Universidad Central "Marta Abreu" de Las Villas
Facultad de Ciencias de la Información y de la Educación

Trabajo de Diploma

Título:

Análisis de Dominio de la temática Criptografía

Autora:
Yaniceli Sosa Avalos

Tutores:
Dra. Aida María Torres Alfonso
MSc. Guillermo Sosa Gómez

2013

"La mayoría de las ideas fundamentales de la ciencia son esencialmente sencillas y, por regla general pueden ser expresadas en un lenguaje comprensible para todos."

Albert Einstein

Dedicatoria

.....Dedico el esfuerzo empeñado en esta investigación a mis padres, hermana y sobrino. quienes merecen todo, y por quienes obtengo las fuerzas para alcanzar mis sueños.

Agradecimientos

A mis padres por apoyarme cada día y demostrarme que lo único que ciertamente tendremos es lo que seamos capaces de hacer con nuestros esfuerzos.

A mi Hermana por ser mi espejo todos estos años y convertirme en la mujer que soy

A mi Damiancito por darme la fuerza que necesito para vivir.

A Yandy por enseñarme que la vida no es la fiesta que todos deseamos, pero mientras estemos vivos debemos bailar.

A los profesores de la FCIE por ayudarme todos estos años a convertirme en una profesional.

A Dayana Felipe y René por su paciencia y comprensión.

A mis tutores Aidi y Guille por estar ahí siempre que los he necesitado a pesar de las circunstancias.

A los integrantes de Grupo de Criptografía, por acogerme y permitirme formar parte de ellos.

A Yairon, por permitirme ocupar parte de su tiempo

Y no por últimos menos importante.....

A mi amiga de la infancia Cheila, por no abandonarme a pesar de la distancia que el deber nos impuso.

A Osbel mi amigo, hermano y compañero de toda la vida, con quien comparto mis mas sentidas alegrías y quien a depositado en mi toda su fe.

A mi Neysita por estar ahí, sin desmayo, apoyándome cada día y llenando mi vida de fuerzas y alegría.

A Sai, mi nina grandota por enseñarme que el mundo pertenece a quien se atreve y que la vida es demasiado para ser insignificante.

A Ede por creer en mi proceder y aceptarme tal y como soy.

A Alito por comprenderme y acompañarme cada instante.

A Rosi por ser mi guía y demostrarme que siempre podemos ser mejores.

A mi otra familia Carlos, Uria, Maylin, Molina, Alejandro y Francis, por convencerme de que no estamos solos y que la vida es mucho más que sueños.

A Yaniel Hernández por estar ahí dando por hecho que podre lograr cada cosa que me proponga.

A Irenia y Yanquiel por permitirme ser su pequeña nene

A las chicas de 101B por acogerme cuando más lo necesité.

A quienes han dedicado parte de su tiempo a escucharme y brindarme su apoyo.

... A todos Muchas Gracias

Resumen

Resumen

La presente investigación pretende examinar la Producción Científica de la temática Criptografía desde la perspectiva de Análisis de Dominio considerando principalmente los años 2008, 2009, 2010, 2011, 2012. Se utilizan dos enfoques, dirigidos en específico, a los estudios bibliométricos con el fin de organizar patrones sociológicos de reconocimiento explícito entre documentos individuales, y los estudios empíricos de usuarios para organizar dominios según la preferencia, comportamiento o los modelos mentales de sus usuarios. Se toma como referencia el Grupo Científico de Criptografía de la Universidad Central Marta Abreu de Las Villas, teniendo en cuenta que fue creado para potenciar el uso de esta ciencia en el centro del país, y se describen de este, sus líneas de investigación, principales temáticas estudiadas, autores más citados y redes de colaboración.

Palabras Clave: PRODUCCIÓN CIENTÍFICA; ANÁLISIS DE DOMINIO; CRIPTOGRAFÍA.

Abstract

Abstract

This investigation aims to examine the Scientific Production related to Cryptography science from the perspective of the Domain Analysis, considering mainly the years 2008, 2009, 2010, 2011 and 2012. Two points of view are used, the first, is directed to the bibliometrical studies with the purpose of organizing sociological patterns of explicit recognition among individual documents, and in the other way the empiric studies of users to organize domains according to the preference, behavior or the mental models of the users. The Cryptography Scientific Group that belongs to the *Universidad Central Marta Abreu de Las Villas (UCLV)* is taken as a reference to the research, considering that it was created to stimulate the application of this science in the central part of Cuba. An important objective of this study is to describe investigation lines, mainly studied themes, mostly quoted authors and collaboration networks of the Scientific Group.

Key Words: SCIENTIFIC PRODUCTION; DOMAIN ANALYSIS; CRYPTOGRAPHY.

Universidad Central "Marta Abreu" de Las Villas
Facultad de Ciencias de la Información y de la Educación
Carrera Ciencias de la Información

Índice

Tabla de Contenidos

Introducción

Introducción

Nuestro mundo ha entrado en una era de informatización donde no sólo las actividades de gobierno e inteligencia necesitan de vías seguras de tránsito de la información, sino también las transacciones comerciales y de negocios que se realizan por medio de la INTERNET e inclusive las comunicaciones telefónicas y satelitales. Ejemplos de actividades on-line son: banca, pago de salarios, tiendas virtuales, comercio mayorista, comercio de acciones, identificación electrónica, acceso a actas médicas, oficinas virtuales, procesamiento y archivo seguro de datos, envío de documentos certificados, firmas de contratos, elecciones, compra de boletos, juegos interactivos, librerías digitales, y muchas otras. (Aguirre, 2006)

Tras la conclusión de la Segunda Guerra Mundial, la Criptografía tuvo un desarrollo teórico importante, siendo Claude Shannon y sus investigaciones sobre teoría de la información esenciales hitos en dicho desarrollo. Además, los avances en computación automática suponen tanto una amenaza para los sistemas existentes como una oportunidad para el desarrollo de nuevos sistemas, lo cual deja abierto el camino al estudio profundizado del espectacular desarrollo de la tecnología criptográfica.

Con la evolución de esta ciencia se desarrollan novedosas investigaciones que permiten analizar la producción científica sobre Criptografía, utilizando técnicas de análisis de dominio que permite examinarla como una disciplina o especialidad científica, en la que los miembros de la comunidad dedicada a su investigación comparten los mismos objetivos, y utilizan los conocimientos especializados para la colaboración entre ellos, empleándolos además como mecanismo de intercomunicación.

Situación Problémica

Pocos son los estudios que se han realizado referentes a la Criptografía como ciencia puramente matemática y de acceso público, pero ninguno va

dirigido a profundizar en la estructura, organización del conocimiento, dominio y desarrollo de esta temática, lo cual permitiría fomentar los avances en la tecnología criptográfica. Por lo que con la presente investigación se pretende realizar un análisis de dominio que permita conocer como se desarrolla esta ciencia, cuáles son sus principales puntos de apoyo y ahondar en la necesidad de que sea conocida, estudiada y aplicada, teniendo en cuenta que no se cuenta con un estudio similar y que este podría ser la antesala de investigaciones que marcarían el desarrollo de la Criptografía por el resto de la historia, motivo por el cual se propone la siguiente:

Interrogante Científica:

- ¿Qué características posee la Producción Científica de Criptografía desde la perspectiva de Análisis de Dominio?

Objeto de investigación: Producción Científica de la Criptografía.

Campo de acción: Producción Científica de Criptografía desde la perspectiva de Análisis de Dominio

Para dar respuesta a la interrogante se presentan los siguientes objetivos.

Objetivo General:

- Caracterizar la Producción Científica de la Criptografía desde la perspectiva de Análisis de Dominio.

Objetivos Específicos:

- Abordar los Referentes teóricos- conceptuales de Producción Científica, Análisis de Dominio y Criptografía.
- Determinar los enfoques de Análisis de Dominio para evaluar la temática Criptografía.
- Describir el comportamiento de la Producción Científica sobre Criptografía desde la perspectiva de Análisis de Dominio.

Justificación de la Investigación

La presente investigación desde el punto de vista teórico ofrecerá una conceptualización de Producción científica, Análisis de Dominio y Criptografía, para la obtención de un profundo conocimiento de esta ciencia desde diferentes perspectivas teniendo en cuenta que, el diseño y construcción de sistemas informáticos se basa en la aplicación de una serie de técnicas y metodologías que aseguran la evolución de unas especificaciones formuladas en lenguaje natural hasta su representación en código escrito en un lenguaje de programación. Es importante señalar que, a pesar de que algunos avances se mantenían y se siguen manteniendo, en secreto, financiadas fundamentalmente por la NSA (Agencia Nacional de Seguridad de los EE.UU.), la mayor parte de las investigaciones hasta hace relativamente poco tiempo han sido tratadas como secretos militares, lo que a propiciado que haya un crecimiento espectacular de la Tecnología Criptográfica, motivo por el cual se hace necesario realizar dicho análisis de dominio.

El aporte metodológico se basa fundamentalmente en la aplicación de los enfoques de análisis de dominio dirigidos a los estudios bibliométricos y los estudios empíricos de usuarios, teniendo en cuenta que estos pueden organizar dominios según la preferencia, comportamiento o los modelos mentales de sus usuarios, lo cual posibilitará profundizar en el análisis del consumo de información y el desarrollo de la Criptografía, así como su aplicación a otras ciencias. Además se utilizan algunos métodos y técnicas de recogida de la información, como es el caso del Análisis Documental, con la revisión de algunas investigaciones realizadas sobre el desarrollo de la Criptografía como ciencia y otras dirigidas al análisis de dominio como es el caso de: Aproximación al Análisis del Dominio Higiene y Epidemiología en Cuba a través de Técnicas Conexionistas y Multivariantes; Análisis de Dominios por Medio de la Visualización de Mapas de Grandes Dominios

Científicos; utilización de la transformada, matrices de Hadamard en las funciones booleanas y en el Criptoanálisis, la Gestión de Información en el grupo de Criptografía de la UCLV desde la visión de las Ciencias de la Información, entre otras. Se utilizan también algunos indicadores bibliométricos que permiten fundamentar el estudio con sus respectivas clasificaciones y unidades de análisis, dotando a la investigación de argumentos solidos y coherentes.

Su aporte práctico puede declararse en la medida que sean identificadas las principales investigaciones realizadas referentes a la Criptografía, para confeccionar con ellas una Base de Datos que permite identificar las primordiales aristas en las que se ha desarrollado esta ciencia, así como sus áreas de conocimiento; partiendo de que en los últimos años, investigaciones serias llevadas a cabo en universidades de todo el mundo han logrado que esta sea una ciencia al alcance de todos, y que se convierta en la piedra angular de asuntos tan importantes como el comercio electrónico, la telefonía móvil, o las nuevas plataformas de distribución de contenidos multimedia, lo cual ha dejado a campo abierto el estudio de esta ciencia desde muchas otras, como es el caso de la Ciencias de la Información; en cuya disciplina a pesar de la tradición que arrastran los típicos estudios bibliométricos basados en el análisis de una o dos variables, parecen haber sido superados por los estudios dedicados al análisis de dominio, pues si bien se encuentran varios de ellos dentro de la literatura especializada (White and McCain, 1998), la mayoría se aplican al campo de la Ciencias de la Información a nivel internacional, por lo cual pretende realizarse un análisis de dominio de la Criptografía de forma que permita conocer hasta que medida se ha investigado y profundizado en esta ciencia ya que muchas son las voces que claman por su disponibilidad pública y que la experiencia ha demostrado que la única manera de tener buenos

algoritmos es que estos sean accesibles, para que puedan ser sometidos al escrutinio de toda la comunidad científica.

Antecedentes del estudio

Muchas son las investigaciones que se han realizado sobre producción científica y análisis de dominio, pero ninguna ha tratado la temática Criptografía, puesto que era una ciencia poco accesible, lo que convierte a esta investigación en la primera en la que se aborda la producción científica sobre criptografía utilizando técnicas de análisis de dominio para examinar el desarrollo y evolución de dicha ciencia. Entre las principales investigaciones llevadas a cabo se encuentran:

- La gestión de información en el grupo de Criptografía de la UCLV desde la visión de las Ciencias de la Información, de Yaniceli Sosa Avalos, Aida María Torres y Guillermo Sosa Gómez.
- Aproximación al Análisis del Dominio Higiene y Epidemiología en Cuba a través de Técnicas Conexionistas y Multivariantes, de Nancy Sánchez Tarragó.
- Análisis de Dominios por Medio de la Visualización de Mapas de Grandes Dominios Científicos, de Benjamín Vargas-Quesada de la Universidad de Alcalá, Facultad de Documentación y Félix de Moya Anegón, Zaida Chinchilla-Rodríguez, Antonio González-Molina.
- Aproximación cienciométrica al análisis y visualización del dominio científico argentino, 1990-2005 de Sandra Miguel y Félix de Moya Anegón.

Tanto estas investigaciones como otros estudios posteriormente referenciados son un punto de apoyo para el sustento teórico de la presente investigación, para la cual son tomadas como referencia, no solo por estar dirigidas al análisis de dominio sino también porque constituyen un estudio más exacto de la temática en materia.

Estructura Capitular:

La investigación se organiza por capítulos, estructurados según los objetivos propuestos. El primer Capítulo aborda las bases conceptuales del estudio para comprender la temática y respaldar el decursar de la pesquisa. Se ofrece una conceptualización de Producción Científica y su importancia para la realización del Análisis de Dominio, así como los enfoques establecidos para el mismo y se define la Criptografía como ciencia puramente matemática, enfatizando fundamentalmente en las investigaciones que apuntan hacia el desarrollo y crecimiento de la tecnología criptográfica.

El segundo capítulo explica el trabajo metodológico que rige la investigación, el tipo de estudio, las etapas por la que transcurrió la misma, los métodos y las técnicas empleados, la población y la muestra seleccionada, así como los enfoques escogidos para la realización del Análisis de Dominio y los indicadores métricos a seguir para conocer los avances referentes a dicha ciencia.

El capítulo tres presenta los resultados que arrojó la investigación, mostrando esencialmente las líneas de investigación, los autores más citados, las temáticas más concretas y las redes de colaboración entre las investigaciones, así las series temporales, la distribución geográfica, el tipo de institución y el índice de firmas por trabajo que conforman en si los indicadores de producción y colaboración analizados así como sus respectivas clasificaciones y unidad de análisis.

Declaración de la Norma Bibliográfica aplicada

Se utilizará para la organización de la bibliografía de este estudio, la Norma Bibliográfica Harvard.

Capítulo 1

Capítulo 1 . Fundamentos teóricos- conceptuales.

El capítulo presenta las premisas y definiciones que fundamentan la investigación. Se definen los conceptos de Producción Científica, utilizando el Análisis de Dominio y sus respectivos enfoques, y la temática Criptografía como dominio temático.

1.1. Producción Científica

Las publicaciones científicas son el reflejo de la actividad investigativa que desarrolla una persona, institución o país, asimismo, permite el intercambio de conocimientos mediante su difusión continua en revistas científicas indizadas en base de datos, tanto selectivas como exhaustivas, que brindan acceso a artículos, producto de investigaciones originales y otras formas de comunicación científica como reportes de casos y cartas al editor, constituyendo una fase esencial dentro del proceso de investigación y el más importante indicador de producción científica.

Los indicadores de producción científica son aquellos que muestran uno de los aspectos más importantes de la actividad investigadora, como es el crecimiento que experimenta una determinada disciplina, país, institución o grupo de investigación. A través de estos se pueden medir aspectos como la obsolescencia, colaboración, temática o tipología documental(Sanz et al., 2001).

Los indicadores bibliométricos de producción científica no son más que medidas que tiene su fundamento en el recuento de las publicaciones, con el fin de cuantificar los resultados científicos atribuibles a gentes determinados o agregados significativos de estos agentes.

Los indicadores bibliométricos presentan una serie de características que los identifican (Sanz et al., 2001). La parcialidad es la primera de ellas, puesto que cada indicador pone de manifiesto un aspecto de la evaluación que está siendo realizada. La convergencia también les identifica, ya que todos los

indicadores utilizados confluyen para proporcionar un conocimiento de la actividad científica objeto de análisis. Por esto, se recomienda utilizar un gran número de indicadores para evitar un conocimiento sesgado de una actividad multidimensional como es la científica, que no puede ser por tanto, caracterizada a partir de un indicador aislado. Por último, la información que aportan los indicadores es relativa a la disciplina estudiada, por lo que no puede ser extrapolada a otras, dado que los hábitos de investigación son distintos entre unas y otras.

El análisis de la actividad investigadora se complementa con el estudio de las referencias bibliográficas que aparecen en los documentos y de las citaciones que reciben los autores o documentos de otros posteriores. A partir de lo segundo se puede conocer un aspecto de gran interés, en la actualidad, para la evaluación científica; el impacto o visibilidad de la producción científica.

Por su parte el número de publicaciones constituye el indicador de producción más sencillo y el primero utilizado como indicador bibliométrico, se basa fundamentalmente en que mientras mayor sea la cantidad de documentos científicos publicados, mayor será el número atribuible de resultados obtenidos.

Es importante resaltar que el objetivo prioritario tanto de los indicadores de producción como de indicadores bibliométricos es permitir la comparación entre un conjunto de agentes o de agregados científicos, con el fin de detectar diferencias relevantes que sirvan para caracterizar el comportamiento de cada uno de ellos o del sistema del que pueden formar parte.

Los indicadores de producción establecen una conexión entre una colección de agentes científicos y sus correspondientes resultados o productos de la actividad que les es propia. Los recuentos de publicaciones son el medio que permite realizar esa conexión. Aunque su resultado bruto, el número de

publicaciones, puede ser directamente empleado como indicador de producción, existen limitaciones e inconvenientes que aconsejan efectuar transformaciones sobre esos recuentos para obtener indicadores con un ámbito de aplicación más extenso y menos problemático.

Los recuentos han de verse como una operación previa a la construcción de indicadores bibliométricos de este tipo, por lo que esta operación a de ser analizada con cierto detalle, pues de ella depende de un modo crítico, la validez de todo lo realizado a partir de sus resultados. Un examen minucioso propiciará las guías para la definición de indicadores, que permita que la investigación posea un mayor grado de credibilidad, lo que demuestra que, el procedimiento por el que se define una colección de agentes sobre el que se aplicará un indicador de producción; debe incluir un criterio claro y explícito que especifique cuales son los rasgos compartidos, o aquellos a los que se pueden recurrir como causantes de las diferencias que se observan.

Estos argumentos demuestran que la ciencia necesita mediciones para apreciar sus logros y precisar metas cuantificables que permitan trazar objetivos, por lo que las instituciones que ejercen un papel gerencial en esta área, deben organizar la documentación referente al número de sus publicaciones, patentes registradas, costo y efecto de la investigación.

1.2. El Análisis de Dominio para Los Estudios de Producción Científica

El análisis de dominio es considerado un nuevo paradigma de la Ciencia de la Información (CI), que postula que la mejor forma de entender los dominios de conocimiento es analizándolos como comunidades discursivas, puesto que la organización del conocimiento, su estructura, los patrones de cooperación, el lenguaje, los modos de comunicación y los criterios de relevancia de un dominio determinado son un fiel reflejo de esas

comunidades y del rol que desempeñan en la sociedad (Hjorland and Albrechtsen, 1995).

Tras la propuesta de Hjorland y Albrechtsen (1995), conocida como Análisis de dominio, subyace la idea de que puede considerase como el entramado de relaciones e interacciones que se establece entre los autores y científicos que comparten estructuras de pensamiento, patrones de cooperación y lenguaje y formas de comunicación en un entorno laboral, social, económico y político dados. Por tanto, la producción científica, las relaciones de colaboración y las diferentes asociaciones entre las citas bibliográficas de los trabajos científicos pueden constituir reflejo del dominio y utilizarse para su análisis.

Un dominio en un sentido amplio, es una comunidad de discurso vinculada a cualquier ámbito en el que se desarrolla una actividad. Es un conjunto de actores que comparten algo en común, más el entramado de relaciones que se establece entre ellos. Lo cual en los estudios de producción científica permite cuantificar mediante indicadores bibliométricos los resultados atribuibles a los métodos y enfoques utilizados, propiciando a este tipo de estudios datos precisos y confiables, teniendo en cuenta que la base de este y de los otros indicadores de producción es, en circunstancias equivalentes a mayor cantidad de documentos científicos publicados, mayor número atribuible de resultados obtenidos.

Por su parte en los dominios temáticos, como una disciplina o especialidad científica, los miembros de la comunidad comparten objetivos comunes, un cuerpo de conocimientos especializados, mecanismos de intercomunicación, participación y medios de comunicación establecidos como revistas científicas de la especialidad, un vocabulario especializado**.**

En los dominios científicos geográficos, como es el caso de un país, las comunidades comparten además, y entre otros, un mismo contexto político, social, económico y cultural (Subramanyam, 1983).

Ello hace que más allá de la universalidad de las formas fundamentales del pensamiento y prácticas disciplinarias, cada país vaya configurando su propio estilo de hacer ciencia en función de las peculiaridades de una práctica científica condicionada por el contexto en la que ésta se lleva a cabo (Vessuri, 1995).

1.2.1. Enfoques del Análisis de Dominio

1. Según Hjorland, (2002). Las guías de literatura organizan fuentes de información en un dominio en correspondencia con sus tipos y las funciones que sirven. Hacen énfasis en descripciones ideográficas de fuentes de información y descripciones de cómo las fuentes complementan unas a otras, ofreciendo un tipo de perspectiva sistémica.

Son publicaciones que listan y describen el sistema de recursos de información en una o más áreas. Una guía es un tipo de bibliografía de documentos en un dominio, pero se desvía de las típicas bibliografías temáticas, porque primero, se concentra en literatura de referencia (bibliografías, diccionarios, enciclopedias, etc.) a costa de la literatura primaria. Es selectiva (más o menos) mientras que por ejemplo, una bibliografía de bibliografías tiende a ser exhaustiva. Aclara las debilidades y fortalezas de diferentes trabajos, y debe proveer la base para una sección racional de trabajos para usar y ayudar al usuario a navegar en la literatura, bases de datos e información.

Los trabajos de este tipo están poco representados en las revisiones de libros que aparecen en las publicaciones científicas en las Ciencias de la Información y los autores/compiladores son poco citados. Otro problema radica en que estos trabajos consumen mucho tiempo y se tornan obsoletos muy rápidamente, aunque también tiene lados fuertes por lo que es

conveniente conocer las fuentes de información más importantes en uno u otro dominio a un nivel de detalle relativamente alto, ya que tiene mucha relevancia para el trabajo informativo práctico.

Las investigaciones en esta área pueden aportar beneficios al combinarse con otros enfoques del análisis de dominio, en particular:

- La producción de clasificaciones especiales
- Los documentos y los estudios de genero
- Los estudios críticos y epistemológicos y
- Los estudios acerca de estructuras e instituciones en la comunicación científica

Por tanto puede decirse que las Ciencias de la Información necesitan producir guías temáticas de calidad y desarrollar criterios de cómo explicar y evaluar ese trabajo así como combinarlo con otros enfoques del análisis de dominio, ya que una guía es una explicación de lo que hacen los bibliotecarios cuando forman colecciones y las aprenden a usar para ofrecer servicios de referencia.

2. Las clasificaciones especiales y los tesauros (especialmente los de enfoque basado en facetas) organizan las estructuras lógicas de categorías y conceptos en un dominio así como las relaciones semánticas entre conceptos.

Tanto los sistemas de clasificación como los tesauros consisten básicamente en conceptos centrales de un dominio, organizados de acuerdo a las relaciones semánticas como las genéricas y de asociación, lo que permite establecer diferencias entre los sistemas de clasificación para documentos (sistemas de clasificación bibliográficos) y los sistemas de clasificación para los objetos de estudio de diferentes disciplinas tales como animales, enfermedades mentales, elementos químicos, períodos históricos, etc. Las clasificaciones por tanto, están muy conectadas con las teorías científicas.

La investigación en la clasificación de dominios temáticos puede recibir beneficios al combinarla con otros enfoques hacia el análisis de dominio, en particular con:

- La investigación en las especialidades de indización y recuperación
- Estudios bibliométricos
- Estudios históricos
- Estudios epistemológicos y críticos y
- Estudios terminológicos y lenguajes para propósitos específicos (LSP)

Podría decirse entonces que la investigación en clasificación con frecuencia se considera como arrinconada en BCI, por lo que se necesita ampliar la perspectiva y tomarlo con más seriedad como campo de investigación ya que parece compartir muchas de las debilidades y fortalezas con la producción de guías temáticas; pues tiene un alto valor práctico pero es dificultoso y consumidor de tiempo y además tiene muy poco reconocimiento académico.

3. Las especialidades de indización y recuperación organizan documentos sencillos o colecciones para optimizar la recuperabilidad y visibilidad de sus "potencialidades epistemológicas" especificas.

En las bases de datos temáticas, se indizan mensualmente miles de documentos y esta indización está abierta a estudios mediante diferentes métodos. Las investigaciones acerca de la indización, la representación del documento y su recuperación deben evaluar las malas prácticas y mejorarlas. Si esto no se hace, se hace difícil argumentar para investigaciones ulteriores en esta área.

A menudo los especialistas en bibliotecología e información sienten que les faltan conocimientos adecuados acerca de un campo temático por lo que hay que desarrollar suficiente conocimiento temático en al menos un campo de estudio (por ejemplo, la propia BCI) con el fin de demandar la existencia de un campo de estudios lo suficientemente serio, puesto que la aplicación

de los principios de BCI a una tarea específica puede hacer más relevante y realista la investigación en Ciencia de la Información (CI), aunque es importante mencionar que solo unas pocas escuelas de BCI ofrecen grados avanzados en Ciencias de la Información, motivo por el cual parece ser una necesidad obvia fortalecer y ampliar estas iniciativas.

Estas investigaciones pueden aportar beneficios mediante la cooperación con otros tales como:

- Producción de clasificaciones especializadas y tesauros
- Estudios bibliométricos
- Estudios epistemológicos y críticos y
- Estudios terminológicos, lenguajes para propósitos específicos (LSP), estudios del discurso.

4. Los estudios empíricos de usuarios pueden organizar dominios según la preferencia o comportamiento o los modelos mentales de sus usuarios.

Los estudios empíricos acerca de los usuarios también han sido enaltecidos sobre la creencia de que los especialistas en información pueden aprender lo que necesitan conocer acerca de la información de los usuarios, ya que estos deben ser los expertos en la organización y búsqueda de información y que esta se necesita para solucionar un problema dado, pues no es una cuestión psicológica, sino teórica/filosófica. Esto significa que los usuarios no saben que documentos buscar y cuando han encontrado la información que necesitan, pueden ser incapaces de reconocer esto. Los científicos de la información no deben esperar aprender como organizar y buscar información mediante la consulta o el estudio de sus usuarios, por el contrario: cualquier interpretación del comportamiento de los usuarios debe presuponer un principio prioritario en la CI.

Por tanto los estudios empíricos de usuarios pueden representar un enfoque importante para el análisis de dominio en la CI si están informados por teorías apropiadas. Ellos pueden, por ejemplo, proveer información acerca

de diferencias en las necesidades de información en diferentes comunidades y deben estar combinados con otros enfoques como:

- Estudios bibliométricos
- Estudios epistemológicos y críticos; y
- Estudios acerca de las estructuras e instituciones en la comunicación científica.

5. Los estudios bibliométricos organizan patrones sociológicos de reconocimiento explícito entre documentos individuales.

La bibliometría es una interesante área de estudio aunque es muy disputado su empleo como un instrumento en la evaluación de la investigación. Puede ser empleada en diferentes formas, como una herramienta y como un método en el análisis de dominios. Por ejemplo se ha vuelto popular para hacer mapas bibliométricos o visualizaciones de áreas científicas a partir del análisis de co-citación. Un ejemplo bien conocido es el de White y McCain (1998) quienes explícitamente se refirieron a ellos como análisis de dominio y conocimiento.

La bibliometría es un enfoque fuerte porque muestra muchas conexiones reales y detalladas entre documentos individuales (Hjorland, 2002). Estos vínculos representan el reconocimiento explicito de los autores de la dependencia entre, por ejemplo, trabajos, investigadores, campos, enfoques y regiones geográficas.

La bibliometría es un fuerte enfoque para el análisis de dominio por ser empírico y basarse en el análisis detallado de las conexiones entre documentos individuales. Se necesita considerar diferentes sesgos en forma muy cuidadosa. Además, para interpretar adecuadamente el análisis bibliométrico, se necesita conocimientos de otros tipos, que incluyan:

- Estudios históricos y
- Estudios epistemológicos y críticos.

6. Los estudios históricos organizan las tradiciones, los paradigmas así como los documentos y formas de expresión y sus influencias mutuas.

Los métodos históricos y sus estudios no se han empleado mucho en la Ciencia de la Información y son, sin embargo, relevantes en una forma mucho más amplia y profunda. Mientras que la historia de la ciencia en general es demasiado amplia para ser considerada parte de la Ciencia de la Información, se puede hacer una distinción entre los estudios históricos ordinarios de dominio temático por una parte y los estudios históricos que hacen énfasis en el desarrollo de la terminología, categorías, literaturas, géneros, sistemas de comunicación, por otra parte. En la última parte mencionada puede verse como un acercamiento al análisis de dominio en la CI. Por dicho motivo no solo se deben considerar los estudios históricos como una vía para celebrar un campo y darle un status superior.

Los métodos históricos deben ser considerados como métodos sustanciales en la CI. Cuando se trata de comprender documentos, organizaciones, sistemas, conocimientos e información, una perspectiva histórica y métodos históricos permiten proveer una perspectiva más profunda y más coherente en comparación con tipos no-históricos de investigación de naturaleza mecanicista.

7. Los estudios de documentos y géneros revelan la organización y estructura de diferentes tipos de documentos en un dominio.

Los conceptos de arquitectura de información (AI) así como géneros y estructuras informativas se han tornado importantes en la ciencia de la información y campos relacionados, parcialmente debido a la introducción de sistemas de recuperación a texto completo, sistemas de recuperación de "pasadizos" así como sistemas hipertexto basados en HTML en Internet.

Estos importantes conceptos necesitan basarse en teorías más generales acerca de los documentos, sus propósitos y funciones comunicativas, sus elementos y composición y sus valores potenciales en la recuperación de

información. Diferentes disciplinas o comunidades discursivas desarrollan tipos especiales de documentos como una adaptación a sus necesidades específicas. Ejemplos de tipos de documentos únicos son:

- En la música: las partituras de música;
- En geografía: los mapas y los atlas
- En el derecho: los códigos; y cuerpos legales
- En astronomía: los almanaques
- En genealogía: los pedigríes y árboles genealógicos y
- En psicología: los test.

El estudio de las estructuras documentales y géneros ha sido algo descuidado en CI, pero algunos desarrollos recientes en la recuperación a texto completo lo han traído a un primer plano. Los estudios cualitativos y cuantitativos de diferentes géneros en diferentes comunidades, puede proveer servicios de información más ricos y diferenciados. Como una vía para el análisis de dominio, debe verse combinado con otros enfoques como:

- Investigaciones en la indización y la recuperación
- Estudios históricos
- Estudios epistemológicos y críticos

8. Los estudios epistemológicos y críticos organizan el conocimiento de un dominio en "paradigmas" según sus presupuestos básicos acerca del conocimiento y la realidad.

Los estudios epistemológicos son estudios que examinan los supuestos explícitos o implícitos que respaldan tradiciones investigativas. Tales supuestos con frecuencia se vinculan a creencias ontológicas relativas al objeto de estudio. Representan un análisis de los enfoques o paradigmas en campos investigativos. Los estudios epistemológicos de dominios de conocimiento frecuentemente se combinan con estudios históricos. Esto incluye estudios de cómo se han recibido determinados trabajos (estudios

de recepción, en particular aquellos de naturaleza más histórica y social en contraposición a estudios de recepción de naturaleza más psicológica).

Los estudios de este tipo también son valiosos para la interpretación de patrones bibliométricos porque los investigadores que trabajan bajo un punto de vista especifico tienen una tendencia muy alta a citar a otros investigadores que comparten por mismos presupuestos básicos y visión mundial (Hjorland, 2002). Pueden por otra parte beneficiarse de los estudios bibliométricos por tanto hay una interacción mutua.

Puede decirse que los estudios epistemológicos y críticos de los dominios de conocimiento proveen el conocimiento acerca de los fundamentos de los dominios y las evaluaciones críticas de sus demandas. Proveen lineamientos críticos para la selección, organización y recuperación de información y proveen el nivel de generalidad más alto acerca de las necesidades de información y los criterios de relevancia que puedan obtenerse. Todos los otros enfoques hacia el análisis de dominio se tornan superficiales si se abandona la epistemología.

9. Los estudios terminológicos, los lenguajes para propósitos específicos (LSP) y los estudios del discurso organizan palabras, textos y enunciados en un dominio siguiendo criterios semánticos y pragmáticos.

Los profesionales de información siempre han tenido una intima relación con los problemas asociados a la terminología, las relaciones semánticas y problemas similares de naturaleza lingüística. La construcción de tesauros, los problemas relativos a la eficacia de la recuperación de los lenguajes naturales y controlados son ejemplos obvios de esta relación. Pueden existir diferentes razones para la relativa falta de contacto entre la CI y la lingüística y una razón fundamental tiene que ver con los problemas teóricos fundamentales de la propia lingüística. Los lingüistas han estado reacios a considerar los sublenguajes (o lenguajes para propósitos especiales, LSP), los lenguajes propios y objetos de estudio.

En las Ciencias de la Información los LSP y la semántica de las bases de datos en la CI han sido hasta el presente de naturaleza teórica y se relaciona con cuatro presupuestos básicos (Hjorland, 2002):

1. Los signos y su significado se forman por grupos sociales, primariamente como parte de la división social del trabajo en la sociedad. Tales comunidades discursivas pueden ser de diferentes tamaños y estructuras. Un gran número de grupos puede desarrollar sistemas de símbolos y compartir conocimiento, que no comparten con el resto de la sociedad. Tanto en la ciencia como en las humanidades puede existir un grado considerable de conocimiento común y significados compartidos.
2. Diferentes comunidades desarrollan tipos específicos de documentos de más o menos diferente composición. Todos los elementos en esos documentos son potencialmente puntos de acceso temático en la recuperación electrónica. El valor informativo de un punto de acceso específico es relativo a las convenciones usadas en un dominio específico o en una tradición.
3. Las comunidades discursivas o epistémicas supramencionadas siempre reciben influencia de varias normas y tendencias epistemológicas, que también ejercen influencia en la construcción social de sistemas simbólicos, medios, conocimiento, significado y distancias semánticas. Tales epistemologías son probablemente los modelos explicativos mas general que están disponibles.
4. Cuando los documentos son insertados en las bases de datos, se pierde la información acerca de los significados implícitos procedentes de los contextos previos. Mientras mayor sea el grado de inserción mayor será la perdida de información implícita. Los sistemas para la organización del conocimiento y la recuperación de información deben

ser desarrollados para poder con esta perdida de información implícita haciéndola explicita (semántica de las bases de datos).

Por tanto el lenguaje y la terminología son dos objetos muy importantes para la CI porque afectan nuestro pensamiento y también a las preguntas que hacemos a las bases de datos así como a los textos que buscamos. La CI necesita de una base funcional/pragmática para estudiar los LSP. La terminología como un enfoque de los estudios de dominio en la CI puede ser combinada con:

- estudios bibliométricos
- estudios históricos y
- estudios epistemológicos y críticos.

10. Los estudios de estructuras e instituciones en la comunicación científica organizan a los actores e instituciones principales siguiendo la división interna del trabajo en el dominio.

El estudio de la comunicación, interna en dominios y externa entre dominios puede estar inspirada por diferentes teorías sociológicas, incluidos el análisis del discurso, la teoría de sistemas o la teoría de auto-organización (Leydersdorff, 2000; citado en Hjorland, 2002).

Esta perspectiva puede ser útil también para la CI e indica como el estudio de estructura e instituciones en la comunicación científica esta relacionado con puntos de vista sociológicos, por cuyo motivo puede decirse que el estudio de las estructuras de la división interna del trabajo dentro de los dominios y el intercambio de información entre dominios provee información útil para la comprensión de la función de tipos específicos de documentos y servicios de información y para la construcción de guías de literatura. Este campo es rico en preguntas que aun están abiertas entre otros tipos de estudios, a investigaciones bibliométricas.

11. El análisis de dominio en la cognición profesional y la inteligencia artificial provee modelos mentales de un dominio o métodos para la elicitación del conocimiento para producir sistemas de expertos.

El análisis de dominio es un método utilizado en el desarrollo de sistemas y en la ingeniería de software. Centra la atención en capturar tanto los aspectos comunes y la variabilidad de los sistemas dentro de un dominio para mejorar la eficacia del desarrollo y mantenimiento de estos sistemas. Los resultados del análisis, conocidos colectivamente como el modelo de dominio, se capturan para su reempleo en el desarrollo futuro de sistemas similares. Hay varias formas de definir "dominio". Por ejemplo, Berard (1992) hace dos caracterizaciones (Hjorland, 2002):

1. Una colección de aplicaciones (software) en curso y futuras que comparten un conjunto de características comunes.
2. Un conjunto bien definido de características que describen estrecha y totalmente pero con precisión, una familia de problemas para los cuales se buscan y buscaran soluciones mediante aplicaciones computacionales.

Los conceptos de dominio y análisis de dominio son más estrechos en la ciencia de la computación que los conceptos correspondientes en la CI discutidos en este trabajo. Hay una superposición obvia en intereses, especialmente vinculados a los problemas relativos a la terminología y el significado. La perspectiva básica de que un sistema o servicio debe reflejar un dominio (oponiéndose a las "estructuras mentales") es también la misma.

Estos enfoques juntos forman una perspectiva única para la Ciencia de la Información, la cual ofrece investigaciones prácticas y teóricas, pues esta

combinando podrá fortalecer la identidad de la esta y la relación entre la investigación y la práctica.

En el caso especifico de la presente investigación, serán utilizados los enfoques dirigidos a los estudios empíricos de usuarios pueden organizar dominios según la preferencia o comportamiento o los modelos mentales de sus usuarios y los estudios bibliométricos organizan patrones sociológicos de reconocimiento explícito entre documentos individuales.

1.3. La Criptografía como dominio temático

La Criptografía es la Ciencia sobre los modos o maneras de transformación de la información con el objetivo de su defensa o protección de las acciones de los malhechores (intrusos), es una rama de las investigaciones científicas, técnico-ingenieras y de actividades prácticas, que se dedica a la elaboración, desarrollo, análisis y argumentación de la fortaleza de los medios criptográficos de protección de la información de las amenazas del enemigo. Los problemas fundamentales de la Criptografía son garantizar el secreto o la confidencialidad, la integridad, la autentificación, la imposibilidad de repulsa (no repudio) y la no suplantación. La criptografía es el estudio de los métodos de enviar mensajes codificados de modo que sólo el receptor (en posesión de la clave) sea capaz de comprenderlo. Así mismo el criptoanálisis se dedica al estudio inverso, es decir, al estudio de las formas de decodificar mensajes en clave (desconociendo ésta).

1.3.1. Terminología Empleada

En muchos libros sobre Criptografía aparecen términos como encriptar y desencriptar, aunque ambos son neologismos erróneos adoptados con toda probabilidad del verbo anglosajón encrypt y decrypt todavía sin reconocimiento académico (Fúster et al., 2004).

En la jerga de la criptografía, la información original que debe protegerse se denomina texto en claro o texto plano. El cifrado es el proceso de convertir el texto plano en un galimatías ilegible, denominado texto cifrado o criptograma (Abadi and Warinschi, 2008).

Por lo general, la aplicación concreta del algoritmo de cifrado (también llamado cifra) se basa en la existencia de una clave: información secreta que adapta el algoritmo de cifrado para cada uso distinto. Cifra es una antigua palabra arábiga para designar el número cero; en la Antigüedad, cuando Europa empezaba a cambiar del sistema de numeración romano al arábigo, se desconocía el cero, por lo que este resultaba misterioso, de ahí probablemente que cifrado signifique misterioso (Lucera, 2010).

Las dos técnicas más sencillas de cifrado, en la Criptografía clásica, son la sustitución (que supone el cambio de significado de los elementos básicos del mensaje, las letras, los dígitos o los símbolos y la transposición, que supone una reordenación de los mismos); la gran mayoría de las cifras clásicas son combinaciones de estas dos operaciones básicas.

El descifrado es el proceso inverso que recupera el texto plano a partir del criptograma y la clave (Fúster et al., 2004). El protocolo criptográfico especifica los detalles de cómo se utilizan los algoritmos y las claves (y otras operaciones primitivas) para conseguir el efecto deseado. El conjunto de protocolos, algoritmos de cifrado, procesos de gestión de claves y actuaciones de los usuarios, es lo que constituyen en conjunto un criptosistema, que es con lo que el usuario final trabaja e interactúa. Por tanto podemos decir que el hecho de codificar un mensaje para que sea secreto se llama cifrado. El método inverso, que consiste en recuperar el mensaje original, se llama descifrado.

Esto permite decir que la Criptografía tiene como objetivo enmascarar las representaciones caligráficas de una lengua de forma discreta (Sosa, 2010).

La siguiente figura muestra este proceso:

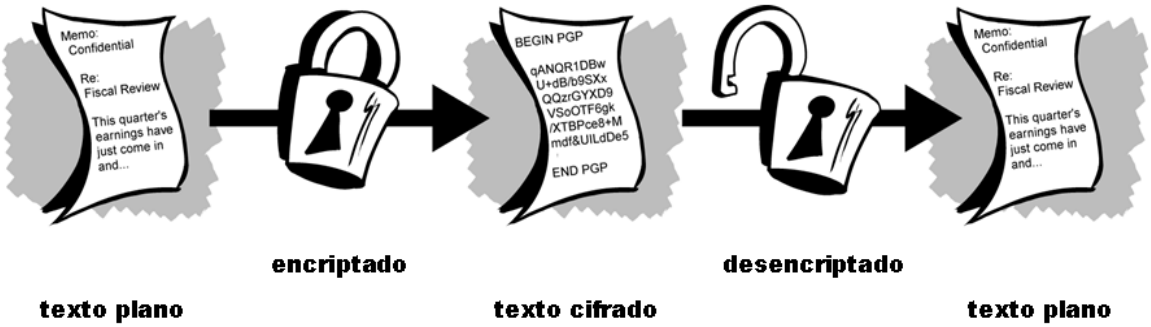

Gráfico 1: Proceso de enmascaramiento de la información (Sosa et al., 2011).

Diríamos entonces que la **Criptografía** es la ciencia que emplea las matemáticas para encriptar y desencriptar datos y permite almacenar información sensible o transmitirla a través de redes inseguras (como Internet) de forma que no puede ser leída por nadie más que quien debe leerla.

Mientras que la **Criptografía** es la ciencia que se encarga de asegurar la información, el **Criptoanálisis** es la ciencia que analiza y rompe comunicaciones seguras (Aguilar and Oktaç, 2004). El criptoanálisis clásico requiere una interesante combinación de razonamiento analítico, aplicación de herramientas matemáticas, búsqueda de patrones, paciencia, determinación y suerte.

En la actualidad se emplean diferentes tipos de Criptografía (de Bustos, 2001), tales como:

- **Criptografía estratégica:** Actualmente su aplicación se ha extendido a diversas actividades basadas en el uso de la tecnología de la información y las comunicaciones (TIC) constituyéndose en elemento indispensable para garantizar la seguridad en el manejo de la información. Estas herramientas han permitido proteger cada

caracter con una llave que puede conformarse hasta por 256 bits. Es decir, que para encontrar esta llave en particular, tendríamos que buscarla entre combinaciones posibles".

- **La Criptografía simétrica**, es en donde se usa la misma contraseña o llave para encriptar y para desencriptar la información. El usar la misma llave para encriptar y para desencriptar es un problema a la hora de enviar datos, ya que el remitente debe enviar previamente la llave al destinatario para que éste pueda desencriptar la información, y debe hacerlo por un canal seguro. Por lo tanto la Criptografía simétrica se emplea especialmente para almacenamiento seguro de datos (solamente una persona necesita la llave). Para envío de datos es preferible la Criptografía asimétrica".
- **La Criptografía asimétrica**, que emplea un esquema de llave pública y llave privada. La información se encripta con la llave pública, y se desencripta con la llave privada. No presenta el problema de transmisión de la llave que tiene la Criptografía simétrica, ya que la llave pública no sirve para desencriptar la información.

Es importante destacar que en los procesos de intercambio de archivos es necesario proteger el archivo para asegurarse que no sea modificado en el camino, y para ello existen 2 formas (Fúster et al., 2004):

- **Encriptado con clave**: Una forma fácil y segura es el encriptado del documento, el cual entrando una palabra clave que sirve como llave para encriptar el documento, se genera entonces un archivo ilegible, que no puede ser leído por ninguna aplicación mientras no se desencripte con la misma clave original.
- **Encriptado con firma segura**: Una segunda forma es encriptar el archivo original y producir un archivo que certifique su autenticidad

con una firma digital. También se puede incluir en un mismo archivo la firma digital y el texto encriptado.

En este aspecto es importante mencionar entre los pilares más importantes de la Seguridad Informática, la conocida Teoría de la Información (Lucera, 2010), que no es más que un estudio de la cantidad de información contenida en los mensajes y claves, así como su entropía; la Teoría de los Números que es el estudio de las matemáticas discretas y cuerpos finitos que permiten las operaciones de cifrado y descifrado; la Teoría de la Complejidad de los Algoritmos que es el estudio de la clasificación de los problemas como computacionalmente tratables o intratables.

La Teoría de la Información mide la cantidad de información que contiene un mensaje a través del número medio de bits necesario para codificar todos los posibles mensajes con un codificador óptimo (Fúster et al., 2004), y esta cantidad de información puede medirse:

1. En función de la extensión del mensaje: Ante una pregunta cualquiera, una respuesta concreta y extensa nos entregará mayor información sobre el tema en particular, y diremos que estamos ante una mayor "cantidad de información".
2. En función de la utilidad del mensaje: Ante una pregunta cualquiera, una respuesta más útil y clara nos dejará con la sensación de haber recibido una mayor "cantidad de información".
3. En función de la sorpresa del mensaje: Ante una pregunta cualquiera, una respuesta más inesperada y sorprendente, nos dará la sensación de contener una mayor "cantidad de información".
4. Dependencia del entorno (sorpresa): Ante una pregunta cualquiera, una respuesta inesperada y sorprendente en el entorno, nos dará la sensación de contener una mayor "cantidad de información".

5. En función de la probabilidad de recibir un mensaje: este enfoque probabilístico es el que nos interesará en cuanto a la definición de Cantidad de Información.

Capítulo 2

Capítulo 2 : Diseño Metodológico de la Investigación.

El presente capítulo aborda los componentes metodológicos de la investigación, se especifica el tipo de estudio desarrollado, así como las etapas investigativas por las que se ha ido transitando. Se aclaran además los métodos y las técnicas empleados, las categorías analíticas, el universo o población objeto de estudio y el tipo de muestra escogida. Por ultimo se presentan las principales técnicas de análisis de dominio que serán empleadas.

2.1. Diseño metodológico

La presente investigación se considera un estudio de tipo descriptivo. Este criterio se sustenta con el análisis de la Producción Científica sobre Criptografía en los años 2008, 2009, 2010, 2011 y 2012, que demuestran cuál ha sido el desarrollo de esta ciencia y la relevancia su estudio y dominio para posteriores investigaciones.

2.1.1. Tipo de investigación

Según la tipología de investigaciones que propone Hernández et al., (2006), la presente investigación se considera un estudio con enfoque cuantitativo predomínate. Criterio que se respalda en la medida que se pretende describir y conocer el desarrollo de la Criptografía en los años comprendidos entre 2008 y 2012, a partir de un estudio bibliométrico de la Producción Científica de la misma, centrado en los enfoques establecidos para el Análisis de Dominio.

2.1.2. Métodos Investigativos

Para la recogida de información se utilizaron varios métodos.

Métodos del Nivel Teórico

Analítico-sintético: El método consta de dos etapas para el desarrollo de la investigación, en primer lugar el análisis contribuyó a realizar un estudio de los contenidos necesarios para la comprensión del tema que se aborda y la necesidad del examinar la producción científica sobre Criptografía desde la perspectiva de análisis de dominio. La síntesis permitió un acercamiento a la concepción de la comunicación como habilidad mediatizada fomentando los conocimientos claves obtenidos de la revisión bibliográfica y favoreciendo la exposición de criterios y nexos necesarios para determinar la medida en la que ha sido investigada dicha temática. Este método facilita la conformación del capítulo teórico-metodológico como unidad dialéctica de estudio, mostrando las técnicas necesarias para la realización de la investigación.

Inductivo-deductivo: Primeramente la inducción particulariza en los conocimientos generales obtenidos, reflejando a través de la intuición las principales temáticas que hay en común, para delimitar las investigaciones individuales que, a su vez conforman la ciencia criptográfica. Ayudó a determinar cuáles son las investigaciones medulares que rigen el desarrollo de la Criptografía, así como los estudios que intentan convertirla en una ciencia al alcance de todos. La deducción admite llegar a conclusiones y razonamientos lógicos partiendo de un estudio general a cuestiones precisas, a partir de una visión particular que enriquece el estudio del fenómeno desde las Ciencias de la Información con perspectiva interdisciplinar.

Histórico-Lógico: Este método posibilitó indagar cómo se ha desarrollado la Criptografía desde sus inicios hasta la actualidad, y la medida en la que ha sido utilizada por otras ciencias. Por ende contribuye a expresar una serie de ideas que destacan las ventajas y desventajas del estudio y conocimiento de esta ciencia, ayudando a la comunidad científica dedicada

a este tipo de investigaciones a tener un punto de apoyo determinante en la visión y comprensión de dicho fenómeno, teniendo en cuenta que las investigaciones hasta hace relativamente poco tiempo han sido tratadas como secretos militares.

Sistémico-Estructural: Este método ayuda a ver todo de forma integral, con sus estructuras y relaciones, pues a pesar de no ser utilizados todos los enfoques de análisis de dominio se tiene en cuenta la relevancia de cada uno y su influencia en la presente investigación y en otras que podrán ser realizadas con posterioridad, ya que ha habido un crecimiento espectacular de la tecnología criptográfica.

Métodos del Nivel Empírico

Análisis documental: El elemento teórico de la investigación se sustentó en la consulta de la literatura especializada en el tema y otras fuentes de información relacionadas con el objeto y campo de estudio para favorecer la aproximación al contexto que se investiga. Los documentos que se toman como fuente bibliográfica fundamental para este estudio son: Libro de Introducción a la Criptografía de José Ángel de Bustos; El artículo Análisis de dominio en Ciencias de la Información -once enfoques- tradicionales e innovativos de Birger Hjorland; La gestión de información en el grupo de Criptografía de la UCLV desde la visión de las Ciencias de la Información, de Yaniceli Sosa Avalos, Aida María Torres y Guillermo Sosa Gómez; entre otras, cuyo estudio es la génesis de los resultados que se obtienen.

Método de Análisis de Dominio: Se utilizó el método bibliométrico derivado de los enfoques establecidos para el análisis de dominio con el fin de organizar patrones sociológicos de reconocimiento explícito entre documentos individuales. Este enfoque se combina con los estudios empíricos de usuarios, los cuales pueden organizar dominios según la preferencia o comportamiento o los modelos mentales de sus usuarios. La

combinación de estos enfoques suple las necesidades informativas de la muestra seleccionada y complementa el análisis referente a la producción científica estudiada, con el fin de obtener metas cuantificables.

Métodos matemáticos estadísticos: El método estadístico se emplea en la utilización de los indicadores bibliométricos y sus aristas (diferentes técnicas y métodos referentes a la metría), así como para el análisis porcentual, lo cual dará a la investigación un alto valor y credibilidad en cuanto a resultados obtenidos se refiere.

Encuesta: Este método hizo posible conocer el avance de las investigación realizadas referente a la temática, y ayudó a la recopilación adecuada y rápida de los datos necesarios para determinar cuáles son las principales líneas de investigación de la muestra seleccionada, así como sus principales publicaciones y redes de colaboración, facilitando de este modo la confección de la Base de Datos que será utilizada para el análisis de la Producción Científica.

2.1.3. Técnicas de recogida de la información

Con fines exclusivamente investigativos, se llevó a cabo un proceso de búsqueda entre los meses de Enero/Marzo del año 2013, utilizando como fuente el Google Scholar. Es utilizada esta base de datos porque en un inicio se realizó la búsqueda en SCOPUS y los documentos recuperados, estaban relacionados con las palabras claves utilizadas en Español e Ingles, pero carecían de relevancia con respecto a la temática estudiada que en este caso es la principal línea de investigación del grupo científico dirigida a los Algoritmos Criptográficos de cifrado en flujo. La carencia de documentos encaminados hacia esta línea hace necesario realizar la búsqueda en esta otra base de datos ya mencionada con anterioridad.

Para dicha búsqueda se seleccionaron todos los registros correspondientes a los años 2008, 2009, 2010, 2011, 2012. Los resultados arrojados permitieron identificar documentos como artículos de revista, tesis y monografías o libros, fundamentalmente.

La estrategia diseñada para recuperar la información tuvo en cuenta varias categorías tales como:

En español: Criptografía, Encriptado de información, Algoritmos criptográficos. Con estas se obtuvo un total de 225 documentos, de los cuales fueron eliminados 107, de estas 27 estaban repetidas y 80 no presentaban gran relevancia para el estudio; dejando finalmente un total de 118 documentos distribuidos entre artículos de revista, monografías o libros y tesis fundamentalmente.

En Ingles: Cryptography, Cryptographyc Algorithms, Encrypted Information. Estas categorías facilitaron la obtención de 241 documentos de los que fueron eliminados 115; por estar repetidos se descartaron 46 y por no tener relación con la temática 69, lo cual arrojó un total de 126 documentos destacando se entre ellos los artículos de revista, aunque también se pueden encontrar memorias de congresos y tesis.

Ambas estrategias en su totalidad proyectaron 466 documentos, de los cuales 73 fueron eliminados por estar repetidos; dejando un total de 393 documentos, que después de ser revisados, se descartaron 149 por no presentar información relevante sobre la temática; arrojando finalmente un total de 244 documentos con información notable sobre el tema investigado.

Para procesar los documentos que arrojó la búsqueda, se utiliza el Zotero como herramienta para el procesamiento de datos y el Microsoft Excel para calcular los indicadores que proyectan los diferentes resultados de la investigación.

Además se utiliza el Bibexcel, teniendo en cuenta que es un programa especializado en el procesamiento y análisis de información y Bases de Datos, con el fin de confeccionar una matriz de co-ocurrencia (redes de colaboración y temática).

2.1.4. Selección del universo y la muestra

Universo o población: Estudiantes y profesores que investigan la temática Criptografía.

Selección de la Muestra

Para este criterio se tuvo en cuenta el tipo de muestra dirigida (no probabilística) teniendo en cuenta que se utiliza un criterio de selección informal y un poco arbitrario, donde la muestra a seleccionar, en este caso son los 7 estudiantes y 4 profesores pertenecientes al Grupo científico de Criptografía de la UCLV puesto que estos son los más especializados en la temática que se aborda y en el propio desarrollo de las investigaciones que hasta el momento son llevadas a cabo en el centro del país, por lo que es válida este tipo de muestra y requerida para investigaciones de esta índole, donde los resultados son aplicables solamente a la muestra en sí, y no existe una generalización ni extrapolación a otra población.

2.2. Etapas de la investigación

Toda investigación transita por tres fases o etapas indispensables (Hernández et al., 2006). Dichas etapas dependen una de la otra, por lo cuál ninguna debe ser omitida, y se precisa conservar el orden en que han sido establecidas originalmente, puesto que serán utilizadas para describir el desarrollo del estudio y con ello alcanzar los objetivos propuestos.

Fase preparatoria o inicial:

Esta etapa vislumbró una investigación teórica acerca de la temática estudiada, mediante una revisión bibliográfica y la aplicación de algunas herramientas para la recuperación de la información, con el fin de cumplir los objetivos propuestos y detallar la importancia del objeto y campo que se investiga, enfatizando fundamentalmente en el análisis de la producción científica sobre Criptografía y la importancia de conocer el dominio de esta ciencia. Se especifican los métodos y técnicas manejados en la investigación y se determinan los enfoques que son utilizados, siendo estos:

- Los estudios empíricos de usuarios, que consideran los dominios y tradiciones como factores importantes en el comportamiento informacional y son aplicables porque hacen posible proveer información acerca de las diferencias existentes en las necesidades de información en distintas comunidades.
- Los estudios bibliométricos, que constituyen un enfoque fuerte porque muestra muchas conexiones reales y detalladas entre documentos individuales. Por lo que estos vínculos representan el reconocimiento explicito de los autores de la dependencia entre trabajos, investigadores, campos, enfoques y regiones geográficas respectivamente.

Finalmente se procede a determinar el tipo de investigación, la unidad de análisis, la población, la muestra y atendiendo al problema de investigación se operacionalizan las variables.

Intervención:

En esta etapa se realizó un estudio detallado del grupo científico de Criptografía perteneciente a la Universidad Central "Marta Abreu" de Las Villas y se aplica la encuesta a la muestra seleccionada, para obtener los elementos relacionados con la variable que se investiga.

Análisis de los resultados:

En esta etapa se presentan los resultados obtenidos en la investigación, para lo cual, se hizo necesario confeccionar una Base de Datos que permitió analizar la producción científica sobre Criptografía del 2008 al 2012.

Esta Base de Datos fue normalizada, teniendo en cuenta primeramente la revisión de los documentos para corroborar su relevancia, partiendo de que estos deben responder a las principales líneas de investigación de la muestra seleccionada, que en este caso son los Algoritmos Criptográficos de cifrado en flujo.

Dicha búsqueda en un inicio arrojó 466 documentos, de los cuales 73 fueron eliminados por estar repetidos y 149 fueron desechados por no contener información apreciable para la investigación. Estos documentos fueron importados al Zotero para procesar los datos pertinentes y en conjunto con el Microsoft Excel mostrar los resultados necesarios para el estudio.

Además se tuvo en cuenta para la normalización la existencia de algunos campos de la Base de Datos que son la piedra angular del desarrollo de la investigación, y que permiten la confección de las redes de colaboración y temáticas existentes, tales como:

- Autor
- Título del trabajo
- Palabras clave
- Institución a la que pertenece
- País del que proviene
- Año de publicación.

Después de culminada esta tarea, se procedió a confeccionar los gráficos que muestran las particularidades de los documentos por año, así como los porcientos que verifican dichas resultados, utilizando para ello los enfoques seleccionados y sus respectivos indicadores.

2.3. Principales Indicadores utilizados

De los enfoques establecidos para el Análisis de Dominio fueron seleccionados el enfoque número cuatro, dedicado a los estudios empíricos de usuarios teniendo en cuenta que estos pueden organizar dominios según la preferencia o comportamiento o los modelos mentales de sus usuarios; y al enfoque número cinco dedicado a los estudios bibliométricos puesto que organizan patrones sociológicos de reconocimiento explícito entre documentos individuales.

2.3.1. Estudios empíricos de usuarios

Este enfoque es utilizado en la medida en que investiga el comportamiento de los usuarios, que en este caso es el grupo científico, del cual se estudia su actuación ante la búsqueda de información, para lo cual se utiliza el Modelo teórico integrador para el estudio de usuarios, por Mónica Izquierdo Alonso. (Izquierdo, 1999).

Este modelo se pone de manifiesto a través del análisis independiente de cada una de las variables del proceso informativo documental. Para su desarrollo e implementación se llevan a cabo una serie de pasos que permiten identificar las principales necesidades informativas de los usuarios, así como las líneas de investigación, las principales temáticas estudiadas, los autores más citados y las redes de colaboración y temáticas existentes entre ellos.

Los pasos necesarios para la realización del modelo son:

1. Estudio de los Autores
2. Estudio de los Documentos
3. Estudio de los Tipos de Usuarios

4. Establecimiento de relaciones entre el tipo de documento, tipo de autores, y tipo de usuarios.

La utilización del análisis documental como técnica de recopilación de datos permitió obtener la información necesaria para el desarrollo del modelo.

2.3.2. Estudio bibliométrico

En el presente estudio la bibliometría es utilizada como un método en el análisis de dominio, teniendo en cuenta que es un enfoque empírico y se basa en el análisis detallado de las conexiones entre documentos individuales. Por lo que en correspondencia al tipo de estudio y a los propósitos que se persiguen, este enfoque brindó los indicadores necesarios para fundamentar el estudio, por lo que se tomaron en cuenta tanto los de tipo Univariados como los Multivariados.

Organigrama de indicadores

En los de tipo Univariados según el tamaño de la población o muestra a medir, puede decirse que se trata de un análisis MESO, pues lo que se analiza es el consumo de información en el Grupo Científico de Criptografía. En los Multivariados se relacionan los indicadores a medir, con sus respectivas, clasificaciones y unidades de análisis:

Variables	Indicadores	Tipo de Indicador
Actividad Científica	Series temporales Distribución Geográfica Tipo de Institución	De Producción
Conexiones entre trabajos y autores científicos	Número y distribución de referencias y la vida media.(Ley de Price)	De Producción
Coautoría	Índice de firmas por trabajos.	De Colaboración

Tabla 1: Organigrama de Indicadores.

Estos indicadores permitieron obtener resultados que enriquecieron la investigación y la dotaron de credibilidad, teniendo en cuenta que:

- Los indicadores de actividad científica, los cuales están basados en el recuento de publicaciones científicas o patentes de la unidad objeto de estudio, permiten la realización de series temporales, distribuciones geográficas, por tipo de institución.
- Los indicadores de las conexiones entre trabajos y autores científicos, los cuales estudian las referencias que un trabajo hace a otros anteriores concernientes al tema investigado, permiten conocer el número y distribución de referencias y la vida media, (Ley de Price).
- Los indicadores basados en coautoría, los cuales facilitan conocer la colaboración existente entre los investigadores, así como el índice de firmas por trabajos.

Se muestran además las fuentes documentales de las referencias encontradas en los 244 documentos existentes en la base de datos, los cuales proyectaron 2533 referencias. De estas referencias, 963 son procedentes de revistas, para las cuales se realizó el análisis del Modelo de Bradford.

Capítulo 3

Capítulo 3 . Comportamiento de la Criptografía desde la perspectiva de Análisis de Dominio.

El capítulo describe el comportamiento de la Producción Científica de Criptografía desde la perspectiva de Análisis de Dominio, teniendo en cuenta los enfoques e indicadores bibliométricos seleccionados; con el fin de mostrar cuál ha sido el desarrollo de la Criptografía tomando como referencia el quinquenio comprendido entre los años 2008/2012.

3.1. Estudios Empíricos de Usuarios.

Los estudios de usuarios integran áreas multidisciplinares del conocimiento que, a través de métodos de investigación cuantitativos y cualitativos, intentan analizar los hábitos, comportamientos, motivaciones, actitudes, opiniones, expectativas, deseos, necesidades y demandas de las personas en relación con la información.

Es importante destacar que bajo este tipo de estudios es factible el análisis de los elementos que permiten cuantificar las necesidades de los usuarios, enfatizando en ¿qué necesitan, cuándo y cómo?, así como los propósitos que inducen la necesidad de información o el uso que se le espera dar a la misma.

En este caso se realiza un estudio de usuarios en el grupo científico de Criptografía de la Universidad Central "Marta Abreu" de Las Villas. El grupo esta integrado por 11 personas, divididas en 7 estudiantes y 4 profesores cuya principal línea de investigación va dirigida a los Algoritmos de Cifrado en flujo, enfatizando fundamentalmente en el Análisis y diseño de algoritmos de cifrado en flujo y el Criptoanálisis de los algoritmos de cifrado en flujo.

Teniendo en cuenta el grupo que se investiga y sus necesidades, se hace oportuno el uso del Modelo Teórico Integrador para el estudio de usuarios, por Mónica Izquierdo Alonso, en el que se proponen 4 pasos fundamentales

para la implementación del estudio. Estos pasos serán desarrollados a continuación.

3.1.1. Estudios de los autores

Para realizar un estudio de los autores es necesario aclarar que todas las personas pertenecientes al grupo, a pesar de su grado científico, dirigen sus investigaciones a la misma temática. Esto facilita la identificación de los autores más utilizados, y sus porcientos de colaboración (Anexo 1). Estos son:

- Julio López
- Yevgeniy Dodis
- Bruce Schneier
- Manuel José Lucena López
- José Ramió Aguirre
- Rudolf Lidl
- Harald Niederreiter
- Claude Shannon
- Martín Abadi
- José Ángel de Bustos
- Amparo Fúster
- Fausto Montoya
- María Catalá Carbonero
- Joaquim Borges
- Edilson Fernández Da Cruz
- Jeffrey Ullman
- Victor Shoup
- Wilson Vicente Ruggiero
- Marcello Barra

El siguiente gráfico muestra lo antes expuesto:

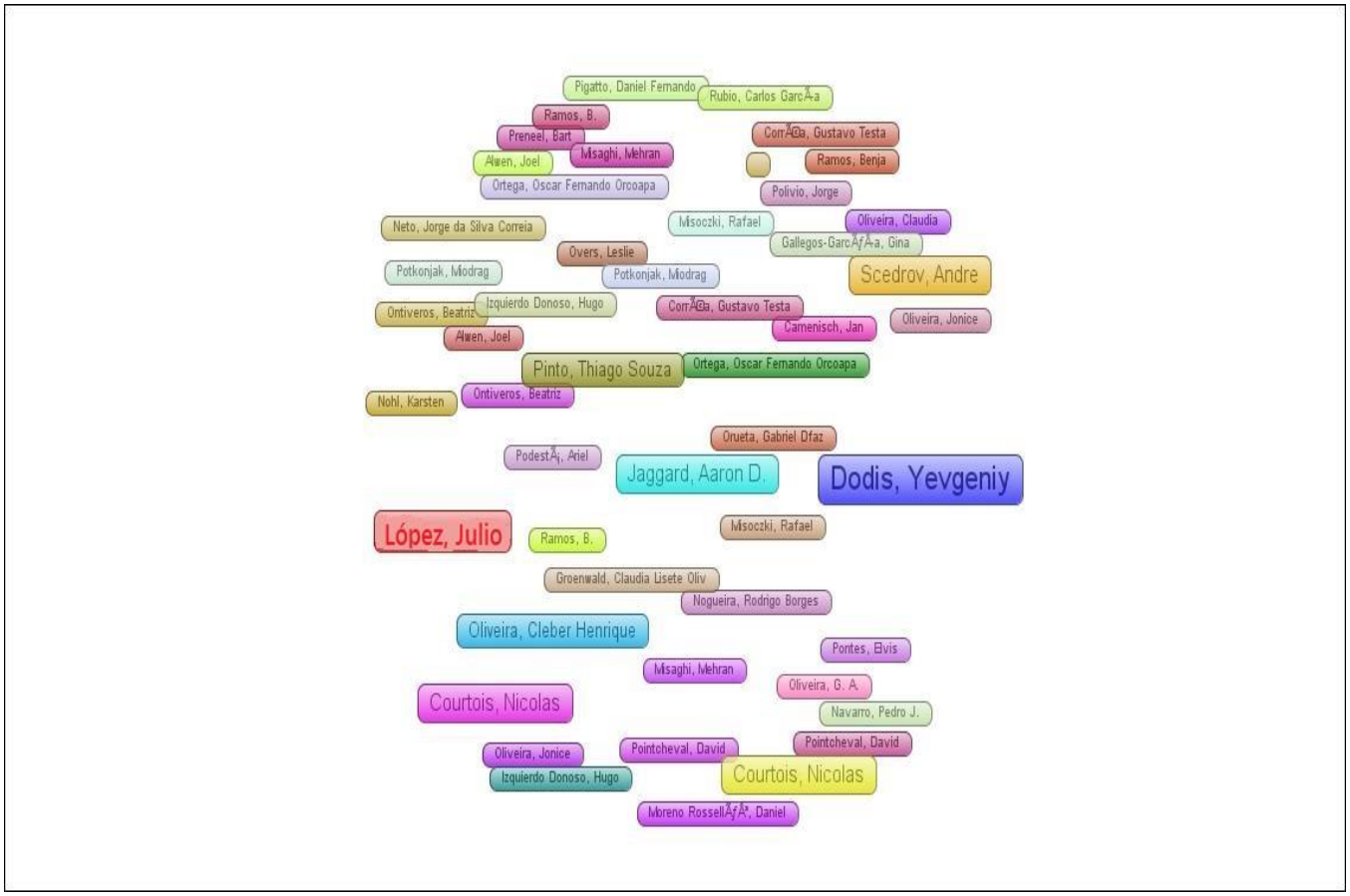

Gráfico 2: Autores más citados.

Dicho análisis facilita conocer las principales **redes de colaboración** existentes entre los autores más utilizados por el grupo científico escogido, teniendo en cuenta el análisis de los documentos y artículos existentes dentro del grupo, así como sus publicaciones en otros países. El siguiente gráfico representa lo antes expuesto:

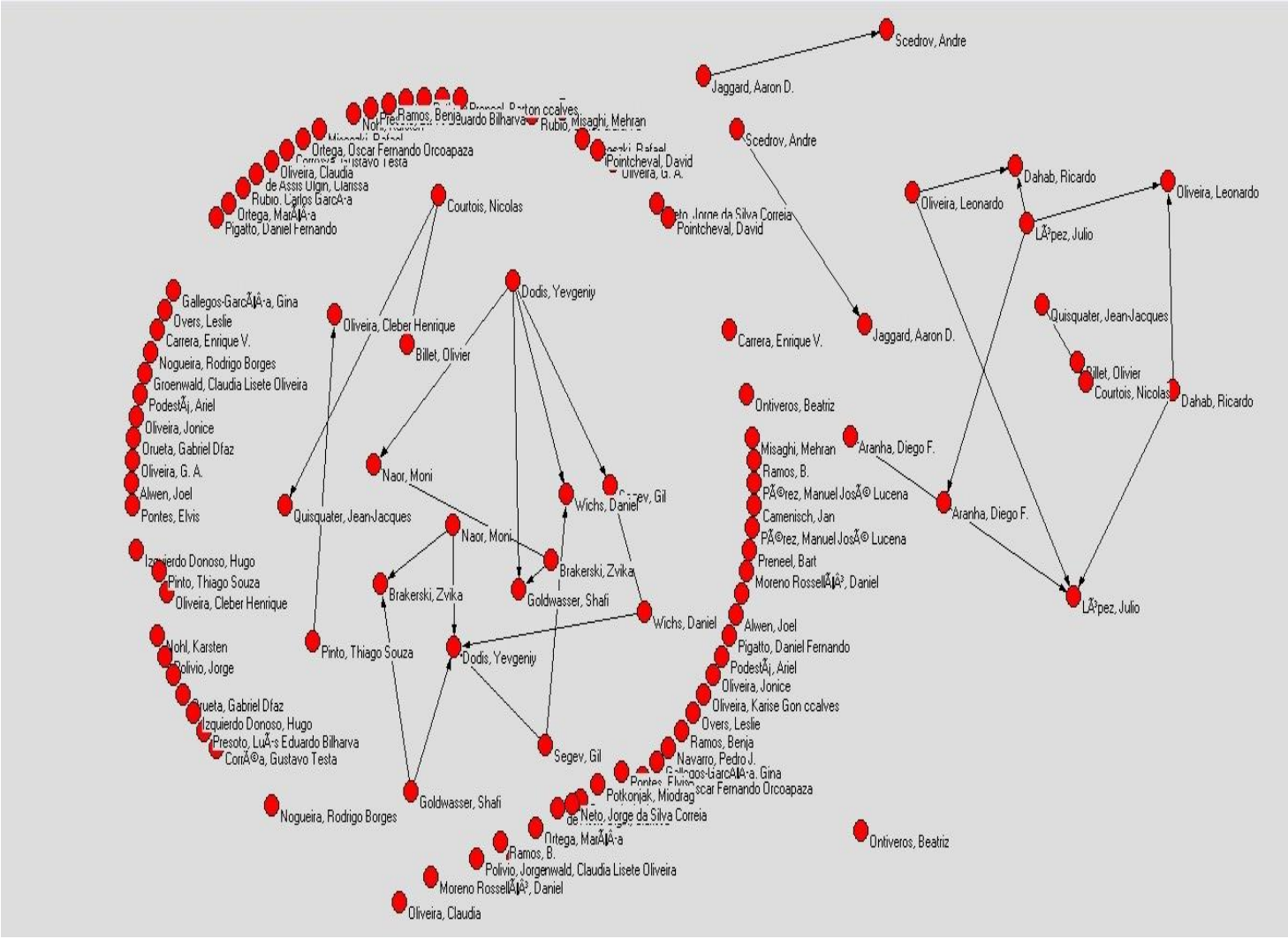

Gráfico 3: Redes de colaboración.

Estos autores son utilizados en la medida en que sus publicaciones permitan al grupo obtener los siguientes resultados:

- Dominio de los algoritmos de cifrado en flujo conocidos.
- Dominio de los fundamentos matemáticos de estos algoritmos. .
- Dominio de las implementaciones de los algoritmos conocidos.
- Diseño de nuevos algoritmos o proponer modificaciones a los ya existentes.

- Análisis y aplicación de las técnicas de criptoanálisis a los algoritmos diseñados.
- Elaboración de una monografía sobre los Cifradores de Flujo.
- Conformación de artículos para publicar y participación en eventos.

3.1.2. Estudio de los Documentos

Para el análisis de los documentos que son utilizados, se hace conveniente conocer que el grupo tiene como propósito lograr que la Criptografía se convierta en objeto de investigación en las universidades y esto puede lograrse mediante el desarrollo de proyectos de investigación que posibiliten evaluar los Criptosistemas que se aplican en el mundo globalizado actual y desarrollar las herramientas tecnológicas necesarias para diseñar nuevos algoritmos.

Para lograr su objetivo el grupo cuenta con una serie de planificaciones que les facilitan la capacitación de estudiantes de las carreras de Licenciatura en Matemática y Licenciatura en Ciencias de la Computación, así como la tutoría de los cadetes insertados, enfatizando fundamentalmente en:

- Profundizar en el estudio de los temas de las Estructuras Algebraicas, los Campos Finitos, las Funciones Booleanas.
- Estudiar los algoritmos de cifrado en flujo conocidos y que se aplican en la actualidad.
- Obtener los conocimientos teóricos que permitan la demostración de las propiedades matemáticas de estos algoritmos criptográficos conocidos y de los que se diseñen.
- Demostrar que son resistentes a los métodos criptoanalíticos conocidos, fáciles de implementar en cualquier plataforma y que corran a velocidades adecuadas a los sistemas criptográficos a diseñarse en el país.
- Someter los algoritmos criptográficos diseñados al trabajo criptoanalítico.

Este análisis permitió identificar los principales documentos existentes en el grupo, los cuales fomentan el cumplimiento del objetivo trazado. Estos son:

- Seminarios de investigación
- Dictamen de aprobación de proyectos
- Diseño curricular
- Diseño de programas de maestría y diplomados
- Evaluación de estudiantes
- Estrategia educativa
- Actas de notas
- Asignación de estudiantes a proyectos
- Asignación de tiempo de maquina
- Listado de estudiantes por año y carrera
- Plan de trabajo científico metodológico del grupo
- Base de Datos con las principales publicaciones realizadas
- Base de datos con las publicaciones de otros países referentes al desarrollo de la temática.

3.1.3. Estudio del Tipo de Usuarios

El grupo esta vinculado con una de las asociaciones profesionales más importantes del país y esta es la Dirección Nacional de Criptografía del Ministerio de Educación Superior (MES) quien además constituye su entidad ejecutora.

Los usuarios del grupo son los estudiantes de las carreras de Licenciatura en Matemática y Cibernética principalmente aunque también lo visitan algunos estudiantes de Licenciatura en Física e Ingeniería Informática, así como algunos investigadores interesados, y esto se debe principalmente a que lo profesores que integran el grupo imparten clases en estas carreras.

El grupo cuenta con 11 personas, de ellas 7 estudiantes y 4 profesores que a pesar de ser los lideres del grupo, imparten clases en las Carreras antes mencionadas.

En el caso de los profesores su ocupación dentro del grupo esta sujeta a una jerarquización en la que pude encontrase:

1. Jefe de Grupo
2. Segundo jefe de grupo
3. Secretaria de actas
4. Jefe de seguridad

En el caso de los estudiantes 5 de ellos pertenecen a la carrera de Licenciatura en Matemática y 2 a Licenciatura en Ciencias de Computación su rol dentro del grupo depende de la línea en que se encuentre investigando, siempre centrada en Algoritmos de Cifrado en flujo.

Entre las principales temáticas investigadas pueden destacarse:

- Profundización en el estudio de los temas de las Estructuras Algebraicas, los Campos Finitos, las Funciones Booleanas.
- Estudio de los algoritmos de cifrado en flujo conocidos y que se aplican en la actualidad.
- Demostración de las propiedades matemáticas de algoritmos criptográficos conocidos y de los que se diseñen.
- Demostración de la resistencia a los métodos criptoanalíticos conocidos, que son fáciles de implementar en cualquier plataforma y que corran a velocidades adecuadas a los sistemas criptográficos a diseñarse en el país.
- Someter los algoritmos criptográficos diseñados al trabajo criptoanalítico.

Este estudio facilita la confección de una red temática que muestra con claridad, las principales líneas de investigación, resaltando las que cumplen con el objetivo del grupo investigado, teniendo en cuenta que su objetivo

principal son las investigaciones referentes a los Algoritmos Criptográficos de cifrado en flujo, y a todas las temáticas mencionadas anteriormente.

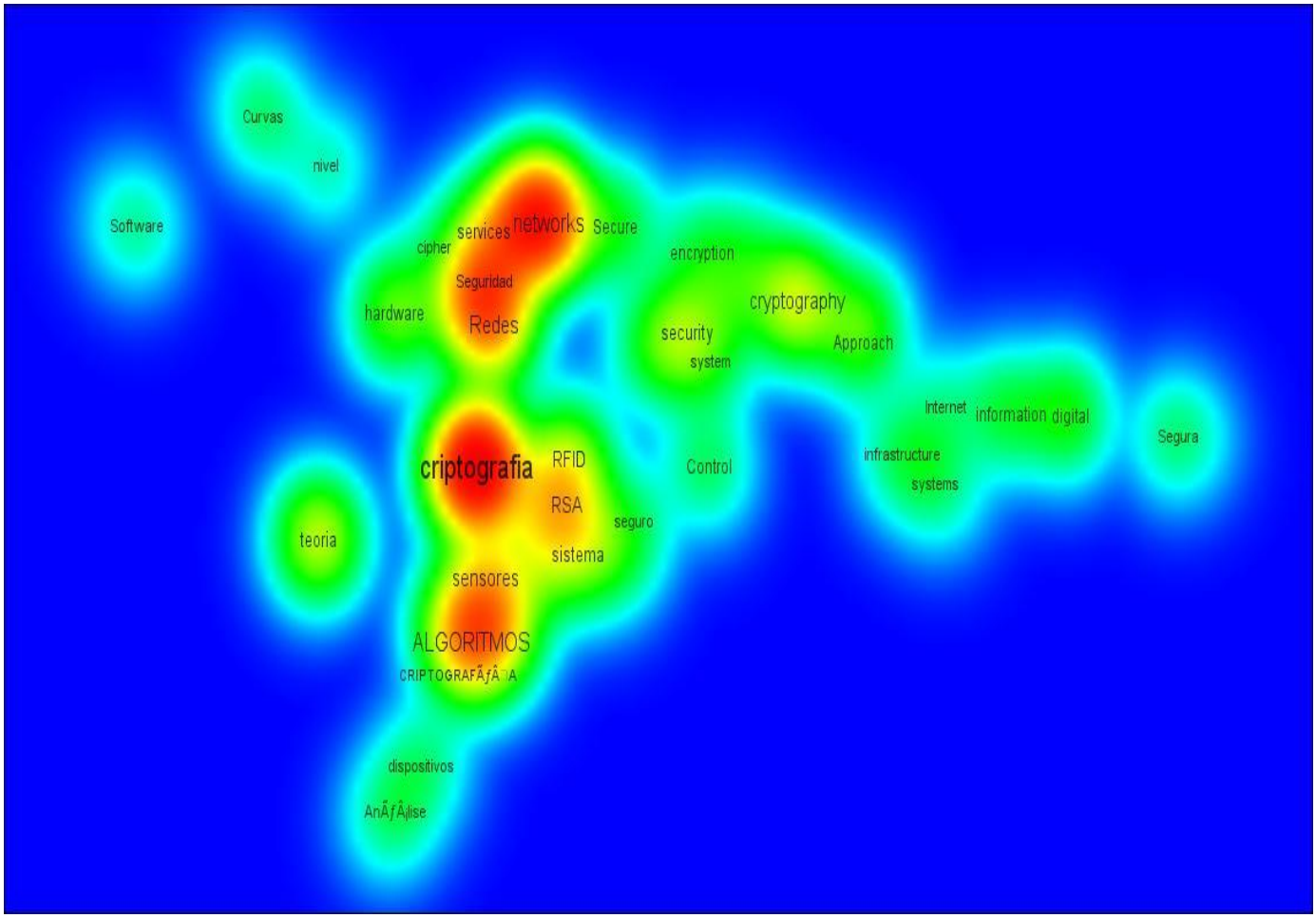

Gráfico 4: Redes temáticas.

3.1.4. Establecimiento de relaciones entre el tipo de documentos, tipo de autores y tipo de usuarios.

Teniendo en cuenta las personas que integran el grupo y sus características, puede decirse que existe una interesante relación entre sus investigaciones, los documentos generados y los autores consultados. Esto puede afirmarse teniendo en cuenta los estudios que hasta el momento convierten al grupo

en un punto clave para el diseño e implementación de algoritmos criptográficos de cifrado en flujo, que permiten crear las bases para ir dotando al país de algoritmos y herramientas propias para la protección de la información, y de esta forma potenciar el estudio de esta ciencia en el centro de país.

Estas investigaciones se encuentran en total correspondencia con el objetivo de creación del grupo y les facilita la participación en eventos que en gran escala son la piedra angular del desarrollo de la ciencia.

3.2. Estudios Bibliométricos

La bibliometría es un fuerte enfoque para el análisis de dominio por ser empírico y basarse en el análisis detallado de las conexiones entre documentos individuales. Por lo cual se necesita considerar diferentes sesgos en forma muy cuidadosa, teniendo en cuenta que este enfoque muestra muchas conexiones reales y detalladas entre documentos individuales y estos vínculos representan el reconocimiento explicito de los autores de la dependencia entre trabajos, investigadores, campos, enfoques y regiones geográficas respectivamente.

3.2.1. Análisis de los indicadores bibliométricos medidos.

Para obtener los documentos con los que fue confeccionada la Base de Datos se utilizó el Google Scholar, puesto que los documentos encontrados en la Base de Datos SCOPUS a pesar de estar en correspondencia con las palabras claves seleccionadas, carecían de relevancia con respecto a las líneas de investigación del grupo científico, dirigida fundamentalmente a los Algoritmos Criptográficos de Cifrado en Flujo, lo que imposibilito encontrar una cantidad notable de documentos que contribuyeran al desarrollo de la investigación.

Se seleccionaron los documentos pertenecientes a los años 2008, 2009, 2010, 2011 y 2012 respectivamente, con los cuales se realizó dicha Base de Datos y se normalizó, utilizando para ello el Zotero como procesador de

datos. Se obtuvieron un total de 466 documentos, de los cuales 73 estaban repetidos y después de ser eliminados, resultaron 393. Este último dato fue analizado para corroborar que todos los artículos mostraban contenidos significativos, siendo descartados 149, por lo que solo se seleccionaron 244 documentos, divididos en artículos de revista, tesis, sitios web, conferencias y monografías o libros fundamentalmente.

Después del análisis realizado con la confección de la Base de datos puede decirse que en las 244 publicaciones seleccionadas hay un total de 2533 referencias entre todos los años mencionados anteriormente. En ellas fueron identificados 636 autores referenciados. Por otra parte de estas 2533 referencias 963 son publicaciones periódicas representando un 38,0%; 676 monografías o libros para un 26,6%; 484 memorias de congresos para un 19,1%, 298 tesis representando un 11,7% del total y 115 páginas Web, siendo un 4,5% del total. La siguiente figura muestra la representación de estos datos.

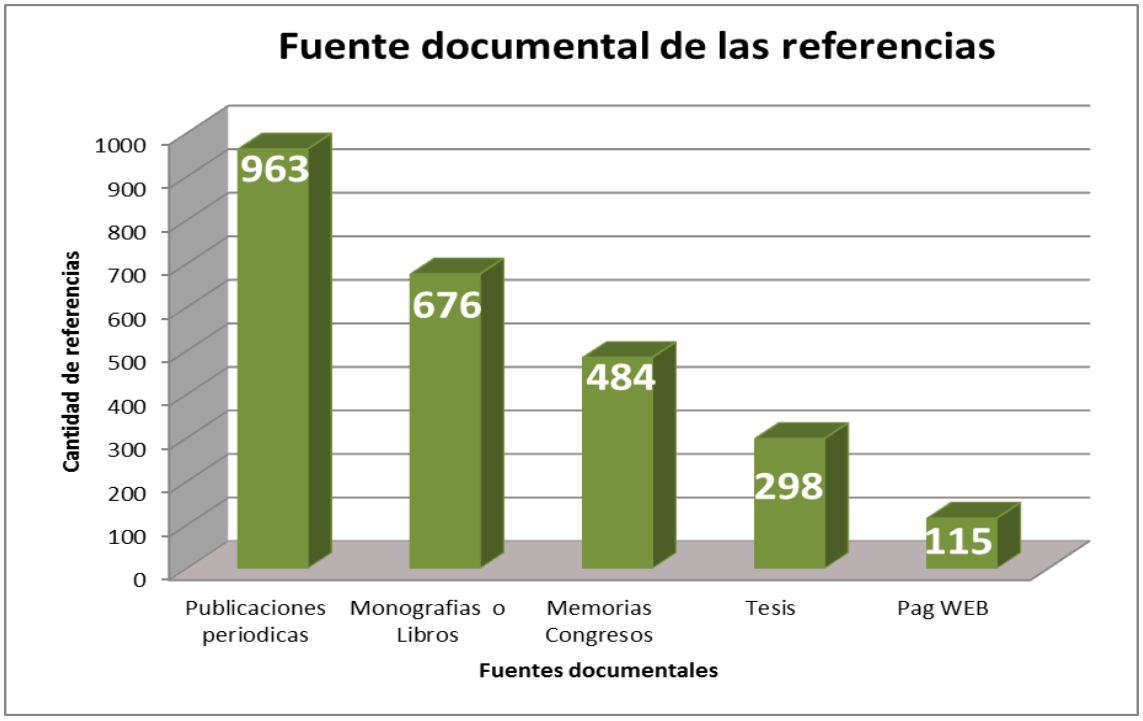

Gráfico 5: Fuente documental de las referencias.

Es importante señalar que las publicaciones periódicas constituyen una de las fuentes más utilizadas y que permitirán representar claramente las Áreas de Bradford, en las cuales se agruparon las 963 referencias en 28 revistas.

Zonas	Cantidad de Referencias	Total de Referencias
Núcleo	1	298
Zona 1	2	377
Zona 2	23	288

Tabla 2: Áreas de Bradford

La revista núcleo, que en este caso es la más utilizada o en las que mayor número de publicaciones se encontró:

- Journal of Cryptology

Se encuentran además algunas revistas menos utilizadas, pero que son referenciadas en una porción considerable de las publicaciones y que por ende formarían la Zona 1 de las Áreas de Bradford, estas son:

- Bulletin of Security and Cryptography
- Journal of Discrete Mathematical Sciences & Cryptography

Por último se encuentran las revistas que se utilizan pero no en gran escala, sino que en algunas ocasiones constituyen fuentes de consulta, las cuales formarían la Zona 2 de las Áreas de Bradford, estas son:

- Advances in Applied Mathematics
- Elsevier
- IEEE Transaction on Software Engineering
- IEEE Transactions on Pattern Analysis and Machine Intelligence
- IEEE Transactions on Information Theory
- Security Protocols
- Journal of the Association for Computing Machinery
- International Journal of Information Security
- International Journal of Computer Science and Engineering
- Mathematics of Computation
- Computer Comunications
- Journal of Future Generation Communication and Networking
- Journal of InformationSystems and Technology
- Journal of the R amanujan Mathematical Society
- Commentarii Mathematici Universitatis Sancti Pauli
- Acta Morphologica Neerlando-scandivanica
- Journal of the Optical Society of America
- Digital system Research Center

- Machine Vision and Applications
- Pattern Recognition

A continuación se muestra todo el estudio mencionado anteriormente sobre la división de las publicaciones periódicas en las **Áreas de Bradford.**

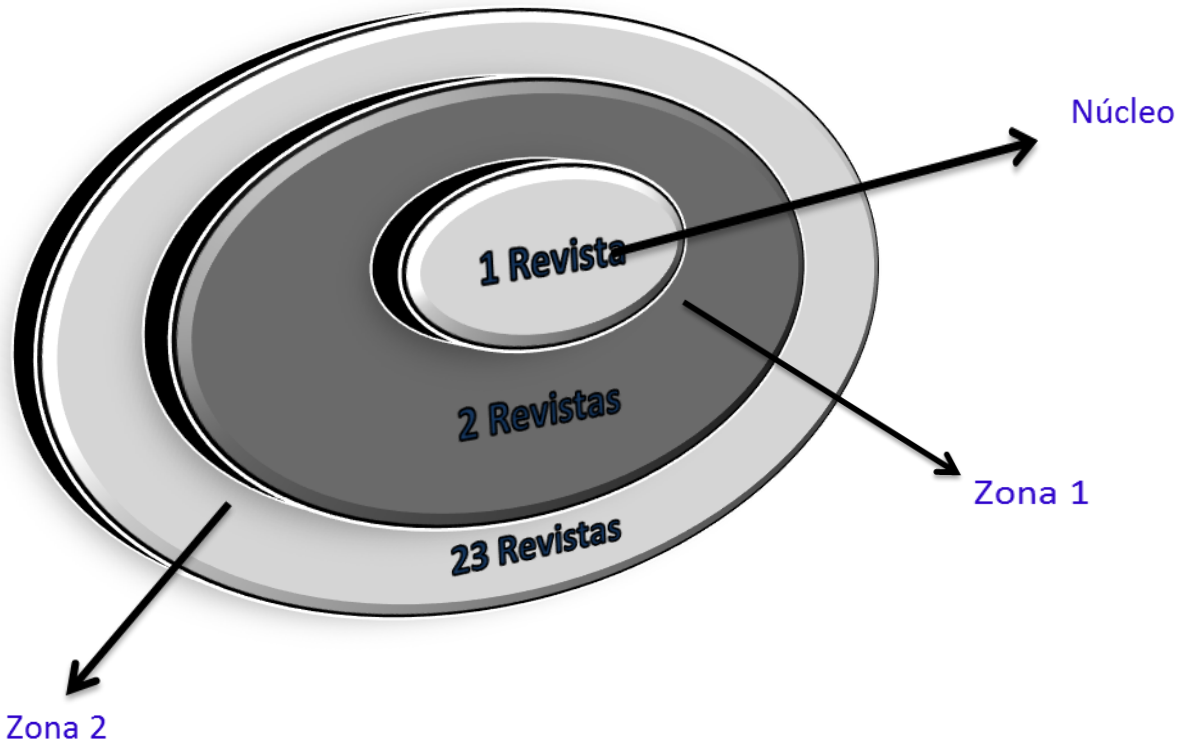

Gráfico 6: Publicaciones Periódicas: Áreas de Bradford.

3.2.2. Indicadores de actividad científica

Distribución temporal

De un total de 466 documentos recuperados solo se procesaron 244, puesto que se creyó conveniente analizar los documentos más relacionados con el tema, que en este caso esta en correspondencia con las líneas de investigación del grupo científico de Criptografía y de esta forma identificar los principales avances en la temática, por lo que se determinó que el estudio comprendiera solo las publicaciones referentes a los años 2008, 2009, 2010, 2011y 2012.

En cuanto a los indicadores de actividad científica, después del análisis realizado han podido determinarse las Series temporales, en las cuales se analizan las investigaciones referentes a Criptografía en los años 2008, 2009, 2010, 2011 y 2012. De un total de 244 publicaciones, 29 pertenecen al año 2008 representando un 11,8% del total; 36 al año 2009 para un 14,7%; 50 al 2010 representando el 20,4%; 58 al 2011 siendo un 23,7% y 71 al 2012 para un 29,0% del total de documentos existentes en la Base de datos, representando el año en que mayor cantidad de documentos se encontraron. Estos datos demuestran la medida en la que es tratada esta ciencia y el nivel de censura existente, teniendo en cuenta que a pesar de haber pasado a dominio publico, aun existen restricciones en cuando al uso del termino, lo que causa gran influencia en el conocimiento de la temática y de importantes investigaciones llevadas a cabo. En la siguiente gráfica se puede observar claramente que existe un crecimiento exponencial de esta ciencia en los años seleccionados y esto se debe a la importancia que han cobrado las investigaciones que demuestran que las única forma de obtener buenos Algoritmos Criptográficos es sometiéndolos al escrutinio de la comunidad científica.

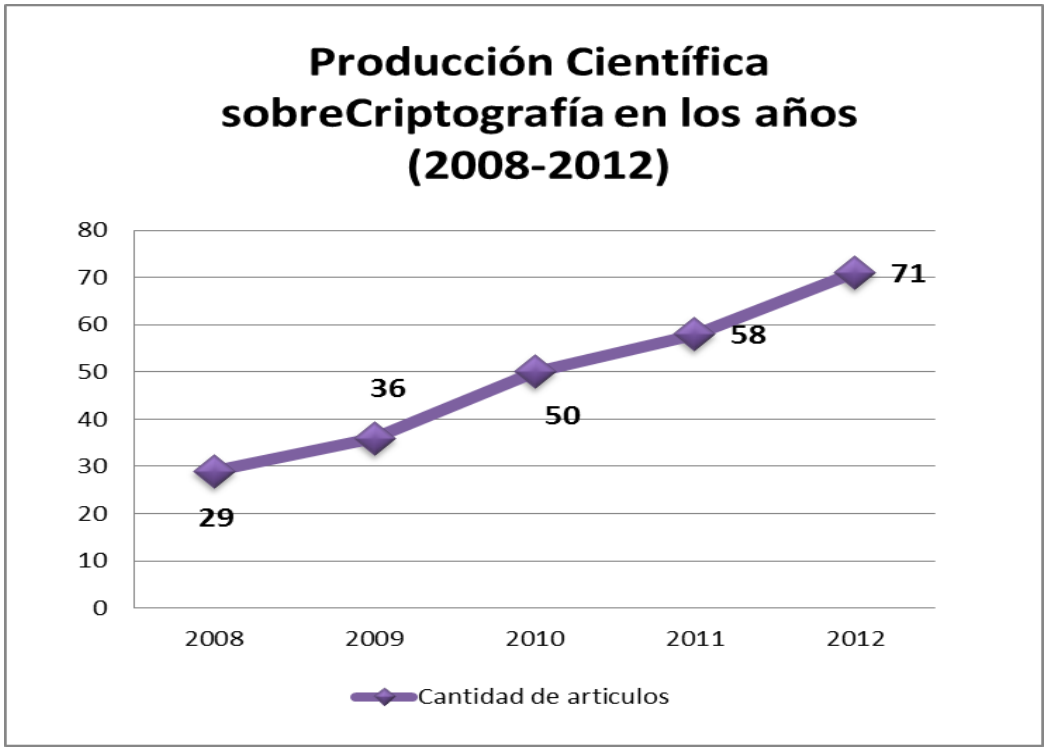

Gráfico 7: Presencia de la Criptografía en investigaciones referentes a los años (2008-2012).

Distribución geográfica

El análisis para determinar uno de los indicadores definidos, referido al índice de firmas por trabajo en cuanto a la temática abordada, dio a conocer la existencia de trabajos con 1, 2, 3 y hasta siete firmas , proporcionando a su vez, una distribución que se ha dividido en nacional e internacional.

En el caso de las ***investigaciones nacionales***, fueron identificadas 91 publicaciones provenientes principalmente de centros de educación superior, entre ellos universidades como la Universidad central Marta Abreu de la Villas (UCLV) con 22 publicaciones, representando un 24,1%. Por otra parte la Universidad de la Habana (UH) con 34 publicaciones para un 37,3%, representando el mayor exponente. La Universidad de Ciencias

Informáticas (UCI) arrojando 10 publicaciones siendo un 10,9%; Además el Instituto de Cibernética, Matemática y Física (ICIMAF) con 10 publicaciones para un 10,9%: y el Instituto Politécnico Superior José Antonio Echeverría (IPSJAE) en el que fueron identificadas 15 publicaciones, representando el 16,4% del total. Estos resultados muestran la medida en la que esta siendo desarrollada en el país, lo que no significa que estas sean las únicas instituciones que se dedican a estudiar esta ciencia, sino que hasta el momento son las investigaciones que pueden ser accedidas.

Por tanto puede decirse que de 5 instituciones que publican sobre el tema, 3 son centros de educación superior, representando un 60%; y 2 institutos que representan un 40% del total. Para lo cual se presenta el siguiente gráfico:

Gráfico 8: Productividad de la Instituciones Nacionales sobre Criptografía.

En el caso de las ***investigaciones internacionales*** las instituciones que se dedican a investigar sobre esta ciencia son principalmente Universidades, Centros de Investigación y Organismos Oficiales. Estas instituciones están asociadas a una Red Temática de Criptografía y Seguridad de la Información, en la que colaboran principalmente países como Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Republica Dominicana, Ecuador, El Salvador, España, México, Nicaragua, Panamá, Perú, Portugal, Uruguay, Venezuela, Australia, Canadá, Francia, Suecia.

Entre las instituciones pertenecientes a esta red se puede destacar:

- Laboratorio de Investigación y desarrollo en nuevas tecnologías (Argentina)
- Universidad de Buenos Aires (Argentina)
- Universidad Tecnológica Nacional (Argentina)
- Escuela Militar de Ingeniería (Bolivia)
- Universidad Estatal Paulista (Brasil)
- Instituto Nacional de Tecnología da Informaçao (Brasil)
- Universidad de Concepción (Chile)
- Universidad de los Llanos (Colombia)
- Escuela militar de aviación Marco Fidel Suárez (Colombia)
- Centro de investigación FUNDACRID (Costa Rica)
- Pontificia Universidad Católica Madre y Maestra (Republica Dominicana)
- Corporación Ecuatoriana de Comercio Electrónico (Ecuador)
- Escuela superior politécnica de Chimborazo (Ecuador)
- Universidad Don Bosco (El Salvador)
- Consejo superior de investigaciones científicos (España)
- Universidad autónoma de Barcelona (España)
- Universidad Carlos III de Madrid (España)
- Universidad Politécnica de Cataluña (España)

- Centro de investigación y Estudios Avanzados (México)
- Instituto tecnológico de ciudad Guzmán (México)
- Universidad Autónoma de Nicaragua (Nicaragua)
- Universidad Interamericana de Panamá (Panamá)
- Universidad nacional de Ingeniería (Perú)
- Universidad de Ciencias Aplicadas (Perú)
- Instituto superior de Matemática e Gestao (Portugal)
- Universidad de la República (Uruguay)
- Colegio universitario Francisco de Miranda (Venezuela)
- Universidad de Simón Bolívar (Venezuela)
- Queennsland University of Technology (Australia)
- Carleton University (Canadá)
- École Polytechnique (Francia)
- Université de Technologie de Troyers (Francia)
- CHalmers University of Technology (Suecia)

Además de estos países pertenecientes a la Red Temática existen otros en los que se investiga esta ciencia, y que no se encuentran asociados a la Red por la poca disponibilidad pública de los estudios que se realizan, lo cual no infiere que no existan publicaciones, y esto puede afirmarse teniendo en cuenta que en la Base de Datos realizada el mayor porciento de los documentos son provenientes de Estados Unidos, Rusia, La India, Alemania. Estos países a pesar de no pertenecer a la Red se presentan como el mayor exponente en cuanto a investigaciones se refiere.

La gráfica siguiente demuestra dichos argumentos:

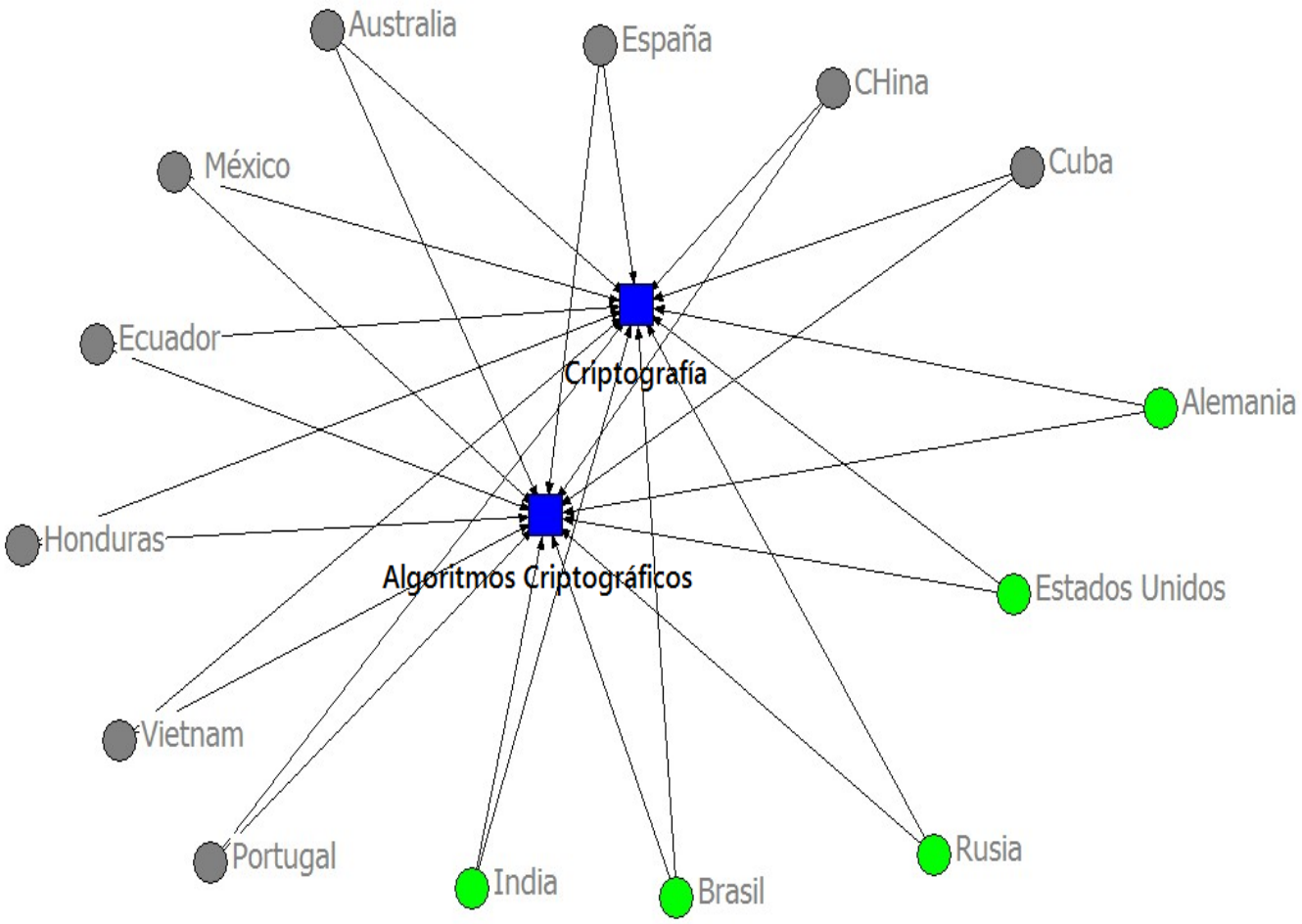

Gráfico 9: Países más Productivos

3.2.3.Indicadores de las conexiones entre trabajos y autores científicos

Este tipo de indicador, no es más que un estudio de las referencias que un trabajo hace a otros anteriores referentes al tema investigado, por lo cual se creyó conveniente calcular el número y distribución de referencias, teniendo en cuenta para ello la cantidad absoluta y media de las referencias por año.

En este estudio se normalizaron un total de 244 publicaciones de las cuales se analizó la cantidad de referencias con que contaba cada una. Esto permitió calcular la frecuencia absoluta, que no es más que la suma de la cantidad de referencias de los documentos por año y la media que se obtiene de la división de la cantidad de referencias por año entre la cantidad total de estas.

En el año 2008 con solo 29 artículos se obtuvo una frecuencia absoluta de 377, sin embargo en el año 2009 se encontraron un total de 36 publicaciones, para una frecuencia absoluta de 412. Ya en el año 2010 con solo 50 publicaciones, la frecuencia es de 575. Por su parte el 2011 arrojó un total de 58 documentos para una frecuencia de 743. Por último en el año 2012 en el cual se encontró la mayor cantidad de publicaciones con un total de 71, se tiene una frecuencia absoluta de 426. Este análisis permitió conocer que entre los cinco años mencionados la frecuencia absoluta suma un total de 2533 que sería el total de referencias encontradas en las 244 publicaciones que arrojó la confección de la Base de Datos.

Año	Frecuencia absoluta	Cantidad de artículos
2008	377	29
2009	412	36
2010	575	50
2011	743	58
2012	426	71

Tabla 3: Cantidad Absoluta de las referencias por año

Esta tabla facilitó la confección de la gráfica que se expone a continuación en la cual se representa claramente el aumento y descenso de la frecuencia absoluta que proyectó el análisis de las referencias encontradas por año y el total de estas, siendo de 2533.

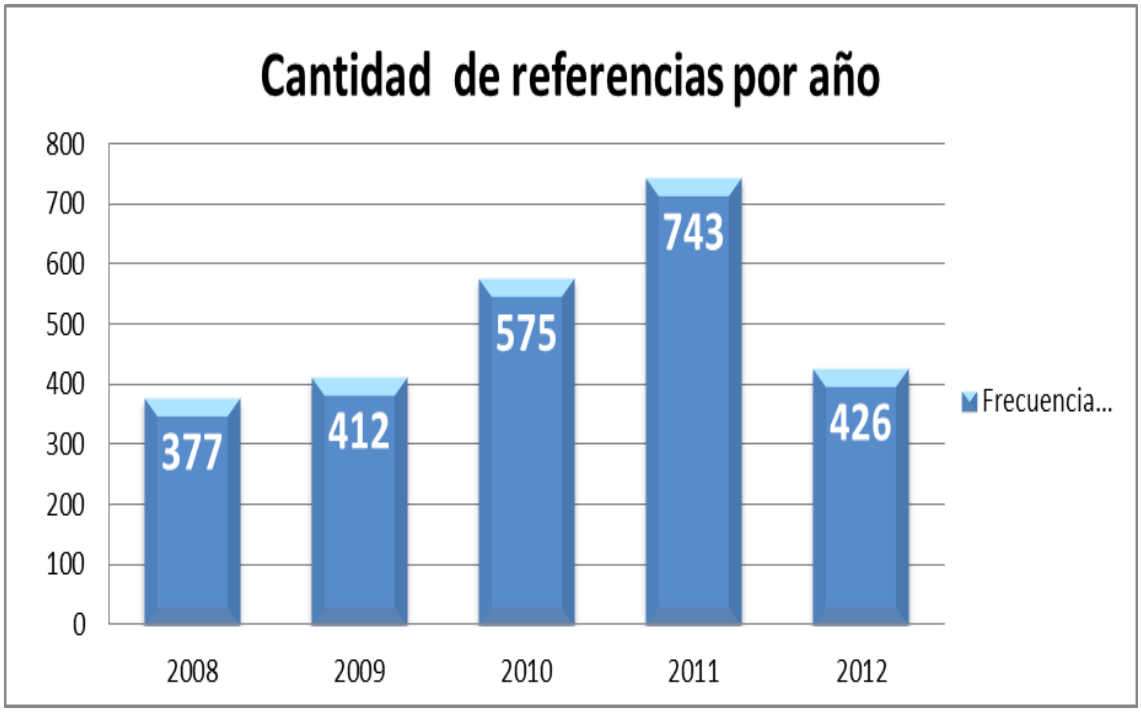

Gráfico 10: Cantidad de referencias por año.

Se calcularon además las frecuencias de las referencias por décadas, según el año de publicación, analizando fundamentalmente de las 2533 referencias, las que no presentaban fecha, sumando un total de 42, así como las referencias de menos de 5 años, para un total de 307, lo que demuestra que el 87,9% de las publicaciones presentan años, y solamente en el 12,1% no aparecen, lo que da a las publicaciones más fiabilidad y facilita la búsqueda a las personas que deseen o necesiten consultarlas.

Para la aplicación de este tipo de indicador además del número y distribución de referencias, se hace necesario analizar la Vida Media (Ley de Price). Este dato se obtiene a partir del cálculo de la durabilidad de las publicaciones, o sea, el tiempo que son consultadas o referenciadas hasta que pasan a ser obsoletas. Dicho cálculo no es más que la división de la cantidad de referencias por año entre la cantidad de referencias menores de cinco años.

La siguiente fórmula permite realizar dicho cálculo:

$$IO = \frac{\text{Documentos - 5 años}}{\text{Total}} \times 100\%$$

Al indagar las referencias menores de 5 años localizadas en el quinquenio establecido se obtuvo un total de 307. Las cuales fueron analizadas y divididas según el año al que corresponden.

Año	Documentos menores de 5 años	Cantidad de artículos
2008	99	29
2009	66	36
2010	54	50
2011	71	58
2012	17	71

Tabla 4: Documentos menores de 5 años

La tabla permitió calcular la vida media de los documentos por año.

En el año 2008 se encontraron 99 menores de 5 años, lo que ofrece una vida media de 26%; en el caso del 2009 se obtuvieron 66 referencias menores de 5 años, lo que refleja un 16% de vida media. En el caso de 2010 con un total de 54 referencias menores de 5 años, para una vida media de 9%, mientras que el año 2011 posee 71 referencias menores de 5 años, para una vida media de 9%. Por último en el año 2012 el cual arrojó 17 referencias menores de 5 años, se presenta un 4% de vida media.

Año	Cantidad de artículos	Cantidad de autores	# de documentos 1 autor	# de documentos 2 autores	# de documentos 3 autores	# de documentos 5 autores	# de documentos 6 autores	# de documentos 7 autores	IC
2008	29	85	10	4	6	7	0	2	2,93
2009	36	81	7	19	8	0	2	0	2,25
2010	50	120	9	21	17	0	3	0	2,4
2011	58	155	4	11	43	0	0	0	2,67
2012	71	195	12	19	33	0	3	4	2,74

Tabla 5: Cantidad de firmas por artículos.

3.2.4. Indicadores basados en coautoría

Para medir este tipo de indicadores se tuvo en cuenta el Índice de firmas por trabajos, lo que permite conocer la colaboración existente entre los autores de cada publicación, revelando sus intereses por una temática determinada.

La tabla 3 facilitó conocer la cantidad de firmas por artículos, teniendo en cuenta la cantidad de artículos publicados en cada año.

En los años seleccionados pueden encontrarse con un autor, un total de 42 publicaciones; con 2 autores 74 publicaciones; con 3 autores 107 publicaciones, respresentando la mayor cantidad de publicaciones

encontradas. Con 4 autores no se encontro ningún documento en la base de datos, motivo por el cual no aparece representada esta cantidad; en el caso de 5 autores se analizaron 7 publicaciones; con 6 autores se visualizaron 8 publicaciones; y con 7 autores se encontraron 6 publicaciones. Por tanto se hace conveniente presentar el siguiente gráfico que muestra el porciento de coautoria existente en cada caso.

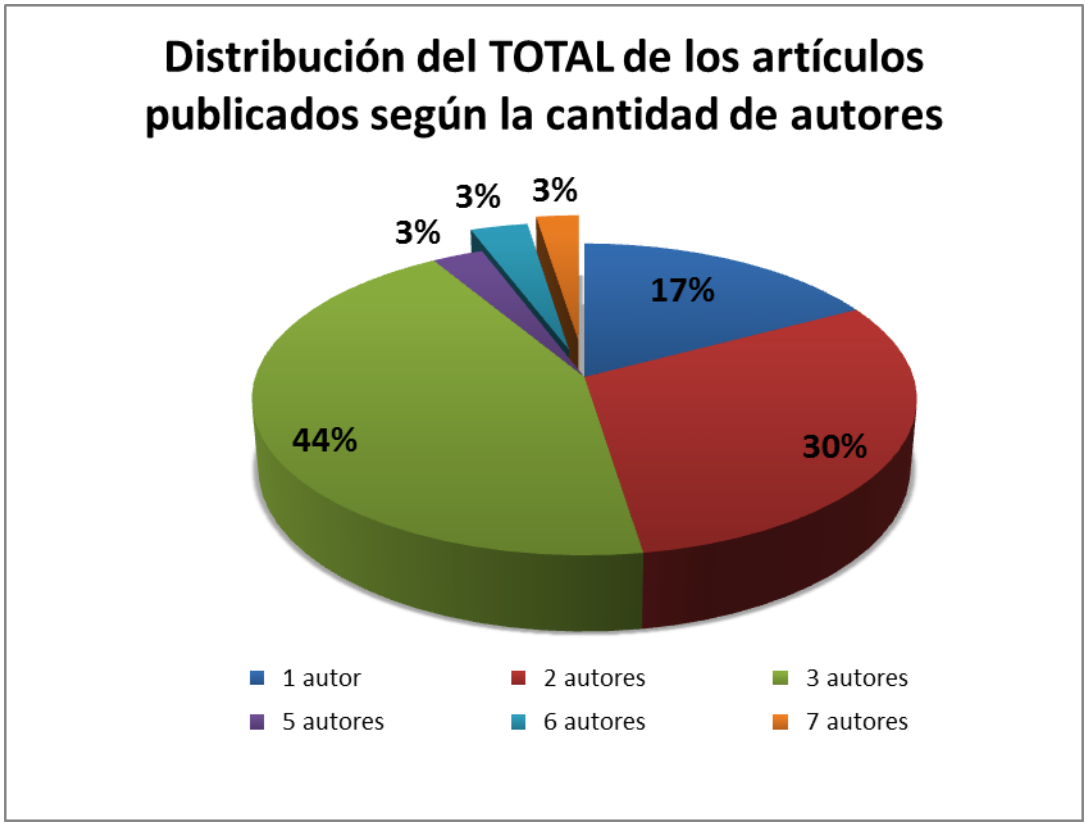

Gráfico 12: Distribución del total de los artículos publicados según el número de autores.

El análisis anterior hace posible la representación de la distribución de los artículos según la cantidad de firmas encontradas en cada unos de ellos, teniendo en cuenta el año al que pertenecen, lo cual se muestra que de los 244 documentos existentes en la base de datos, el 44% cuenta con 3 firmas siendo este un aparte considerable del total, partiendo de que identifica el nivel de colaboración existente. Por otra parte con un 1 autor se encontró el 17% del total, con 2 autores el 30%. En el caso de cuatro autores no aparece ninguna representación, por lo cual no forma parte del porciento identificado. Con 5 autores se registró el 3%; y en el caso de 6 autores se presenta un 3% al igual que los documentos con 7 firmas.

Estos datos y la representación de ellos facilitaron obtener el índice total de la coautoría existente en los documentos seleccionados en los años anteriormente mencionados. Dicho índice se representa en la próxima tabla.

Total de autores	Total de artículos	Índice Total de Coautoría
636	244	2,6

Tabla 6: Índice total de coautoría en los años seleccionados.

La tabla muestra el índice total coautoría existente en las 244 publicaciones seleccionadas, siendo este la división de la cantidad de autores entre el total de artículos, lo que en este caso posibilita conocer que el índice de coautoría es de un 2,2. Este resultado hace necesaria la confección del siguiente gráfico, en el que se muestra el índice de coautoría por años.

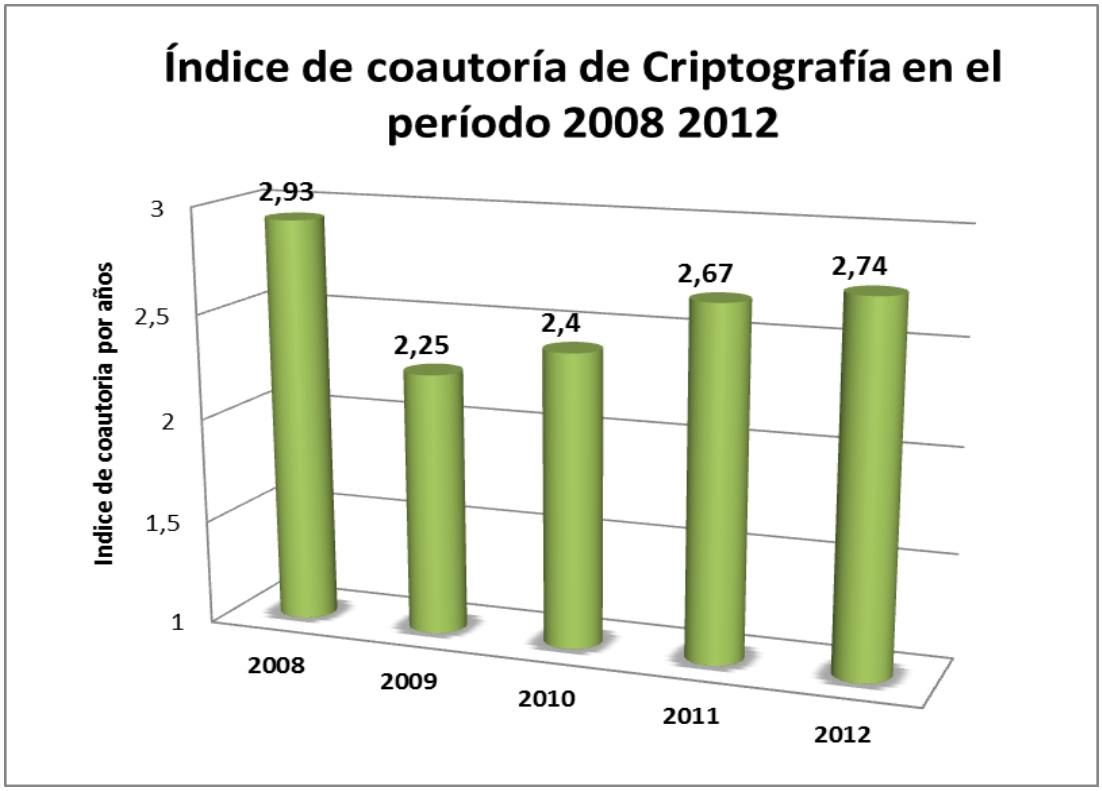

Gráfico 13: Índice de coautoría de Criptografía en los años seleccionados.

Como puede observarse en el año 2008 el índice es de un 2,93, mientras que en el 2009 se obtuvo un índice de 2,25. En el año 2010 se muestra un índice 2,4. Estos resultados no son muy distantes en los restantes años, teniendo en cuenta que se mantiene bastante estable, pues como lo indica el gráfico en el 2011 se tiene un índice de 2,67 y en el 2012 de un 2,74 respectivamente. Estos índices permiten afirmar que esta temática es generalmente estudiada en colectivo.

Conclusiones

Conclusiones

1. La investigación posibilitó un acercamiento a los referentes teórico-conceptuales relativos a la Producción Científica sobre Criptografía y su estudio desde la perspectiva de Análisis de Dominio. Los tópicos fundamentales fueron abordados consecuentemente para sustentar la pesquisa que se presenta.
2. Los enfoques de análisis de dominio utilizados, permitieron realizar un estudio empírico de usuarios en el grupo científico de criptografía de la Universidad central Marta Abreu delas Villas, usando para ello la metodología de Mónica Izquierdo; así como un estudio bibliométrico de la producción científica sobre la temática abordada teniendo en cuenta indicadores de producción y colaboración.
3. El estudio de usuarios facilitó conocer tanto los autores más productivos, como las principales temáticas estudiadas en el grupo, con lo cual se realizaron redes de colaboración y temáticas.
4. La confección de la Base de Datos para el estudio bibliométrico en los años 2008, 2009, 2010, 2011, 2012 arrojó 244 documentos, con 2533 referencia y 536 autores, proyectando 963 publicaciones periódicas, constituyendo la fuente más utilizada.
5. El análisis de los documentos presentó en el año 2012 un crecimiento exponencial de esta ciencia debido a la importancia que han cobrado las investigaciones que demuestran que las única forma de obtener buenos Algoritmos Criptográficos es sometiéndolos al escrutinio de la comunidad científica.
6. La distribución geográfica facilitó conocer que en Cuba las principales instituciones que se dedican al estudio de esta ciencia son centros de educación superior, y la Universidad de la Habana cobra un papel protagónico.

7. En el caso de las instituciones nacionales se presentan como la piedra medular en tecnología criptográfica, países como Estados Unidos, la India, Rusia, Brasil y Alemania, pero solo centros de acceso restringido, colocando a Cuba como un ejemplo de estudios de carácter publico.
8. Se analizan de las 2533 referencias, las que no presentaban fecha, sumando un total de 42, así como las referencias de menos de 5 años, para un total de 307, lo que demuestra que el 87,9% de las publicaciones presentan años, y solamente en el 12,1% no aparecen, lo que da a las publicaciones más fiabilidad y facilita la búsqueda a las personas que deseen o necesiten consultarlas
9. El índice total coautoría existente en las 244 publicaciones con 636 autores es de un 2,6, demostrando que las publicaciones realizadas referentes a la temática son generalmente en colectivo.

Recomendaciones

Recomendaciones

- Continuar con las investigaciones referentes a la Producción Científica sobre Criptografía en años que no han sido analizados para concretar los principales avances existentes en la tecnología criptográfica.
- Socializar los resultados arrojados en la investigación con otros grupos existentes en el país que se dediquen al estudio de la ciencia.

Bibliografía Citada

Bibliografía Citada

ABADI, M. & WARINSCHI, B. (2008) Security analysis of cryptographically controlled access to XML documents. *Journal of the ACM* 55, pág.1–29.

AGUILAR, P. & OKTAÇ, A. (2004) Generación del conflicto cognitivo a través de una actividad de criptografía que involucra operaciones binarias. *RELIME,* 7, 117-144.

AGUIRRE, J. R. (2006) *Seguridad Informática y Criptografía,* Madrid.

DE BUSTOS, J. A. (2001) *Introducción a la Criptografía*.

FÚSTER, A., DE LA GUÍA, D., HERNÁNDEZ, L., MONTOYA, F. & MUÑOZ, J. (2004) *Técnicas Criptográficas de protección de datos,* Madrid, RA-MA.

HERNÁNDEZ, R., FERNÁNDEZ, C. & BAPTISTA, P. (2006) *Metodología de la Investigación,* México.

HJORLAND, B. (2002) Análisis de dominio en Ciencias de la Información - once enfoques- tradicionales e innovativos. *Journal of Documentation,* 58, 422-462.

HJORLAND, B. & ALBRECHTSEN, H. (1995) Toward a new horizon in information science: domain-analysis. *Journal of the American Society for Information Science* 46, 400-425.

IZQUIERDO, M. (1999) Una aproximación interdisciplinar al estudio del usuario: bases conceptuales y metodológicas. *Investigación Bibliotecológica,* 13.

LUCERA, M. J. (2010) *Criptografía y Seguridad en computadores*.

SOSA, G. (2010) Utilización de la transformada y matrices de Hadmord en las funciones booleanas y en el criptoanálisis. *Facultad de Matemática,*

Física y Computación. Cuba Universidad Central "Marta Abreu" de Las Villas.

SOSA, Y., TORRES, A. M. & SOSA, G. (2011) La gestión de información en el grupo de Criptografía de la UCLV desde la visión de las Ciencias de la Información.

SUBRAMANYAM, K. (1983) Bibliometric studies of research collaboration: A review. *Journal of Information Science*, 33-38.

VESSURI, H. (1995) Recent strategies for adding value to scienctific journals in Latin America. *Scientometrics,* 34, 139-161.

WHITE, H. & MCCAIN, K. (1998) Visualizing a discipline: an author co-citation analysis of information science, 1972-1995. *Journal of the American Society for Information Science,* 49, 327-355.

Bibliografía Consultada

Bibliografía Consultada

ABADI, M. & WARINSCHI, B. (2008) Security analysis of cryptographically controlled access to XML documents. *Journal of the ACM* 55, pág.1–29.

AGUILAR, P. & OKTAÇ, A. (2004) Generación del conflicto cognitivo a través de una actividad de criptografía que involucra operaciones binarias. *RELIME,* 7, 117-144.

AGUIRRE, J. R. (2006) *Seguridad Informática y Criptografía,* Madrid.

BRAAM, R. R., MOED, H. F. & VAN RAAN, A. F. J. (1991) Mapping of Science by Combined Co-Citation and Word Analysis. I. Structural Aspects. *Journal of the American Society for Information Science* 42**,** 233-251.

BUSHA, C. H. & HARTER, S. P. (1990) *Métodos de Investigación en Bibliotecología. Técnicas e Interpretación,* México, Félix Varela.

CANALES, H. & MESA, M. (2002) Bibliometría, Informetría, Cienciometría: Su Etimología y Alcance Conceptual. *Congreso Internacional de Información INFO.* Ciudad de la Habana.

CARVAJAL, R. (2009) El índice Hirsch y sus adaptaciones para la evaluación de académicos e investigadores: su aplicación a los dominios Comunicación y Ciencia de la Información en el Siglo XXI. *Bibliotecología y Ciencias de la Información.* Ciudad de la Habana, Universidad de La Habana.

CHAVIANO, O. (2004) Algunas consideraciones teórico-conceptuales sobre las disciplinas métricas. *Acimed,* 12.

DE BUSTOS, J. A. (2001) *Introducción a la Criptografía*.

DEL TORO, B. & LOZANO, I. (2007) Análisis de la Producción Científica de la Universidad de La Habana. *Bibliotecología y Ciencias de la Información.* Ciudad de la Habana, Universidad de la Habana.

DELGADO, E., TORRES, D., JIMÉNEZ, E. & RUIZ, R. (2006) Análisis Bibliométrico y de Redes Sociales aplicado a las Tesis Bibliométricas defendidas en España (1976-2002): Temas, Escuelas Científicas y Redes Académicas. *Revista Española de Documentación Científica,* 29**,** 493-524.

FÚSTER, A., DE LA GUÍA, D., HERNÁNDEZ, L., MONTOYA, F. & MUÑOZ, J. (2004) *Técnicas Criptográficas de protección de datos,* Madrid, RA-MA.

GORBEA, S. (2005) Modelo teórico para el estudio métrico de la información documental. España, Ediciones Trea.

HERNÁNDEZ, R. (2004) *Metodología de la Investigación I,* La Habana, Félix Varela.

HERNÁNDEZ, R., FERNÁNDEZ, C. & BAPTISTA, P. (2006) *Metodología de la Investigación,* México.

HJORLAND, B. (2002) Análisis de dominio en Ciencias de la Información -once enfoques- tradicionales e innovativos. *Journal of Documentation,* 58, 422-462.

HJORLAND, B. & ALBRECHTSEN, H. (1995) Toward a new horizon in information science: domain-analysis. *Journal of the American Society for Information Science* 46, 400-425.

IZQUIERDO, M. (1999) Una aproximación interdisciplinar al estudio del usuario: bases conceptuales y metodológicas. *Investigación Bibliotecológica,* 13.

KONHEIM, A. G. (1934) *Computer Security and Cryptography*.

LASCURRAIN, M. L. (2006) La evaluación de la actividad científica mediante indicadores bibliométricos. Madrid, Departamento de Biblioteconomía y Documentación. España: Universidad Carlos III de Madrid.

LUCERA, M. J. (2010) *Criptografía y Seguridad en computadores*.

MACÍAS, C. (1998) Papel de la informetría y de la cienciometría y su perspectiva nacional e internacional. *Seminario sobre Evaluación de la Producción Científica.* São Paulo por el Proyecto SciELO.

MALTRÁS, B. (2003) *Los indicadores bibliométricos. Fundamentos y aplicación al análisis de la ciencia.,* España.

MARTÍNEZ, A. (2004) Selección de lecturas de Estudios Métricos de la Información. La Habana.

MCCAIN, K. (1990) Mapping authors in intellectual space: a technical overview *Journal of the American Society for Information Science,* 41**,** 433-443.

MIGUEL, S. (2012) Producción científica de la UNLP en las revistas indizadas en Web of Science (WoS) y SCOPUS, 2006-2010.

MIGUEL, S., CAPRILE, L. & JORQUERA, I. (2008) Análisis de co-términos y de redes sociales para la generación de mapas temáticos *El profesional de la información,* 17**,** 637-646.

MOYA, F. & MIGUEL, S. (2009) Aproximación cienciométrica al análisis y visualización del dominio científico argentino, 1990-2005. *IV Encuentro de jóvenes investigadores (I Escuela Doctoral Iberoamericana) de estudios Sociales y Políticos sobre la Ciencia y la Tecnología*.

MOYA, F. et al., (2006) Visualización y análisis de la estructura científica española: ISI Web of science 1990-2005. *El profesional de la información,* 15**,** 258-269.

MOYA, F. et al., (2004) A new technique for building maps of large scientific domains based on the cocitation of classes and categories. *Scientometrics,* 61**,** 129-145.

NEIGHBORS, J. M. (1980) Software Construction Using Components. *Department of Information and Computer Science.* University of California, Irvine.

PERALTA, M. J. (2009) *Evaluación de la investigación científica institucional: la producción científica de la Universidad Central Marta Abreu de Las Villas durante el período 2000-2008*.

RUIZ, F. Estudio bibliométrico sobre la Producción Científica en la UCLM.

SÁNCHEZ, N. (2006) Aproximación al análisis del dominio higiene y epidemiología en Cuba a través de técnicas conexionistas y multivariantes. *VI Congreso Internacional de Informática en Salud.* Unidad de Análisis y Tendencias en Salud. Ministerio de Salud Pública. Cuba

SHNEIER, B. (1996) Applied Cryptography. Segunda ed.

SOSA, G. (2010) Utilización de la transformada y matrices de Hadmord en las funciones booleanas y en el criptoanálisis. *Facultad de Matemática, Física y Computación.* Cuba Universidad Central "Marta Abreu" de Las Villas.

SOSA, Y., TORRES, A. M. & SOSA, G. (2011) La gestión de información en el grupo de Criptografía de la UCLV desde la visión de las Ciencias de la Información.

SPINAK, E. (1996) *Diccionario enciclopédico de Bibliometría, Cienciometría e Informetría* Caracas, UNESCO.

SUBRAMANYAM, K. (1983) Bibliometric studies of research collaboration: A review. *Journal of Infomation Science*, 33-38.

TORRENS, M. E. (2007) Profesionales de la Información, su ámbito de acción y necesidad del cambio de motivación. *II Congreso Iberoamericano de Bibliotecología.*

VESSURI, H. (1995) Recent strategies for adding value to scienctific journals in Latin America. *Scientometrics,* 34, 139-161.

WHITE, H. & MCCAIN, K. (1998) Visualizing a discipline: an author co-citation analysis of information science, 1972-1995. *Journal of the American Society for Information Science,* 49, 327-355.

Anexos

Autores	% de Colaboración	
"Dodis, Yevgeniy"	0.3750	0.8718
"Segev, Gil"	0.3339	0.8571
"Izquierdo Donoso, Hugo"	0.1037	0.5699
"Wichs, Daniel"	0.4366	0.8840
"Brakerski, Zvika"	0.4160	0.8816
"Naor, Moni"	0.3544	0.8644
"Dahab, Ricardo"	0.9000	0.4031
"Aranha, Diego F."	0.6522	0.4521
"Jaggard, Aaron D."	0.5436	0.1282
"Rubio, Carlos García"	0.4080	0.1172
"Pigatto, Daniel Fernando"	0.5590	0.6583
"Scedrov, Andre"	0.5649	0.1331
"Misaghi, Mehran"	0.4336	0.1331
"Misoczki, Rafael"	0.4468	0.1429
"Corréa, Gustavo Testa"	0.1653	0.7748
"Billet, Olivier"	0.8267	0.3748
"Groenwald, Claudia Lisete Oliveira"	0.3940	0.8902
"Courtois, Nicolas"	0.1851	0.2755
"de Assis Olgin, Clarissa"	0.4212	0.8767
"Moreno Rossellé, Daniel"	0.5722	0.5920
"Camenisch, Jan"	0.4468	0.8583
"Carrera, Enrique V."	0.5590	0.3417
"Goldwasser, Shafi"	0.2958	0.8362

"Gallegos-García, Gina"	0.5033	0.7908
"Alwen, Joel"	0.5642	0.6374
"López, Julio"	0.7878	0.2301
"Ortega, Oscar Fernando Orcoapaza"	0.4930	0.8067
"Ortega, María"	0.4080	0.8840
"Pérez, Manuel José Lucena"	0.5766	0.5466
"Navarro, Pedro J."	0.5128	0.7748
"Overs, Leslie"	0.5312	0.7393
"Orueta, Gabriel Dfaz"	0.1396	0.7196
"Neto, Jorge da Silva Correia"	0.4336	0.8681
"Oliveira, Leonardo"	0.6998	0.1982
"Oliveira, G. A."	0.4703	0.1663
"Oliveira, Jonice"	0.5466	0.7000
"Oliveira, Karise Gon ccalves"	0.5392	0.7196
"Ontiveros, Beatriz"	0.4703	0.8350
"Nohl, Karsten"	0.1198	0.6583
"Nogueira, Rodrigo Borges"	0.2078	0.8350
"Oliveira, Cleber Henrique"	0.1271	0.6141
"Oliveira, Claudia"	0.3390	0.9000
"Pontes, Elvis"	0.4820	0.8215
"Potkonjak, Miodrag"	0.4586	0.8472
"Preneel, Bart"	0.5744	0.5699
"Polivio, Jorge"	0.1257	0.6804
"Pinto, Thiago Souza"	0.1337	0.6362
"Podestá, Ariel"	0.5532	0.6804
"Pointcheval, David"	0.4586	0.1540
"Presoto, Luís Eduardo Bilharva"	0.1557	0.7577

"Quisquater, Jean-Jacques"	0.7995	0.3147
"Ramos, Benja"	0.5224	0.7577