

## IOT: UNA APROXIMACION DESDE CIUDAD INTELIGENTE A UNIVERSIDAD INTELIGENTE

### IOT: AN APPROACH FROM INTELLIGENT CITY TO INTELLIGENT UNIVERSITY

Phd. Jorge A. Parra-Valencia <sup>a</sup> Phd. Cesar D. Guerrero <sup>b</sup> MSc. Dewar Rico Bautista <sup>c</sup>

<sup>a</sup> Universidad Autónoma de Bucaramanga. Grupo de Investigación Pensamiento Sistémico  
Bucaramanga, Colombia, [japarra@unab.edu.co](mailto:japarra@unab.edu.co)

<sup>b</sup> Universidad Autónoma de Bucaramanga. Centro de Investigación en Ingeniería y  
Organizaciones, Centro de Excelencia y Apropiación en IoT - Nodo Oriente, Grupo de  
Investigación en Tecnologías de Información, Bucaramanga, Colombia, [cguerrer@unab.edu.co](mailto:cguerrer@unab.edu.co)

<sup>c</sup> Universidad Francisco de Paula Santander Ocaña. Grupo de Ingeniería en Innovación,  
Tecnología y Emprendimiento – GRIITEM, Ocaña, Colombia, [dwracob@ufpso.edu.co](mailto:dwracob@ufpso.edu.co)

**Fecha de recepción:** 08-03-2017

**Fecha de aprobación:** 30-05-2017

**Resumen:** Se contextualiza desde el Internet de las Cosas y su vital importancia para las Smart Cities y el concepto emergente de Smart University. Estos últimos con sus características: Smart Governance, Smart People, Smart Living, Smart Mobility, Smart Economy y Smart Environment. El propósito de este artículo es presentar una revisión sistemática de literatura sobre el concepto y las características de las Universidades inteligentes publicados en la literatura científica, a partir de los cuales se hace énfasis en el rol de IoT, como un elemento fundamental en la concepción e implementación de proyectos e iniciativas que inciden en el desarrollo exitoso de las Universidades.

**Palabras clave:** Internet de las cosas, Modelo, Ciudad inteligente, Universidad inteligente.

**Abstract:** It is contextualized from the Internet of Things and its vital importance for Smart Cities and the emerging concept of Smart University. The latter with their characteristics: Smart Governance, Smart People, Smart Living, Smart Mobility, Smart Economy and Smart Environment. The purpose of this paper is to present a systematic review of literature on the concept and characteristics of intelligent universities published in the scientific literature, from which the role of IoT is emphasized as a fundamental element in the conception and

Implementation of projects and initiatives that have an impact on the successful development of universities.

**Keywords:** Internet of Things, model, Smart City, Smart University.

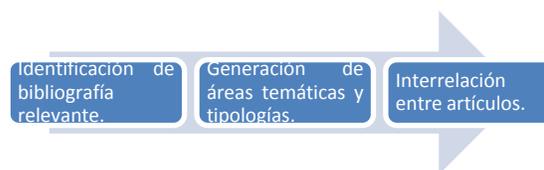
## 1. INTRODUCCIÓN

Internet de las cosas o IoT (Internet of Things), se refiere a la conexión de objetos tecnológicos o que sean electrónicos a Internet, este concepto se deriva del avance de la tecnología y a la necesidad de compartir y controlar las cosas que nos rodean (Li, Xu, & Zhao, 2015). Algunos de los campos en los que IoT se presenta fuertemente son: la adopción generalizada de redes basadas en el protocolo IP (Airehrour, Gutierrez, & Ray, 2016), la economía en la capacidad de cómputo, la miniaturización, los avances en el análisis de datos (Danieletto, Bui, & Zorzi, 2014) y el surgimiento de la computación en la nube, salud, herramientas de aprendizaje, seguridad (Flauzac, Gonzalez, & Nolot, 2015), optimización de procesos (Aziz, 2016), agricultura (Stoces, Vanek, Masner, & Pavlík, 2016), entre otros.

Partiendo de este concepto se realiza una búsqueda referenciada sobre Smart City y Smart University, siempre relacionado con IoT. De la literatura revisada se puede inferir una aproximación a como el concepto emergente de Smart University se subdivide en subsistemas que, como cualquier sistema, son identificables a través de la definición de sus Límites, Funciones, Comunicación y Estructura. (Tecnológico, Humanos, institucionales). También se proyecta la posibilidad de estudiar el comportamiento y las consecuencias de las múltiples interacciones de los elementos del sistema a través del tiempo. Desde el enfoque sistémico, el cual contempla la conexión entre los individuos y el contexto y desde la metodología de dinámica de sistemas, la cual favorece una visión integradora de los fenómenos y las relaciones de las partes, se

proyecta generar en primer lugar el modelo cualitativo, o causal, del sistema, donde se definen las influencias que se producen entre los elementos que integran el sistema; y en segundo lugar el modelo cuantitativo, donde se modifica la estructura del mismo y se analiza su comportamiento bajo distintas condiciones.

## 2. METODOLOGÍA



**Figura 1.** Proceso estructurado de revisión bibliográfica.  
Fuente: Elaboración propia.

La revisión documental se realizó en revistas de alto impacto publicados en las bases de datos SCOPUS, SCIENCE DIRECT, IEEE. Como criterios de búsqueda, se incluyeron los siguientes descriptores: “IoT”, “Smart campus”, “Smart cities”. Estos descriptores fueron combinados de diversas formas al momento de la exploración con el objetivo de ampliar los criterios de búsqueda (Hernández, Fernández, & Baptista, 2010) (ver figura 1).

### 2.1. Identificación de bibliografía relevante.

El inicio del proceso consistió en realizar un rastreo documental en bases de datos especializadas, se preseleccionaron artículos y al final se seleccionaron cincuenta referencias, de acuerdo con los criterios de inclusión y exclusión. “No se tomaron en consideración para el análisis aquellas fuentes primarias que no hacían alusión a los núcleos temáticos y/o

aquellos que no se encontraban en revistas indexadas” (Arevalo, Bayona, & Rico, 2015) (Sánchez, 2011). (ver figuras 2 y 3).

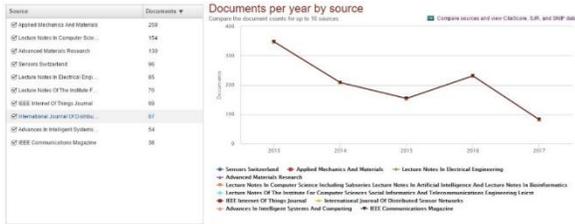


Figura 2. Documentos revista por año.  
 Fuente: SCOPUS

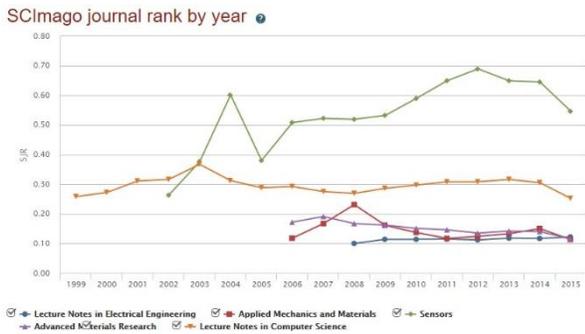


Figura 3. Documentos revista por año, índice SCImago.  
 Fuente: SCOPUS

## 2.2. Generación de áreas temáticas y tipologías.

Como acto seguido, se analiza cada documento, se establecen sus áreas temáticas y tipologías, como punto de entrada del proceso de revisión. Con la ayuda del software de administración de referencias Mendeley Desktop, se genera un documento elaborado en Word con los siguientes campos: título del artículo, autor, año, revista, información de la revista, problema de investigación, objetivos, tipo de investigación, método, descripción, instrumentos utilizados, resultados y núcleo temático. En este aparte, se pretendió identificar puntos de encuentro y diferencia de criterios entre los documentos clasificados que fundamentan la estructura de los ejes descritos para la presente búsqueda.

## 2.3. Interrelación entre artículos.

En este aparte, se pretendió identificar puntos de encuentro y diferencia de criterios entre los documentos clasificados que fundamentan la estructura de los ejes descritos para la presente búsqueda. (Sánchez, 2011)

## 3. DEFINICIÓN DE IOT

IoT posee una arquitectura macro de tres niveles o capas (Hurlburt, Voas, & Miller, 2012) como se presenta en la Figura 4. En el nivel básico despliega diferentes sensores, cada uno de ellos es una fuente de información, y diferentes tipos de sensores capturan diversos contenidos y formatos de información. El nivel intermedio integra varias redes cableadas e inalámbricas para transferir la información de las cosas con precisión. El nivel más superior es de la aplicación que consta de tres capas (capa de tecnología, capa de middleware, capa de aplicación) y se compone de aplicaciones que exportan toda la funcionalidad de los sistemas para el usuario final (Rodríguez, Montenegro, & Cueva, 2015).

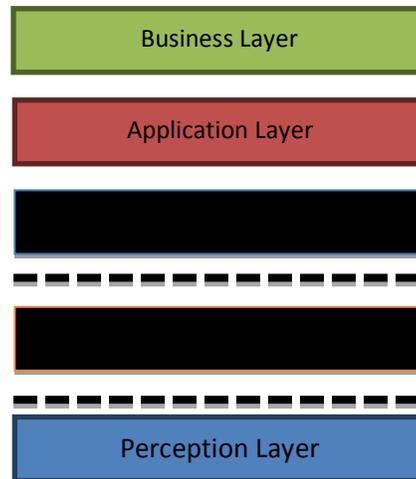


Figura 4. Internet of Things layers.  
 Fuente: Adaptado de (Naeem, Khan, & Shaikh, 2016)

Internet de las cosas es un tema emergente de importancia técnica, social y económica

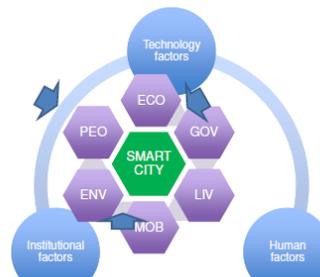
(Whitmore, Agarwal, & Xu, 2015). En este momento se están combinando productos de consumo, bienes duraderos, automóviles y camiones, componentes industriales y de servicios públicos, sensores y otros objetos de uso cotidiano con conectividad a Internet y potentes capacidades de análisis de datos que prometen transformar el modo en que trabajamos, vivimos y jugamos (Won-jun , 2016). Las proyecciones del impacto de la IoT sobre Internet y la economía son impresionantes: hay quienes anticipan que en el año 2025 habrá hasta cien mil millones de dispositivos conectados a la IoT y que su impacto será de US\$ 11.000.000.000.000 (Vongsingthong & Smachat, 2014).

Tener sensores u objetos dispersos que generar información desde cualquier lugar, requiere la interconexión de estos objetos heterogéneos a través de Internet (Jara , Moreno-Sanchez, Skarmeta, Varakliotis, & Kirstein, 2013). Cobran importancia los Smart Objects, objetos físicos con un sistema embebido que le permite procesar información y comunicarse con otros dispositivos y realizar acciones con base en una acción o evento determinado (Ghaleb, Subramaniam, & Zukarnain, 2016). No obstante, todos estos sistemas complejos presentan retos tales como: 1) la interoperabilidad y los estándares (Pathak, 2016) debido a las diferencias entre software y hardware utilizado por cada uno en los diferentes procesos; 2) el análisis avanzado de enormes cantidades de datos producidos por la red de sensores, que requieren de un tratamiento que permita su posterior análisis ( Danieletto , Bui , & Zorzi, 2014); 3) la seguridad entendido como los ataques a dispositivos conectados a Internet, el temor a la vigilancia y las preocupaciones relacionadas con la privacidad (Jin-ho & Seung-Ryul , 2016) y 4) aspectos relacionadas con las economías emergentes (Bleda , Jara, Maestre , Santa, & Gómez, 2012) (Byun, Kim, & Sa, 2016).

El IoT requiere reconocer los objetos inteligentes y mantener un flujo de mensajes constante entre los diferentes objetos (Jaehyeon , Mi-Seon, & Jae-Hyeon , 2016). Cada implementación de diferentes redes de sensores puede presentar diferentes problemas que son atendidos de manera diferente por cada aplicación (Naeem, Khan, & Shaikh, 2016). Un trabajo que se ha adelantado para mejorar la interconexión de objetos en IoT es realizar una arquitectura que soporte el paso de mensajes de los diferentes tipos de dispositivo y que sea capaz de responderles a través de nuevos protocolos como IPv6 (Jara , Moreno-Sanchez, Skarmeta, Varakliotis, & Kirstein, 2013) que puede administrar grandes cantidades de objetos que se conectarán a internet (Rathore, Ahmad, Paul, & Rho, 2016) (ver figura 5).

#### 4. DE SMART CITY A SMART UNIVERSITY

Partiendo de Smart cities, existen muchas definiciones de ciudades inteligentes. Algunos se centran en las TIC como tecnología (A. Gaur, Scotney, Parr, & McClean, 2015), mientras que las definiciones más amplias incluyen el desarrollo socioeconómico (Díaz-Díaz, Muñoz, & Pérez-González, 2017), la gobernanza (Sampri, Mavragani, & Tsagarakis, 2016), uso de la participación social para Sostenibilidad, calidad de vida y bienestar urbano (Rosati & Conti, 2016).



**Figura 5.** Relación entre componentes y características de ciudades inteligentes.

Fuente: (Catriona , Gavin , & Jonathan , 2014)

En cualquier caso, una Ciudad Inteligente es esencialmente habilitada por el uso de tecnologías para mejorar la competitividad y garantizar un futuro más sostenible en la vinculación simbiótica de redes de personas, empresas, tecnologías, Infraestructuras, consumo, energía y espacios (Catriona , Gavin , & Jonathan , 2014). Más concretamente, ver Figura 6, las estrategias e iniciativas de una Smart city deben incluir al menos una de las siguientes características:

- Smart Governance,
- Smart People,
- Smart Living,
- Smart Mobility,
- Smart Economy y
- Smart Environment.

Se puede asumir según Maestre (2015) que:

“Una ciudad inteligente es un territorio caracterizado por el uso intensivo de las tecnologías, principalmente de información y comunicación, para promover la

colaboración, la innovación y la eficiencia para lograr el mejoramiento de la calidad de vida de los ciudadanos y la sostenibilidad de las ciudades a través del mejoramiento de los servicios hacia los ciudadanos” (p.6) .

Ahora partiendo de este concepto de Smart City, trasladado a toda su comunidad y a su entorno, Maciá, Berná, Sánchez, Lozano, & Fuster (2017) generan como resultado el concepto de Smart Campus o Smart University, el cual mantiene el mismo objetivo principal de mejorar la calidad de vida de su comunidad aplicando de forma global, intensiva y sostenible las TI bajo el principio de servicio a la ciudadanía, ver figura 7. Es por eso que se trata de un entorno controlado, en el cual las políticas económicas, de sostenibilidad, construcción o desarrollo deciden en forma local y no dependen de factores externos, aunque siguen criterios similares a las políticas y estrategias nacionales o internacionales.



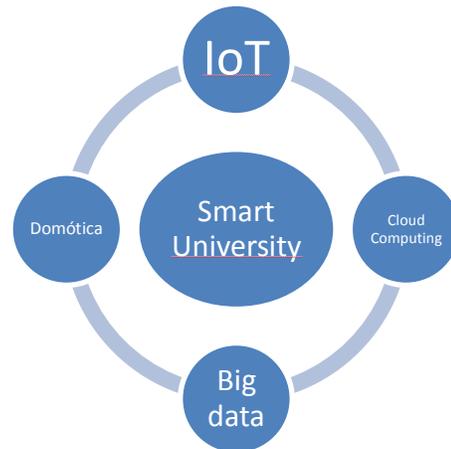
**Figura 6.** Pilares básicos en una comunidad inteligente.  
Fuente: Adaptado de (Maciá, Berná, Sánchez, Lozano, & Fuster, 2017)

Para lograr todo es necesario apoyarse en el poder de las TI que existen actualmente, ya que su correcto uso será el pilar fundamental para el éxito fundamental del proyecto. La infraestructura actual permite disponer de sistemas digitales conectados de manera global, capaces de soportar aplicaciones, servicios, plataformas y sensores, todos ellos funcionando en conjunto bajo un ecosistema o marco estandarizado de normas y protocolos capaces de actuar de manera integral y a su vez desacoplada, desempeñando un papel imprescindible en la generación correcta de conocimiento e interconexión.

Las principales ventajas de emplear TI son:

- Fácil acceso a los datos
- Adquisición de información
- Procesamiento rápido de la información
- Transmisión rápida
- Almacenamiento y análisis de la información
- Interactividad

El mundo ha cambiado, la tecnología ha cambiado el mundo. Tecnología y sociedad son ahora compañeros inseparables, se han fusionado para ofrecer un nuevo nivel de servicios. TI no es sólo hablar de computadores, dispositivos móviles, sensores, redes, es hablar de nuevos conceptos y paradigmas socio-tecnológicos, ver figura 8



**Figura 7.** Paradigmas Ti aplicados a Smart University.  
Fuente: Adaptado de (Maciá, Berná, Sánchez, Lozano, & Fuster, 2017)

El concepto de Smart University, al igual que el de Smart City, está fuertemente anclado al de la potencia de las TI, haciendo especial énfasis en el concepto del “internet de las cosas” (Internet of things) y de las actuales Smart Networks, las cuales interconectan sistemas y personas y, además, estimulan la innovación para facilitar un conjunto de objetivos en beneficio de todos.

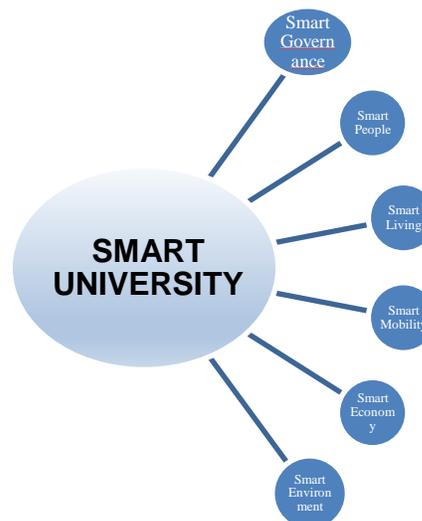
Tener sensores u objetos dispersos que generen información desde cualquier lugar, requiere la interconexión de estos objetos heterogéneos a través de Internet (Jara , Moreno-Sanchez, Skarmeta, Varakliotis, & Kirstein, 2013). Cobran importancia los Smart Objects, objetos físicos con un sistema embebido que le permite procesar información y comunicarse con otros dispositivos y realizar acciones con base en una acción o evento determinado (Ghaleb, Subramaniam, & Zukarnain, 2016). No obstante, todos estos sistemas complejos presentan retos tales como: 1) la interoperabilidad y los estándares (Pathak, 2016) debido a las diferencias entre software y hardware utilizado por cada uno

en los diferentes procesos; 2) el análisis avanzado de enormes cantidades de datos producidos por la red de sensores, que requieren de un tratamiento que permita su posterior análisis (Danieletto, Bui, & Zorzi, 2014); 3) la seguridad entendido como los ataques a dispositivos conectados a Internet, el temor a la vigilancia y las preocupaciones relacionadas con la privacidad (Jin-ho & Seung-Ryul, 2016) y 4) aspectos relacionadas con las economías emergentes (Bleda, Jara, Maestre, Santa, & Gómez, 2012) (Byun, Kim, & Sa, 2016).

El IoT requiere reconocer los objetos inteligentes y mantener un flujo de mensajes constante entre los diferentes objetos (Jaehyeon, Mi-Seon, & Jae-Hyeon, 2016). Cada implementación de diferentes redes de sensores puede presentar diferentes problemas que son atendidos de manera diferente por cada aplicación (Naeem, Khan, & Shaikh, 2016). Un trabajo que se ha adelantado para mejorar la interconexión de objetos en IoT es realizar una arquitectura que soporte el paso de mensajes de los diferentes tipos de dispositivo y que sea capaz de responderles a través de nuevos protocolos como IPv6 (Jara, Moreno-Sanchez, Skarmeta, Varakliotis, & Kirstein, 2013) que puede administrar grandes cantidades de objetos que se conectarán a internet (Rathore, Ahmad, Paul, & Rho, 2016) (ver figura 9).

Ahora para poder evaluar el grado de consecución de los objetivos Smart es necesario definir una serie de métricas e indicadores tanto cuantitativos como cualitativos que ayuden a comprender el funcionamiento en todos los ámbitos Smart en una Universidad. Es necesario para concretar un sistema de seguimiento que permita tomar decisiones en tiempo real y aportar conocimiento. Existen iniciativas globales y normas internacionales que

buscan la estandarización de indicadores, sobresale la norma ISO 37120:2014, donde se busca monitorizar y realizar un seguimiento del progreso del rendimiento y sostenibilidad de los servicios de una ciudad y de la calidad de vida, punto de inicio para ser aplicado a una comunidad como lo es una Universidad ver figura 6.



**Figura 8.** Indicadores de comunidades sostenibles ISO 37120:2014.

Fuente: Adaptado de (Maciá, Berná, Sánchez, Lozano, & Fuster, 2017)

Según el informe UNIVERSITIC realizado al Sistema Universitario Español (SUE)(ESPAÑOLAS, 2015), donde se lleva a cabo un inventario detallado de los elementos TI presentes en nuestros campus y se aborda un análisis de las buenas prácticas en la gestión de las TI, utilizando un catálogo de indicadores agrupados a dos niveles:

- Los Indicadores de descripción de las TI, que nos permiten obtener un inventario pormenorizado de las TI implantadas en nuestras universidades, desde 5 ejes diferentes: enseñanza- aprendizaje,

investigación, procesos de gestión, gestión de la información y formación y cultura TI.

Los Indicadores de gestión de las TI, que sirven para analizar cuáles son las buenas prácticas en gestión de las TI que en estos momentos están en explotación en las universidades, desde seis puntos de vista: recursos TI, proyectos TI, servicios TI, dirección de las TI, calidad, normativa y estándares TI y colaboración.

#### 4. CONCLUSIONES.

En lo referente al análisis de la bibliografía, este consiste en la búsqueda de artículos y documentos sobre los diferentes paradigmas implicados en la investigación y que se han especificado en los objetivos de la investigación, una tecnología emergente alrededor de dos conceptos IoT y Smart city. Se analizan conceptos desde ciudades inteligentes hasta campus o universidades inteligentes, así como a sus pilares (e-Gobierno y e-Gobernanza, Movilidad, Sostenibilidad Ambiental, Desarrollo Económico, Capital Intelectual y Calidad de Vida. (Catalina, 2010)

Como trabajo futuro se propone el proyecto que busca desarrollar una aproximación arquitectónica implementada para un Smart University que integre los elementos requeridos (Rosati & Conti, 2016), (ESPAÑOLAS, 2015), (Catalina, 2010)), generando un modelo (Hussein & Al-Hashimi, 2015) basado en el avance de la IoT en el sector educación y afines; contribuyendo en la toma de decisiones sobre problemáticas relacionadas con: la administración de recursos físicos y financieros, aplicación de controles para el consumo de recursos naturales, sistemas de seguridad y respuestas a emergencias, entre otros.

En lo referente al desarrollo del modelo, se estipula aplicar la metodología de dinámica de sistemas, sus componentes, sus fortalezas y sus aplicaciones. Sus fases son: Identificación del problema y análisis del comportamiento. Tomando la revisión y una vez conocidas las iniciativas prácticas más representativas dentro de aquellas que están siendo implementadas por las ciudades y replicadas en las universidades y de acuerdo con la naturaleza de las mismas, se identificaron y seleccionaron los factores a analizar, para cada uno de los seis ejes. (Catalina, 2010)

#### 5. BIBLIOGRAFÍA

- Abdulla, K., Jones, A., & Anthony, T. (2011). Guidelines for the digital forensic processing of smartphones. *Edith Cowan University - Research Online*.
- Agualimpia, C., & Rodrigo, H. (s.f.). *Universidad del Cauca*. Obtenido de [http://artemisa.unicauca.edu.co/~rherandez/articulos/Articulo\\_UPM-Criptored\\_Symbian\\_OS\\_Forensics\\_UJaveriana.pdf](http://artemisa.unicauca.edu.co/~rherandez/articulos/Articulo_UPM-Criptored_Symbian_OS_Forensics_UJaveriana.pdf)
- Aguilar, K. J. (2013). Principios jurídicos aplicables para la valoración de evidencia electrónica en el campo del despido laboral. *H-TICs, I(1)*, 1(1).
- Álvarez, A., Marín, O., & Victoria, J. (2012). Framework para la computación forense en Colombia. *Ing. USBMed, 3(2)*.
- Álvarez, M. D., & Guamán, V. A. (Febrero de 2008). *Universidad Politécnica Salesiana*. Obtenido de <http://dspace.ups.edu.ec/handle/123456789/546>
- Arias Chaves, M. (2006). Panorama general de la informática forense y de los

- delitos informáticos en Costa Rica. *InterSedes: Revista de las sedes regionales*, VII(12), 141-154.
- Arquillo, J. (Septiembre de 2007). *Universidad de Jaén*. Obtenido de <http://www.portantier.com/biblioteca/seguridad/analisis-forense.pdf>
- Ayers, R., Jansen, W., Cilleros, N., & Daniellou, R. (2005). *Cell Phone Forensic Tools: An Overview and Analysis*. Gaithersburg, MD: National Institute of Standards and Technology.
- Berintato, S. (8 de Junio de 2007). *The Rise of Anti-Forensic*. (CSO) Obtenido de <http://www.csoonline.com/article/2122329/investigations-forensics/the-rise-of-anti-forensics.html>
- Botero, A. C. (2009). *Criptored*. Obtenido de [http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia3-Sesion6\(3\).pdf](http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia3-Sesion6(3).pdf)
- Brezinski, D., & Killalea, T. (Febrero de 2002). Guidelines for Evidence Collection and Archiving. Network Working Group. Obtenido de <http://www.rfc-editor.org/rfc/rfc3227.txt>
- Broucek, V., & Turner, P. (2006). Winning the battles, losing the war? Rethinking methodology for forensic computing research. *Journal in Computer Virology*, 3-12.
- Calzada Pradas, R. (2004). Análisis forense de sistemas. *II Foro de Seguridad RedIRIS*.
- Cano, J. (2006). Introducción a la informática forense. *Sistemas*, 64-73.
- Cano, J. (9 de Septiembre de 2007). *alfa-redi*. (Derecho y Nuevas Tecnologías) Obtenido de <http://www.alfa-redi.org/node/8946>
- Cano, J. (2009). *Computación forense - Descubriendo los rastros informáticos*. Almaomega.
- Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd ed.). Academic Press.
- Catalina, I. M. S. (2010). Modelo de Dinámica de Sistemas para la implantación de Tecnologías de la Información en la Gestión Estratégica Universitaria, 55-84.
- Cifuentes, J. (2010). *Trabajos de grado Ingeniería de Sistemas*. (Pontificia Universidad Javeriana) Obtenido de <http://pegasus.javeriana.edu.co/~CIS0930SD01/files/AntiForenseZFS.pdf>
- Congreso de la República de Colombia. (18 de Agosto de 1999). *Archivo General de la Nación Colombia*. Obtenido de [http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY\\_527\\_DE\\_1999.pdf](http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_527_DE_1999.pdf)
- Congreso de la República de Colombia. (5 de Enero de 2009). *En TIC confío*. Obtenido de [http://www.enticonfio.gov.co/images/stories/normatividad/Ley\\_1273\\_de\\_2009%20.pdf](http://www.enticonfio.gov.co/images/stories/normatividad/Ley_1273_de_2009%20.pdf)
- Congreso de la República de Colombia. (5 de Enero de 2009). *Ministerio de las TIC*. Obtenido de [http://www.mintic.gov.co/portal/604/articles-3705\\_documento.pdf](http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf)
- Congreso de la República de Colombia. (22 de Noviembre de 2012). *Archivo General de la Nación Colombia*. Obtenido de [http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/DECRETO\\_2364\\_DE\\_2012.pdf](http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/DECRETO_2364_DE_2012.pdf)
- Curran, K., Robinson, A., Peacocke, S., & Cassidy, S. (2010). Mobile Phone Forensic Analysis. *International Journal of Digital Crime and Forensics*, 2(2).
- De León, F. J. (Diciembre de 2009). *Instituto Polotécnico Nacional*.

- Obtenido de [http://tesis.bnct.ipn.mx:8080/jspui/bitstream/123456789/7879/1/2386\\_tesis\\_Diciembre\\_2010\\_933405487.pdf](http://tesis.bnct.ipn.mx:8080/jspui/bitstream/123456789/7879/1/2386_tesis_Diciembre_2010_933405487.pdf)
- Catalina, I. M. S. (2010). Modelo de Dinámica de Sistemas para la implantación de Tecnologías de la Información en la Gestión Estratégica Universitaria, 55–84.
- Díaz-Díaz, R., Muñoz, L., & Pérez-González, D. (2017). Business model analysis of public services operating in the smart city ecosystem: The case of SmartSantander. *Future Generation Computer Systems*.  
<https://doi.org/10.1016/j.future.2017.01.032>
- ESPAÑOLAS, C. U. (2015). *Analisis de las TIC en las Universidades Españolas. Universitic 2015*.  
<https://doi.org/10.1017/CBO9781107415324.004>
- Gaur, A., Scotney, B., Parr, G., & McClean, S. (2015). Smart city architecture and its applications based on IoT. In *Procedia Computer Science* (Vol. 52).  
<https://doi.org/10.1016/j.procs.2015.05.122>
- Gaur, A., Scotney, B., Parr, G., & McClean, S. (2015). Smart City Architecture and its Applications Based on IoT. *Procedia Computer Science*, 52, 1089–1094.  
<https://doi.org/10.1016/j.procs.2015.05.122>
- Rosati, U., & Conti, S. (2016). What is a Smart City Project? An Urban Model or A Corporate Business Plan? *Procedia - Social and Behavioral Sciences*, 223, 968–973.  
<https://doi.org/10.1016/j.sbspro.2016.05.332>
- Sampri, A., Mavragani, A., & Tsagarakis, K. P. (2016). Evaluating Google Trends as a Tool for Integrating the “Smart Health” Concept in the Smart Cities’ Governance in USA. *Procedia Engineering*, 162, 585–592.  
<https://doi.org/10.1016/j.proeng.2016.11.104>
- Eset . (2012). *Guía de seguridad para usuarios de smartphone*.
- ESPAÑOLAS, C. U. (2015). *Analisis de las TIC en las Universidades Españolas. Universitic 2015*.  
<https://doi.org/10.1017/CBO9781107415324.004>
- Fiscalia General de la Nación. (22 de Diciembre de 2004). *Alcaldía de Bogotá*. Obtenido de <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=15634>
- Garfinkel, S. (2007). *Cite Seer X*. (The Pennsylvania State University) Obtenido de <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.109.5063&rep=rep1&type=pdf>
- Gaur, A., Scotney, B., Parr, G., & McClean, S. (2015). Smart City Architecture and its Applications Based on IoT. *Procedia Computer Science*, 52, 1089–1094.  
<https://doi.org/10.1016/j.procs.2015.05.122>
- Ghosh, A. (2004). *Guidelines for the Management of IT Evidence*. Hong Kong, China: APEC Telecommunications and Information Working Group.
- Goel, A. T. (2012). Smartphone Forensic Investigation Process Model. *International Journal of Computer Science & Security*, VI(5), 322-341.
- Google Inc. . (2015). *Android.com*. Obtenido de <http://www.android.com/Guidelines on Mobile Device Forensics>.
- (2014). National Institute of Standards and Technology.
- HEADWAY Digital. (2015). *Tendencias del consumo en móviles Colombia*.

- IAB Spain. (2014). *VI Estudio Anual Mobile Marketing*.
- IDC Analyse the Future. (2015). *Smartphone OS Market Share, 2015 Q2*. Framingham, MA: IDC. Obtenido de <http://www.idc.com/prodserv/smartphone-os-market-share.jsp>
- Jahankhani, H., Anastasios, B., & Revett, K. (2007). Digital Anti Forensics: Tools and Approaches. *The 6th European Conference on Information Warfare and Security*. Shrivenham, UK.
- Jakobsson, M., & Ramzan, Z. (2008). *Crimeware. Understanding New attacks and Defenses* (First ed.). Addison-Wesley Professional.
- Jaramillo, G. E. (2011). Técnicas de análisis forense digital aplicadas a dispositivos y sistemas móviles. *Apuntes de Ciencia & Sociedad*, 167-171.
- Kaspersky Lab. (2013). *Kaspersky Lab Latinoamérica*. (Octubre) Obtenido de <http://latam.kaspersky.com/mx/sobre-kaspersky/centro-de-prensa/comunicados-de-prensa/m%C3%A1s-de-la-mitad-de-usuarios-de-android-no-pro>
- Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response*. Gaithersburg, MD: National Institute of Standards and Technology - NIST.
- León, A., Echeverría, T., & Santander, M. (s.f.). Guía metodológica para la investigación forense en el navegador web Google Chrome. *Kosmos - Universidad Pontificia Bolivariana*, 246-255.
- Maggi, F., Zanero, S., & Iozzo, V. (2008). Seeing the invisible: Forensic Uses of Anomaly Detection and Machine Learning. *Newsletter*, 42, 51-58.
- MinTIC & Ipsos Napoleón Franco. (2013). *Ministerio TIC*. Obtenido de <http://www.mintic.gov.co/portal/604/w3-article-6048.html>
- Pagès López, J. (2013). Temas Avanzados en Seguridad y Sociedad de la Información. *IX Ciclo de conferencias UPM - TASSI*. Madrid, España.
- Rifà, H., Serra, J., & Rivas, J. (2009). *Análisis forense de sistemas informáticos*. Barcelona: Universitat Oberta de Catalunya.
- Rodríguez, F., & Doménech, A. (2011). La informática forense: el rastro digital del crimen. *Quadernos de Criminología. Revista de Criminología y Ciencias Forenses*(14), 14-21.
- Rosati, U., & Conti, S. (2016). What is a Smart City Project? An Urban Model or A Corporate Business Plan? *Procedia - Social and Behavioral Sciences*, 223, 968–973. <https://doi.org/10.1016/j.sbspro.2016.05.332>
- Samprí, A., Mavragani, A., & Tsagarakis, K. P. (2016). Evaluating Google Trends as a Tool for Integrating the “Smart Health” Concept in the Smart Cities’ Governance in USA. *Procedia Engineering*, 162, 585–592. <https://doi.org/10.1016/j.proeng.2016.11.104>
- Santes, L. (Marzo de 2009). *Instituto Politécnico Nacional - México*. Obtenido de <http://tesis.ipn.mx:8080/dspace/bitstream/123456789/3730/1/PROPUESTAMETODFORENSE.pdf>
- Santos, L. M., & Flórez, A. S. (2012). Metodología para el análisis forense en Linux. *Revista Colombiana de Tecnologías de Avanzada*, 2(20), 90-96.

- Symantec Corp. (23 de Agosto de 2011). *Symantec*. Obtenido de [http://www.symantec.com/es/mx/about/news/release/article.jsp?prid=20110823\\_01](http://www.symantec.com/es/mx/about/news/release/article.jsp?prid=20110823_01)
- Torres, D. A. (17 de Noviembre de 2006). *Asociación Colombiana de Ingeniería de Sistemas - ACIS*. Obtenido de <http://www.acis.org.co/index.php?id=856>
- Torres, D. R. (s.f.). *PennState. Department of Computer Science and Engineering*. Obtenido de <http://www.cse.psu.edu/~ruedarod/papers/recsi04.pdf>
- Vidas, T., Zhang, C., & Christin, N. (2011). Toward a general collection methodology for Android devices. *Digital Investigation*, S14-S24.
- Wang, Y., Cannady, J., & Rosenbluth, J. (2005). Foundations of computer forensics: A technology for the fight against computer crime. *Computer Law & Security Review*, 21, 119-127.
- Zuccardi, G., & Gutiérrez, J. D. (Noviembre de 2006). *Trabajos de grado de Ingeniería de Sistemas. Pontificia Universidad Javeriana*. Obtenido de <http://pegasus.javeriana.edu.co/~digital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf>