Ciencias de la Información ISSN: 0864-4659 Vol. 47, No. 2, mayo-agosto, pp. 11- 18, 2016

Modelos y herramientas para la vigilancia tecnológica

Models and tools for Technological surveillance

Yelena Islen San Juan
Felix Ivan Romero Rodríguez

La vigilancia tecnológica es uno de los ejes de la vigilancia estratégica que contempla información de carácter científico y técnico. Los modelos para la vigilancia tecnológica, apoyados en herramientas informáticas contribuyen a desempeñar de manera eficaz este proceso. Se realiza un análisis de los modelos y herramientas existentes para la vigilancia tecnológica, mediante el empleo de métodos como análisis documental, análisis-síntesis, inductivo-deductivo, histórico-lógico y el dialéctico. Los modelos y herramientas para la vigilancia tecnológica analizadas presentan insuficiencias que influyen negativamente en el proceso de vigilancia tecnológica. El desarrollo de un modelo inteligente para la vigilancia tecnológica basado en tecnologías de la Web semántica, contribuirá a mejor eficacia de la información que brinda la Web.

***Palabras clave**: Vigilancia tecnológica, Modelos para la vigilancia tecnológica, Herramientas de vigilancia tecnológica, Web semántica, Agentes inteligentes.*

RESUMEN

ABSTRACT

Technological surveillance is one of the axes of strategic surveillance that includes information of a scientific and technical nature. Models for technology surveillance, supported by computer tools, contribute to the effective performance of this process. An analysis of existing models and tools for technological surveillance is carried out using methods such as documentary analysis, analysis-synthesis, inductive-deductive, historical-logical and dialectical. The models and tools for technology surveillance analyzed have shortcomings that negatively influence the technological surveillance process. The development of an intelligent model for technology surveillance based on semantic Web technologies will contribute to abetter effectiveness of the information provided by the Web.

***Keywords**: Technological surveillance, Models for technological surveillance, Tools for technological surveillance, Semantic Web, Intelligent Agents.*

Introducción

Las organizaciones desempeñan un papel fundamental dentro de la sociedad de la información, por ello: «Una organización que aspire a competir con éxito en el entorno actual debe aprender a aprender, debe hacer explícitos los procesos que permiten incorporar la información pertinente y relevante de que dispone, debe aplicar con creatividad e iniciativa las experiencias y el saber que ofrecen, en primer término, sus propios integrantes, sus proveedores, los grupos de interés y los clientes, es decir, la sociedad en su conjunto y más específicamente aquellos sectores en los que dicha organización actúa.»(Mesa, 2015)

La robustez y competitividad de las organizaciones de hoy, inmersas en la sociedad de la información se encuentran consolidadas por su capacidad para crear valor. Valor que se ve reflejado mediante la solución de los desafíos que promueve el entorno, la identificación y desarrollo de salidas de información útiles, que aporten a sus decisiones y servicios, es

decir, mediante la gestión de la información y el conocimiento; cuyo conocimiento y gestión se encuentran enlazados con la creatividad y capacidad de innovación para lograr su rentabilidad y supervivencia (Murillo, 2010).

El avance en las tecnologías ha ocasionado un cambio cultural y social en las formas tradicionales de enseñanza y en la manera en la cual se trasmite el conocimiento. Estos cambios obligan a las organizaciones a contar con información anticipada de los competidores, convertirla en conocimiento, elaborar un conocimiento que sea relevante para el negocio y utilizarlo para alcanzar sus objetivos. (Aldasoro Aluztiza, L, & Carrasco, 2012).

La actividad organizacional en un medio de constante cambio, implica la necesidad de establecer un sistema de monitoreo. La vigilancia estratégica es una «herramienta de gestión de la innovación que permite transformar la información recogida por una organización en ideas que la lleven a mejorar, haciéndola más competitiva y capaz dentro de su entorno»(CENTINELA, 2015), por lo que facilita el monitoreo dentro de las organizaciones.

La vigilancia estratégica abarca cuatro ejes: vigilancia competitiva, comercial, tecnológica y del entorno (Murillo, 2010). La vigilancia tecnológica es un «proceso ordenado y constante de observación y análisis del entorno y tecnológico. La vigilancia tecnológica identifica cambios que permitan alertar sobre amenazas y oportunidades de desarrollo tecnológico para los diferentes sectores económicos.» (SENA, 2015).

Las organizaciones realizan el proceso de vigilancia tecnológica de dos maneras. La primera forma es acceder a revistas, participar en eventos y ferias nacionales e internacionales, cursos, seminarios, fórum y visitas a otras organizaciones punteras del sector (extranjero). La segunda forma es a través de recursos tecnológicos ,fundamentalmente relacionados al uso de la Internet.

La Web ha evolucionado de forma considerable, en un inicio se comportó como una Web estática (solo lectura), luego pasó a una Web de colaboración e intercambio, la cual se reconoce como la Web 2.0. La Web 2.0 ha marcado un avance en la forma de usar Internet, ya que los usuarios colaboran y contribuyen en el contenido de la red, son parte de una sociedad que genera información y conocimiento. La información se encuentra dispersa en sitios web, blogs, redes sociales, repositorios, revistas electrónicas y otros recursos.Tener acceso a tanta información precisa de una gestión compleja.

El objetivo del presente trabajo es realizar un análisis de los modelos y herramientas existentes para la vigilancia tecnológica con el fin de demostrar la utilidad del uso de la web semántica, agentes inteligentes como herramienta de vigilancia tecnológica.

Contenido

Materiales y métodos

Entre los materiales y métodos de trabajo científico utilizados se destacan los siguientes:

Análisis-síntesis, para el estudio de las fuentes bibliográficas existentes referente a los modelos y herramientas para la vigilancia tecnológica, identificando los elementos más importantes.

Inductivo-deductivo, para el estudio de las principales iniciativas de vigilancia tecnológica, las normas, modelos y herramientas utilizados para llevar a cabo el proceso de vigilancia tecnológica.

Método histórico-lógico y el dialéctico para el estudio crítico de los trabajos anteriores, y para utilizar estos como punto de referencia y comparación de los resultados alcanzados.

Análisis y discusión

Las organizaciones requieren buscar información, mantenerla actualizada y disponible sobre los siguientes aspectos: (SIERRA, 2013)

• Patentes, modelos de utilidad, diseños industriales e internacionales.

• Legislación y Normativas que puedan afectar a la actividad de la organización o la de los clientes o proveedores.

• Coyuntura socio-económica en el país o países objetivo.

• Noticias sobre avances científicos y técnicos. Tesis doctorales, publicaciones científico-técnicas de universidades, centros de investigación y organismos.

• Información sobre ayudas y subvenciones.

• Productos, precios, calidades y condiciones de venta de los competidores.

• Ferias profesionales: sectores emergentes, nuevos competidores, estrategias de distribución, nuevos productos.

La actividad de vigilancia tecnológica abarca un conjunto de procesos que se vinculan a:

• Planeación: identificar necesidades. Validar fuentes.

• Búsqueda y recuperación: observar, descubrir, buscar, detectar, recolectar y captar

• Procesamiento: clasificar, tratar, almacenar. Validar información.

• Análisis: aportar valor añadido a la información. Buscar incidir en la estrategia.

• Difusión de la información: comunicar a los directivos de la organización. Difundir información. Transferir conocimiento.

Caracterización de modelos y herramientas para vigilancia tecnológica

Modelos para vigilancia tecnológica

Montes (2014) realiza un estudio exhaustivo sobre modelos de vigilancia tecnológica que son aplicados en distintos sectores económicos-institucionales. Montes (2014) proyecta que los modelos se documentan a partir de dos enfoques: el primero son modelos para implementar y estructurar así sistemas de vigilancia tecnológica, que incluye actividades como sensibilización, diagnóstico, implementación y puesta en marcha. El segundo enfoque hace referencia a modelos para desarrollar operativamente la vigilancia tecnológica, en los cuales se contemplan cinco actividades básicas que son: planeación, búsqueda, análisis, inteligencia y difusión, y permiten el

Tabla 1: Clasificación de los modelos de vigilancia tecnológica de acuerdo a su enfoque. Fuente: (Montes, 2014)

Modelos	Modelos para implementar y estructurar sistemas de vigilancia tecnológica	Modelos para desarrollar operativamente la vigilancia tecnológica
Modelo de Salgado, Guzmán y Carrillo (2003)	x	
Modelo de Castro (2007)		x
Modelo de Malaver y Vargas (2007)		x
Modelo de Colciencias – TRIZ XXI (2006)		x
Modelo de Coca, García, Santos y Fernández (2010)	x	x
-Modelo de García, Ortoll y López (2011)		x
Modelo de Oroz (2013)	x	x
Montes (2014)		x

el desarrollo de estudios y elaboración de informes de vigilancia.

Modelo de Salgado, Guzmán y Carrillo (2003)
Modelo de Vigilancia Científico-Tecnológica para el Instituto de Investigaciones de la Industria Alimentaria (IIIA). El modelo cumple con la norma francesa AFNOR XP X 50 - 053 y se estructura en diez etapas:

• Sensibilización. Se identifican las personas que liderarán con Factores Críticos de Vigilancia (FCV).

• Conocimiento de la Situación. Se realiza un levantamiento de la información a partir de la realización de varios encuentros con los responsables de cada área y la consulta de diferentes documentos de la empresa en caso de ser necesario para tener un conocimiento detallado de la organización.

• Definición de los Objetivos. Se valora la alineación entre los objetivos y la misión de la organización.

• Ejes de Vigilancia. Se establecen las prioridades entre los objetivos de la organización y se determinan cuáles son las líneas generales y específicas que deben seguirse. En esta etapa se formulan los posibles FCV, en relación con los objetivos estratégicos de la organización y con ello, se procurará que el modelo impacte directamente sobre la estrategia de la organización.

• Diagnóstico de la Organización y de las Prácticas. El suministrador del servicio en esta etapa, realiza un diagnóstico de la organización y las prácticas habituales de las personas en la entidad. En este punto, es importante considerar el sistema de gestión, las prácticas en la difusión de la información y los canales habituales para ello, así como los hábitos en cuanto a la recolección, circulación, procesamiento y utilización de la información en los procesos de decisión.

• Censo de las Fuentes. Se realiza un inventario de las fuentes de información utilizadas por la organización en sus actividades, teniendo en cuenta la disponibilidad de bases de datos comerciales, de mercado y empresariales, científicas, técnicas, sistemas de información internos, entre otros.

• Evaluación de las Diferencias. En esta fase el suministrador del servicio debe disponer de la información que le permita evaluar y analizar las diferencias entre la situación actual de la organización en términos de procesos de información y la situación solicitada, a partir de los ejes de vigilancia.

• Recomendaciones. Esta fase se compone de las actividades siguientes: -censo de las categorías de información que debe recoger la entidad para alimentar sus ejes de vigilancia; -Jerarquización de las fuentes de información necesarias y que deben movilizarse (fuentes controladas o no en el momento del diagnóstico), así como la evaluación de los costos de acceso; -proposición de las herramientas, métodos y una organización adaptada a la cultura empresarial, lo que debe permitir una mejor recolección y selección, circulación, procesamiento y, en ocasiones, el almacenamiento de la información.

Cuando las recomendaciones del suministrador son aceptadas por parte de la entidad, se procede a la ejecución o establecimiento del modelo de vigilancia propuesto.

• Establecimiento. Se considera el modelo de vigilancia dentro de la estructura de la organización, se hace una propuesta sobre las diferentes formas de establecimiento. Por ejemplo, centralizada, matricial, por procesos.

• Acompañamiento. Consiste en asesorar y ayudar a la entidad en la aplicación y desarrollo de su Modelo de vigilancia se realiza durante un largo período, en función de las necesidades del cliente. Esta etapa es opcional.

Modelo de Castro (2007)
Guía Práctica de vigilancia estratégica de Castro (2007). Cuenta con seis procesos:

• Definición de las necesidades
• Búsqueda y recogida de la información

• Tratamiento de la información

• Difusión y protección de la información

• Proceso de decisión de la empresa. En este proceso se pone en marcha nuevos proyectos o programas de I+ D, cambios en la estrategia tecnológica de la empresa, adelantar el lanzamiento de nuevos productos y servicios.

Modelo de Malaver y Vargas (2007)
Modelo propuesto por Malaver y Vargas (2007), aplicado en la investigación «Creación e implementación de cinco unidades sectoriales de vigilancia tecnológica en Bogotá y Cundina». Desarrollado por la Cámara de Comercio de Bogotá (CCB) y el Observatorio Colombia no de ciencia y tecnológica (OCyT). El propósito del trabajo consistió en lograr que los Centros de Desarrollo Tecnológico (CDT) tuvieran la capacidad para ofrecer nuevos servicios, a través de la realización de ejercicios de vigilancia tecnológica enfocados al sector empresarial. Consta de cinco etapas: Planificación, búsqueda y capacitación, análisis y organización, inteligencia y comunicación. Las dos primeras se encuentran relacionadas con el proceso de captura y organización de los datos generales y las tres etapas posteriores están relacionadas con la inteligencia, donde se realiza el procesamiento de la información con valor añadido, lo que genera conocimiento para ser utilizado en la toma de decisiones.

Modelo de Colciencias - TRIZ XXI (2006)
Modelo de vigilancia y prospectiva tecnológica aplicado en los centros de investigación de excelencia en Colombia propuesto por Colciencias TRIZ XXI (2006). Tiene como cometido orientar las capacidades nacionales en prospectiva y vigilancia tecnológica para el desarrollo de áreas estratégicas de la ciencia, la tecnología y la innovación aplicadas a la economía del conocimiento, de manera que genere información relevante y condiciones suficientes para el direccionamiento estratégico y la focalización del ámbito de acción científico y tecnológico de los centros de excelencia. Consta de seis etapas: Identificación del tema y objeto de vigilancia; identificación y validación de fuentes, palabras claves, subsistemas y criterios de selección, búsqueda, recolección y organización de información, análisis de la información, validación de los resultados por expertos e informe de vigilancia tecnológica.

Modelo de Coca, García, Santos y Fernández (2010)
Otro de los modelos encontrados en la literatura y que requiere de especial atención, corresponde a la Guía de Vigilancia Estratégica - Proyecto Centinela construido por Coca et al. (2010). En esta guía de vigilancia estratégica se expone la metodología que se ha desarrollado para organizar el proceso de vigilancia estratégica dentro una entidad, de manera que pueda ser empleada como punto de partida para el desarrollo de una sistemática propia, con base en la experiencia previa de la Fundación PRODINTEC y a las referencias normativas UNE 166006 EX y UNE 166002 (Sistemas de Gestión de la I+D+i).

Modelo de García, Ortoll y López (2011)
Modelo que tiene como objetivo analizar y describir la aplicación y función de la inteligencia en las universidades españolas para definir su estrategia en el diseño de las titulaciones y adaptarse al EEES (Espacio Europeo de Educación Superior). Cuenta con una fase de identificación de necesidades de información; recogida de información y organización; análisis y generación de productos, así como la difusión y uso.

Modelo de Oroz (2013)
Modelo de vigilancia tecnológica propuesto por Oroz (2013). Cuenta con 7 procesos: determinación de los factores críticos de vigilancia / recursos; recogida de la información; filtro y análisis de la información; difusión de los resultados; protección de los resultados; y por último revisión.

Montes (2014)
Modelo cuya base radica en los modelos antes expuestos, el cual consta de cinco fases:

• Generación de oportunidades de investigación: se establece una jerarquía de los factores críticos de vigilancia, con el fin de a bordar aquellos temas que estén orientados con los lineamientos estratégicos. Luego define los recursos humanos, físicos, técnicos y financieros con los que se cuenta para poder abordar dicha necesidad.

• Aproximación al estado del arte: fase que define la estrategia de búsqueda de información identificación de las palabras claves que caracterizan la necesidad.

• Organización y análisis de la información: realiza nuevamente un filtro de la información para garantizar que es útil.

• Ejecución del proyecto de investigación: realiza un fortalecimiento continuo de la información seleccionada, lo cual puede lograrse mejorando la ecuación de búsqueda y/o identificando fuentes de información nuevas.

• Difusión y uso de los resultados de investigación: fase que contempla la creación de un plan de comunicaciones, siendo necesario establecer específicamente la forma como se llevará el proceso de difusión de los resultados, tanto a nivel interno como a nivel de los posibles beneficiarios y/o actores de interés.

Herramientas para la vigilancia tecnológica

En el mercado existen diversas plataformas web que brindan soporte automatizado al proceso de vigilancia tecnológica. Estas plataformas contienen funcionalidades de rastreo, captura y tratamiento de información, gestión de los contenidos y administración de usuarios. De igual forma, facilitan la difusión de los resultados mediante la generación de alertas y boletines para las personas involucradas en la toma de decisiones estratégicas. (Fernando Martínez Rivero, 2014)

Las plataformas web seleccionadas para la investigación fueron tomadas de (Fernando Martínez Rivero, 2014), (Campis & Gámez, 2012) y (Ovit, 2015), quienes realizan un estudio exhaustivo sobre las herramientas que apoyan el ciclo completo de la vigilancia tecnológica.

• **SoftVT** (de AIMPLAS, Instituto Tecnológico del Plástico, España): software diseñado para ayudar en el proceso de vigilancia tecnológica a descubrir tecnologías emergentes, tiene como objetivo fundamental automatizar los procesos relacionados con la captura, administración y distribución de la información estratégica. Cuenta con tres módulos:

1-Recuperación de la información. Módulo autónomo para configurar y descargar las fuentes de información, el usuario puede monitorearlas y obtener los resultados en un formato estándar para su posterior uso. Gestiona información como artículos científicos, noticias, patentes, legislación, normas técnicas, contratos públicos; así mismo realiza comprobación de duplicados, clasifica la información por: indexación, tipología y asignación en el índice temático y la jerarquiza a través de temas y subtemas.

2-Gestión de la información. En el módulo se toma la información suministrada y ofrece estrategias.

3-Módulo gestión de usuarios. Módulo en el cual se admite la creación de diferentes perfiles de usuarios, asignándoles roles para el acceso de información. Este módulo cuenta con un control y renovación de suscripciones a los diferentes productos de información y admite crear listas de favoritos.

• **Vigiale** (de IALE Tecnología, S.L., España): plataforma que integra tecnologías de la Web 2.0 para la gestión de la vigilancia tecnológica. Posibilita vigilar el entorno siguiendo notificaciones de cambio de las fuentes preestablecidas, admite la recuperación de información desde Internet de patentes, publicaciones científicas, noticias, blogs. Al automatizar la búsqueda y recopilación de información, les suministra a los usuarios la mayor información en el menor tiempo posible. Consta de las siguientes características:análisis y clasificación semántica de contenidos; filtros para la selección de información; gestión integral de estudios de vigilancia tecnológica; y búsqueda interna y clúster de resultados.

• **Xerka** (de Aiatek/Diana Tecnología, España): un software permite la vigilancia automáticamente aparición de nueva información de interés para la empresa. Automatiza los procesos de búsqueda, análisis, clasificación y difusión de dicha información. Combina diferentes tecnologías para automatizar las fases del proceso de vigilancia y proporcionar al usuario información lista para su explotación en los procesos de inteligencia competitiva. Tiene como características: alerta acerca del entorno determinado por el usuario; proporciona un repositorio actualizado con información de interés; y precisa de varios sistemas de búsqueda dentro para explotar al máximo la información disponible.

• **Hontza** (de CDE + Investic, España): plataforma que se basa en la norma UNE 166.006: 2011 para la vigilancia tecnológica y la inteligencia competitiva,de la Asociación Española de Normalización (AENOR). Permite gestionar el despliegue estratégico de la organización, las fuentes de información (automatizadas o basadas en personas), el filtrado, la validación, el análisis y la puesta en valor, así como la distribución, la generación de ideas y la toma de decisiones estratégicas. Integra mecanismos de colaboración de la Web 2.0, como son: anotar, puntuar, marcar, etiquetar, adjuntar documentos, o comenzar un debate selectivo a partir de cualquier información.

• **Miniera** (de Miniera S.L., España): software de inteligencia competitiva y vigilancia tecnológica que brinda apoyo a empresas para desarrollar tareas de captura, validación, depuración, análisis, difusión y visualización de información. Integra herramientas para recuperar información comercial, a través de noticias; tecnológica, mediante patentes, literatura científica y publicaciones de referencia; y procedente de las redes sociales, especialmente Twitter y Facebook. Realiza seguimiento de fuentes de libre y de pago, de páginas relevantes a través de sus cambios. Valida, depura y organiza información para aceptar aquella relevante y la difunde a través de múltiples canales y formas de envío, como boletines, alertas y portales.

• **Vicubo** (de e-intelligent, España): Permite la monitorización de fuentes de información, a través de servicios de suscripción y clasificación personalizada (seguimiento de páginas web, blogs, redes sociales, patentes, legislación, noticias). Sistematización del proceso de vigilancia tecnológica e inteligencia competitiva, a través de información personalizada y herramientas avanzadas de: búsqueda, clasificación, almacenamiento, análisis, edición y difusión; alertas de correo electrónico, boletines personalizados y otros servicios que favorecen el trabajo en equipo y la toma de decisiones, siguiendo el ciclo de la norma UNE 166.006.

En relación a los indicadores: apoyo al ciclo completo de vigilancia tecnológica, gestión de contenidos, administración de usuarios, licenciamiento, accesibilidad y uso de normativas se puede evidenciar en la figura 1 que la plataforma Hontza alcanza la puntuación mayor: 93 puntos; seguida de Vigiale y Vicubo, ambas con 88 puntos y SoftVT con 84 puntos, son las mejores plataformas para la vigilancia tecnológica.

Los modelos y herramientas para la vigilancia tecnológica presentan insuficiencias que atentan contra la eficacia de la información que brinda la Web para la vigilancia tecnológica:

• Los modelos para la vigilancia tecnológica no incorporan en las fases de búsqueda y tratamiento de la información agentes inteligentes, lo que incide en la rapidez y efectividad de los resultados.

• Las herramientas que los modelos proponen para la vigilancia tecnológica son en su mayoría privativas, lo cual constituye

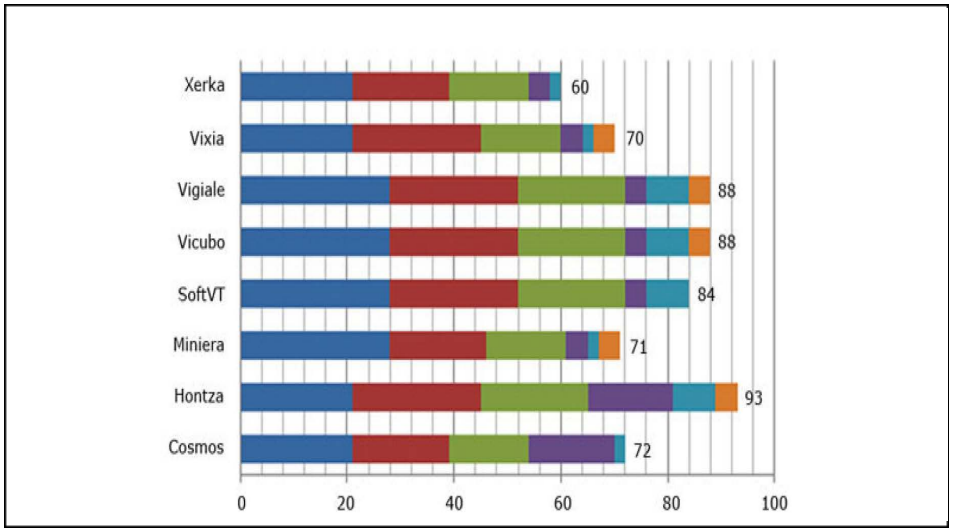

Figura 1. Comparación de herramientas para la vigilancia tecnológica. Fuente: (Fernando Martínez Rivero, 2014)

una limitante para países de pocos recursos y atenta contra la soberanía tecnológica.

- Las herramientas para vigilancia tecnológica no presentan servicios de la Web 3.0 para la búsqueda de información, por lo que no se busca por significado. Buscar por significado mitiga problemas derivados por: falta de normalización, ambigüedad de nombre autor e instituciones.

- Las herramientas para vigilancia tecnológica no incorporan todo tipo de recurso digital, lo que restringe el umbral de la información a consultar.

- Las herramientas para vigilancia tecnológica no delegan el procesamiento de la información a los dispositivos, lo que imposibilita proveer relaciones de equivalencias y conceptos.

- Las herramientas para vigilancia tecnológica no explotan las posibilidades de integración de la información con tecnologías de la web semántica.

- El vigía en su mayoría realiza el proceso de vigilancia tecnológica de forma manual, lo que atenta contra la rapidez y efectividad del proceso.

- Escasa retroalimentación de la información de interés, lo que afecta el aprendizaje organizacional.

Web semántica

La Web semántica constituye una estrategia que contribuye a resolver los problemas relativos al manejo de la información como son: gestión de grandes cantidades de datos, recuperación de la información en datos no estructurados y la falta de relaciones entre los datos (Aldasoro Aluztiza, L, & Carrasco, 2012).

La Web semántica cuenta con un conjunto de tecnologías para cumplir sus metas. Entre ellas se pueden citar (Bernal, Castro, & González, 2014),(Martín Pérez Guevara, 2012):

Los datos enlazados conocido en inglés *linked data* son una ampliación de la WWW, que aprovecha la arquitectura que esta provee para abarcar cualquier objeto o concepto y utiliza los hipervínculos

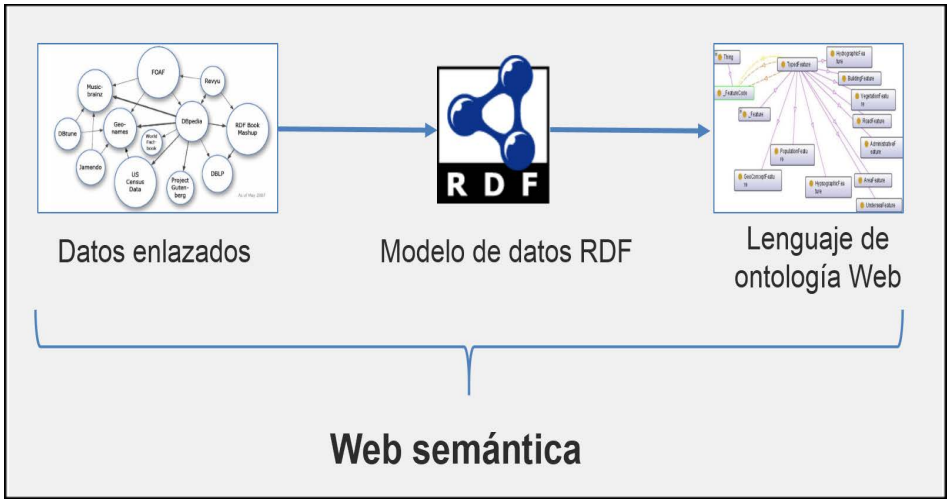

Figura 2: Web semántica

trasfigurados a RDF para distinguirlos de los hipervínculos de documentos clásicos. Los RDF son un estándar para los metadatos, elemento esencial para la recuperación de la información. Estos son datos que describen a otros datos. Las ontologías en este caso OWL (Web Ontology Language) son una extensión del modelo de datos de RDF, permite que la descripción de recursos sea más natural y completa. Tiene como objetivo describir el significado implícito y el por qué se da determinada conceptualización al contexto de cierto elemento.

Agentes inteligentes

Agentes inteligentes es un término que procede del área de la inteligencia artificial y es un sistema computacional capaz de actuar de manera autónoma para satisfacer sus objetivos y metas. Estos contribuyen a la recuperación de la información.

Las técnicas utilizadas en el desarrollo de agentes inteligentes son provenientes del área de técnicas aprendizaje por computadora (*Machine Learning*) de la inteligencia artificial.

Redes neuronales artificiales (RNA): son definidas como una máquina diseñada para modelar la forma en que el cerebro realiza una cierta tarea o función de interés (como una máquina adaptativa). Siendo más formales en la definición, se diría que una red neuronal es un procesador distribuido en forma masivamente paralela hecho de unidades de procesamiento simples, que tiene una propensión natural a guardar conocimiento debido a la experiencia y hacerlo accesible para su uso (Gutierrez, 2012). Debido a su fundamentación, las redes neuronales

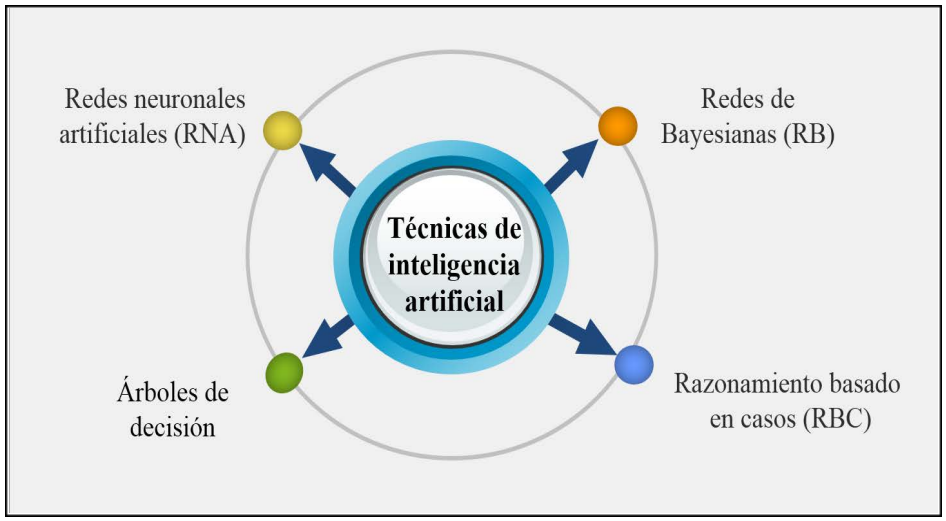

Figura 3: Técnicas de inteligencia artificial para el desarrollo de agentes inteligentes

presentar grandes semejanzas con el cerebro; por ejemplo, ambos son capaces de aprender de la experiencia, generalizar a partir de casos anteriores y casos nuevos, y abstraer características relevantes a partir de un gran número de entradas que representan información irrelevante (Puga, 2012).

Redes de Bayesianas (RB): son herramientas de modelado estadístico destinadas a representar un conjunto de incertidumbres relacionadas. Su estructura gráfica y su fundamento probabilístico las hace apropiadas para modelar sistemas multivariados orientados a la clasificación, el diagnóstico y la toma de decisiones (Lozano, 2011). En el artículo El papel de las redes bayesianas en la toma de decisiones, (Sánchez, 2011)define RB como un modelo probabilístico que relaciona un conjunto de variables aleatorias mediante un grafo dirigido, son redes graficas sin ciclos en el que se representan variables aleatorias y las relaciones de probabilidad que existan entre ellas que permiten conseguir soluciones a problemas de decisión en casos de incertidumbre.

Razonamiento basado en casos (RBC): es una rama de la IA que se preocupa por el estudio de los mecanismos mentales necesarios para repetir lo que se ha hecho o vivido con anterioridad, ya sea por uno mismo, o ya sea por casos concretos recopilados en la bibliografía o en la sabiduría popular. Es un paradigma de solución de problemas que es capaz de utilizar el conocimiento específico adquirido en situaciones previas y utilizarlo en la situación presente. Un problema nuevo se resuelve buscando en la memoria un caso similar resuelto en el pasado.

Incrementa su conocimiento almacenando el nuevo caso para ser usado en situaciones futuras. Esto permite que el mismo se mantenga actualizado en todo momento. Este método intenta llegar a la solución de nuevos problemas, de forma similar a como lo hacen los seres humanos. Es una tecnología de la IA que representa el conocimiento como una base de datos de casos y soluciones. (Abián, 2005)

A los efectos de esta investigación se considera que las RNA no aplican en la investigación debido a que su eficiencia radica en la calidad y cantidad de información que necesita para su entrenamiento. Durante el proceso de aprendizaje se va refinando iterativamente la solución hasta conseguir un nivel de operación adecuado para que pueda ser utilizada. Las RB por presentar limitaciones para manejar la retroalimentación en las relaciones causales, dificultad para determinar de manera exacta las probabilidades en muchos problemas y obtención de las RB a partir de expertos, lo cual dificulta la toma de decisiones (VÁZQUEZ, 2013). Se considera que la técnica de RBC para el desarrollo de agentes inteligentes es factible debido a su capacidadde utilizar el conocimiento obtenido en escenarios anteriores y aprovecharlo en un escenario actual, al comparar el nuevo problema con los casos almacenados previamente en la base de casos (Memoria de Casos) y recuperar los coincidentes, para luego aplicar al problema actual.

Conclusiones

Después de realizado el estudio del estado del arte sobre los modelos y herramientas para la vigilancia tecnológica se concluye:

- Los modelos y herramientas para la vigilancia tecnológica presentan insuficiencias que atentan contra la eficacia de la información que brinda la Web en la vigilancia tecnológica.

- La Web semántica constituyen una evolución importante de la Web que contribuye a mitigar problemas relativos al manejo de la información.

- Los datos enlazados permiten relacionar cualquier concepto u objeto al brindar significado al contenido a través de los RDF, lo que permite delegar tareas específicas al software de manera que sea capaz de procesar su contenido, razonar con este, combinarlo y realizar deducciones lógicas para resolver problemas cotidianos automáticamente.

- Los agentes inteligentes constituyen un elemento esencial para automatizar procesos cotidianos, por ser capaces de aprender y así satisfacer sus objetivos y metas.

- La técnica de razonamiento basado en caso es ventajosa para la incorporación de experiencias obtenidas en la vigilancia tecnológica en los nuevos proyectos que se acometan.

Refrencias, estilo APA 5ta edición

(2011). Intelligent RSS News Aggregation Based on Semantic Contexts .

Abián, M. Á. (2005). El futuro de la Web.

Aenor. (2011). Gestión de la I+D+i: Sistema de vigilancia tecnológica e inteligencia competitiva. Madrid: UNE 166006.

Aldasoro Aluztiza, J., L, C. J., & Carrasco, C. (2012). La vigilancia tecnológica y la inteligencia competitiva en los estándarez de gestión de la calidad en I+D+i. Obtenido de http://adingor.es/congresos/web/uploads/cio/cio2012/SP_04_Gestion_Innovacion_Tecnologica_y_Organizativa//1162-1168.pdf

Bernal, D., Castro, A., & González, J. (2014). Web Semántica, más de una decada de su aparición. Obtenido de Revista Puente Científica: http://puente.upbbga.edu.co/index.php/revistapuente/article/view/145

Berners-Lee, T. (2001). The Semantic Web, Scientifi American.

Berners-Lee, T. (2006). Obtenido de Linked Data - Design Issues: http://www.w3.org/DesignIssues/LinkedData.html. 7,26,82

Campis, L. E., & Gámez, Z. J. (2012). Influencia de los agentes inteligentes en el proceso de vigilancia tecnológica. Gerenc. Tecnol. Inform.

Centinela, P. (23 de 09 de 2015). Fundación PRODITEC. Obtenido de Guía de vigilancia estratégica: http://www.prodintec.es/catalogo/ficheros/aplicaciones/fichero_13_5034.pdf

Fernando Martínez Rivero, E. R. (2014). Evaluación de plataformas web para su implementación

en el sistema de vigilancia tecnológica de la Consultoría Biomundi. Revista Cubana de Información en Ciencias de la Salud.

Guerra, A. (2013). Agentes Inteligentes. Obtenido de http:// www.uv.mx/aguerra/ documents/2013-ia2-01.pdf

Gutierrez. (2012). Descubrimiento de conocimientos en la base de datos académica Universidad Autónoma de Manizales aplicando redes neuronales.

La Web1.0, 2.0, 3.0 Y 4.0. (24 de 09 de 2015). Obtenido de http:// www. La Web 1.0, 2.0, 3.0 Y 4.0.htm

Lozano, M. R. (2011). El papel de las redes Bayesianas en la toma de decisiones.

Martín Pérez Guevara, E. M. (2012). Propuesta de un modelo predictivo de la variación del precio de acciones basado en redes neuronales y análisis de estado financiero. Dialnet, 3-5.

Mesa, L. Y. (22 de 09 de 2015). De la gestión de información a la gestión del conocimiento,2014. Obtenido de http://bvs.sld.cu/revistas/ aci/vol14_1_06/aci02106.htm

Montes, C. O. (2014). Modelo de vigilancia tecnológica e inteligencia competitiva.

MSc. Fernando Martínez Rivero, M. E. (2014). Evaluación de plataformas web para su implementación en el sistema de vigilancia tecnológica de la Consultoría Biomundi. Obtenido de Revista Cubana Información en Ciencia de la Salud: http://rcics.sld.cu/ index.php/acimed/article/ view/559

Murillo. (2010). Los Factores Críticos de Éxito. Revista Delphos – Información a su. Obtenido de http://www.orestesenlared. com.ve/Dilomadounefa/ Los_factores_criticos_del_exito.

OVTT. (10 de 10 de 2015). Instrumentos para la vigilancia tecnológica. Obtenido de http:// www.ovtt.org/vigilancia-tecnologica-instrumentos

Puga, J. L. (2012). Cómo Construir y Validar Redes Bayesianas con Netica.Revista Electrónica de Metodología Aplicada, 1.

Sánchez. (2011). Sistema de detección de personas duplicadas en un Sistema de Gestión de Información Médica.

SENA. (01 de 10 de 2015). Modelo de Vigilancia Tecnológica SENA. Obtenido de http:// es.slideshare.net/mauromesa/ modelo-vigilancia-tecnolgica-sena

Sierra, J. F. (2013). Inteligencia competitiva e ciudades inteligentes caso salud pública. 16-18.

Vázquez, M. Y. (2013). Modelo de ayuda a la toma de decisiones basado en mapas.

Recibido: 10 de febrero de 2016.
Aprobado en su forma definitiva:
19 de mayo de 2016

Yelena Islen San Juan
CITMATEL,
La Habana, Cuba.
Correo-e.:yelena@citmatel.inf.cu

Felix Ivan Romero Rodríguez
Codechanic,
La Habana, Cuba.
Correo-e.: firomeroro4@gmail.com