoo SM. | **A security analysis of the 802.11s wireless mesh network routing protocol and its secure routing protocols** | 2013 | Artículo | Pubmed |
| **22** | Walker, Alastair | Cybersecurity in safety-critical systems<br>DOI: 10.1002/smr.1956 | 2017 | Artículo | EBSCO |
| **23** | Kiminao Kogiso ; Takahiro Fujita | **Cyber-Security Enhancement of Networked Control Systems Using Homomorphic Encryption**<br>**DOI:** 10.1109/CDC.2015.7403296 | 2017 | Artículo | IEEE xplore |
| **24** | Ríos Taipe, Josue Wenceslao | **Sistema de encriptación para optimizar el proceso de Desarrollo de software de una empresa de lima** | 2017 | Tesis pregrado | alicia.concytec.gob.pe |
| **25** | María De Los Ángeles Valle C | Análisis de métodos criptográficos para la gestión de firmas y Certificados digitales dentro de un contexto de supervisión (SBS) Para enfrentar los nuevos requerimientos de seguridad Informática | 2014 | Tesis Pregrado | Repositorio de tesis de grado y posgrado Pontificia Universidad católica ecuador. |