

Integración e implementación de redes convergentes para el soporte de IoT en Smart Cities

Integration and implementation of converged networks for IoT support in smart cities.

Sebastián Palacios Tovar¹
Sebastian.palacios00@usc.edu.co

Fernando Vélez Varela, M.sC²
Fernando.velez00@usc.edu.co

Universidad Santiago de Cali, Facultad de Ingeniería, Programa de ingeniería electrónica (1, 2)

Resumen

Este artículo es la consecución conceptual en IoT, Machine learning e inteligencia artificial, que fundamenta la actual integración e implementación de redes convergentes para el soporte de las actuales tecnologías, soportadas en elementos de hardware y software aplicados en los modelos de Smart Cities (ciudades inteligentes). Estas buscan determinar márgenes de sostenibilidad mediante procesos de mejoras en lo relacionado con infraestructura, innovación y tecnología, para disminuir el consumo energético y emisiones de CO₂. Para esto se tiene concebido usar el modelo Digital Network Architecture® (DNA®) de redes convergentes para el soporte de las referencias de IoT en Smart cities y, a su vez, establecer cual proceso de integración de redes es más eficiente para utilizarse en algunos parámetros de estas mismas. La llegada de las nuevas tecnologías como 5G y el crecimiento de la Internet de las Cosas (IoT), ha forzado a los operadores de telecomunicaciones a converger en una única red para maximizar el uso de sus recursos. Las redes convergentes están en constante desarrollo, debido a que cada vez hay mayores exigencias de conectividad y transmisión de datos.

Palabras Clave: Ciudades inteligentes; Redes convergentes; IoT.

Abstract

This article is the conceptual achievement in IoT, Machine learning and artificial intelligence, which bases the current integration and implementation of convergent networks for the support of current technologies, supported by hardware and software elements applied in Smart Cities models. These seek to determine sustainability margins through improvement processes related to infrastructure, innovation and technology, to reduce energy consumption and CO₂ emissions. For this, it is intended to use the Digital Network Architecture® (DNA®) model of converged networks to support IoT references in Smart cities and, in turn, establish which network integration process is more efficient for use in some parameters of these. The arrival of new technologies such as 5G and the growth of the Internet of Things (IoT) have forced telecommunications operators to converge into a single network to maximize the use of their resources. Convergent networks are constantly developing, because there are increasing demands for connectivity and data transmission.

Keywords: Smart City; converging networks; IoT

1. INTRODUCCIÓN

En los últimos años inicio una fuerte tendencia global en convertir la mayor cantidad de ciudades en ciudades inteligentes. Se puede considerar que una ciudad inteligente, consiste en “la utilización de infraestructuras en red para mejorar la eficiencia económica y política y permitir el desarrollo sociocultural y urbano” (Hollands, 2015). Existen dos enfoques generales para hablar de ciudades inteligentes: el método impulsado por la tecnología (TDM¹) y el método impulsado por el ser humano (HDM²). El primero, define que las tecnologías de la información y comunicación (TIC) son el pilar fundamental para tener un modelo de ciudad inteligente, que buscan brindar el soporte para mejorar el desempeño socioeconómico, ecológico, logístico y competitivo de las ciudades, pero para esto es necesario implementar e integrar redes de telecomunicaciones inteligentes, que sean escalables a futuro y brinden seguridad a todos sus dispositivos de red (Kummitha & Crutzen, 2017). Como última instancia, Las ciudades inteligentes se esfuerzan por

¹ TDM: Technology Driven Method

² HDM: Human Driven Method

aumentar la competitividad de las comunidades locales mediante innovación y al mismo tiempo mejorar la calidad de vida de sus ciudadanos mediante mejores servicios públicos y privados, y con un medio ambiente más limpio (Appio, Lima, & Paroutis, 2019).

Para cumplir con los anteriores propósitos, las ciudades inteligentes están soportadas en las tecnologías de información y comunicación de vanguardia, que disponen de una infraestructura física determinada por ejemplo con redes de fibra óptica, sensores y dispositivos conectados, y en la parte lógica con el análisis de datos abiertos, Internet de las cosas (IoT), lo que determina los marcos de planificación participativa habilitados para las TIC. (Sutanta, Aditya, & Astrini, 2016). Por otro lado (Albino, Berardi, & Dangelico, 2015), dentro de esta especificación tecnológica todo lo connotado como Smart City determina que todo se basa en un pilar fundamental que es el capital humano (universidades de investigación, empresas intensivas en conocimiento e instituciones públicas), lo cual tiene como propósito el desarrollo humanístico y social a través de la educación, la cultura, la inclusión social, la innovación social (Holm & Travis, 2017).

Bill Hutchison (Bedford, Hutchison, & Bedford, 2011), diseñó un marco piramidal de 5 niveles denominado "Arquitectura inteligente de comunidad abierta". Dentro de este, los dos niveles inferiores se enfocan en las estrategias de lugares e infraestructura. Los tres niveles superiores son ecosistemas de colaboración, aplicaciones y vida. Las ciudades inteligentes no se define por el hecho simplemente de conectar el hardware y la infraestructura, sino crear entornos colaborativos donde la innovación y la calidad de vida puedan prosperar (De Maio, Fenza, Loia, & Orciuoli, 2017). Mientras tanto, según (*Smart cities: Ranking of European medium-sized cities*, s. f.) Define las características de ciudades inteligentes en torno a seis dimensiones primordiales: calidad de vida (Smart Living), competitividad económica (Smart Economy), capital social y humano (Smart People) servicios públicos y sociales y participación ciudadana (Smart Governance), infraestructura de transporte y comunicación (Smart Mobility) y recursos naturales (Smart Environment). En la figura 1 se puede apreciar las dos definiciones anteriores.

Figura 1. Infraestructura física de ciudad inteligente según el marco de Hutchison y sus dimensiones



Fuente: Adaptado de (Appio et al., 2019)

En el mundo de hoy la digitalización incide en todo, convirtiendo la sociedad en “seres digitales”. Al vivir en la era de la información, y que la mayoría de esta misma era dada en forma de “átomos” (periódicos, revistas, libros, etc.) y no en bit (unidad básica de información digital), se considera que se pasó de una época de átomos a una época digital, y de la producción masiva a la época de la información, en consecuencia, de la época de los ordenadores a la época post-

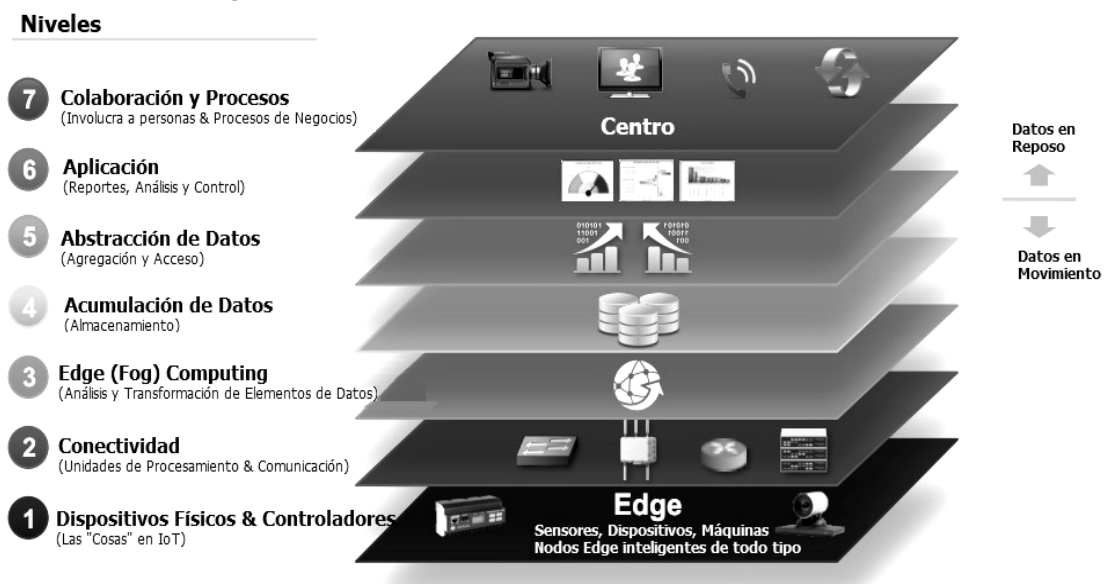
informativa, donde todo es hecho a la medida y la información está supremamente personalizada (Vélez, Marín, & Castillo, 2019).

Esta creciente digitalización en las prácticas de la vida da como resultado procesos que “se hacen a distancia”, que los soportan los objetos inteligentes de Internet de las cosas (IoT), dentro de lo que podría ser una Smart City, donde dichos objetos son controlados a través de Internet. Esto hace que exista telepresencia y conceptos como la telemetría, la cual conglomerada tres principios tecnológicos que son la robótica, la telecomunicación y la realidad virtual. De este modo, un usuario puede realizar actividades dentro de un entorno virtual por telecomunicación mediante un robot u objetos inteligentes dirigidos a distancia, y de retorno recibir respuestas de la misma experiencia sensorial del suceso a distancia (Vélez et al., 2019).

Las nuevas aplicaciones de IoT están permitiendo el crecimiento de Smart City en todo el mundo. IoT es la capacidad de monitorear, administrar y controlar dispositivos de forma remota, y de controlar y brindar información procesable mediante el flujo de datos en tiempo real (Kim, Ramos, & Mohammed, 2017). Básicamente las IoT es una base para conectar cosas, sensores, actuadores y otras tecnologías inteligentes, para establecer unas comunicaciones de persona a objeto y/o de objeto a objeto. («Internet de las Cosas», 2017). Lo cerrado relación con IoT, se fundamenta en la instalación de sensores (RFID, IR, GPS, escáneres láser, etc.) para todo, para posteriormente conectarlos a Internet a través de protocolos específicos para el intercambio de información y comunicaciones, con el propósito de tener un reconocimiento inteligente, ubicación, seguimiento y gestión de cada dispositivo conectado a internet («IoT», s. f.). Con el soporte de IoT, las ciudades inteligentes deben tener tres características: ser instrumentadas, interconectadas e inteligentes. Solo así se puede formar una Smart City integrando todas estas características inteligentes en su etapa avanzada de desarrollo de IoT (Liu, 2018).

En IoT se sigue una arquitectura por capas como se aprecia en la figura 2. La arquitectura tiene que cumplir ciertos requerimientos para que esta tecnología sea viable. Debe permitir que la tecnología sea distribuida, donde los objetos puedan interactuar entre ellos, escalable, flexible, robusta, eficiente y segura. Esta arquitectura incluye los aspectos físicos y los aspectos virtuales (como los servicios y los protocolos de comunicación), además de al menos tener la capacidad de gestionar dispositivos y sus datos, la conectividad y comunicación, y la analítica y aplicaciones («Simplifique el desarrollo de sus- soluciones de IoT con arquitecturas de IoT», 2017).

Figura 2. Modelo de Referencia de Internet de las Cosas



Fuente: Tomado de (Vélez et al., 2019)

Para soportar la gran cantidad de flujo de datos es vital contar con redes eficientes que tengan la capacidad e inteligencia para esto. Las Smart Cities requieren infraestructuras de red con mayor capacidad de ancho de banda para conectar dispositivos y aplicaciones de IoT (Camero & Alba, 2019). Según con *Smart Cities Week*, las redes de comunicaciones proporcionan las conexiones esenciales entre los dispositivos IoT y las aplicaciones que procesan y actúan según la información recopilada, la conectividad de banda ancha es requisito indispensable para la existencia de una ciudad inteligente («Smart Cities Week San Diego, CA, 2019—Global Platform for Cities», s. f.).

Las redes cableadas (ya sea de fibra o cobre) son el soporte de conectividad para conectar edificios y "dispositivos periféricos" tales como cámaras de vigilancia, puntos de acceso WiFi, small cells y sistemas de antena distribuida (DAS³); al mismo tiempo, la red inalámbrica debe cumplir con protocolos inalámbricos, los cuales pueden incluir Wi-Fi, LTE, 5G, Bluetooth, Zigbee, entre otros («No existirán ciudades inteligentes sin redes eficientes—Noticias—Infraestructuras—Redes & Telecom», s. f.).

La empresa Cisco Systems Systems, dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones en los años recientes está trabajando en el proyecto “Digital Network Architecture (DNA)” para ciudades y comunidades, industrias, gobernanza, etc. La red DNA es una red intuitiva de autoaprendizaje, con bajo consumo energético y de grandes capacidades para el manejo y transporte de datos. Es por eso que en este artículo se ha decidido tomar esta arquitectura de red como referencia y, al mismo tiempo, como esta se podría integrar en las presentes y/o futuras ciudades inteligentes.

En la siguiente sección se habla de las redes convergentes. Luego se detalla la “Digital Network Architecture” y la integración de software y hardware de esta misma en ciudades. Posteriormente se darán conclusiones del tema y por ultimo las referencias bibliográficas que se tomaron como base para este artículo.

2. CONVERGENCIA DE REDES

Las redes convergentes o redes de multiservicio hacen referencia a la integración de los servicios de voz, datos y video sobre una sola red. Esto permite que dispositivos distintos como los Smartphone, sensores, ordenadores, tabletas o electrodomésticos requieran una única infraestructura de red, como se puede ver en la figura 3.

Las redes deben admitir una amplia variedad de aplicaciones y servicios, como así también funcionar con diferentes tipos de infraestructuras físicas. El término arquitectura de red, en este contexto, se refiere a las tecnologías que admiten la infraestructura y a los servicios y protocolos programados que pueden trasladar los mensajes en toda esa infraestructura.

Una red de convergencia se construye sobre tres elementos claves:

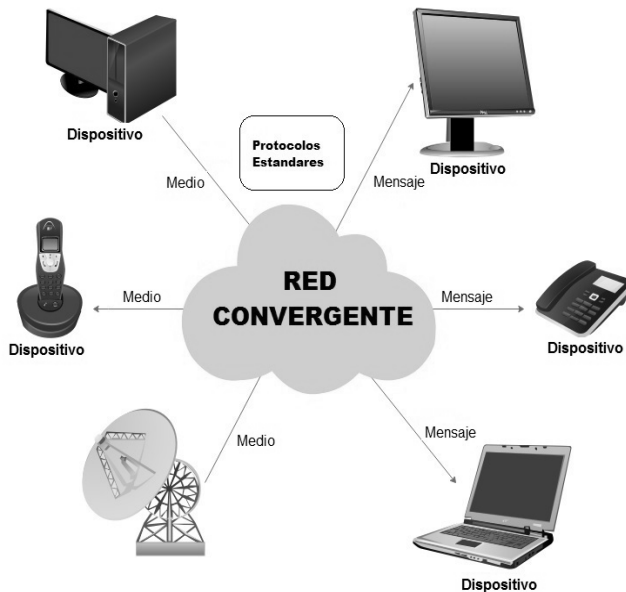
- Tecnologías que permitan ofrecer múltiples servicios sobre una red de datos.
- Una red multipropósito, construida sobre una arquitectura de red funcionalmente distribuida.
- Un sistema abierto de protocolos estándares e internacionalmente aceptado.

La convergencia de las redes IP está basada en estándares IETF⁴, lo que hace posible unificar la planificación, la gestión y la ingeniería de las capas de red óptica y capas de la red IP, con la consiguiente mejora de la eficiencia y ahorro de costes («El futuro de la conectividad está en la convergencia de redes—Noticias—Tendencias—Redes & Telecom», s. f.).

³ DAS: Distributed Antenne System

⁴ IETF: Internet Engineering Task Force, es un grupo que desarrolla y promueve estándares de Internet.

Figura 3. Red convergente



Fuente: Propia

Al evolucionar las redes se mejoran sus funciones. Las redes de comunicación convergentes ofrecerán mucho más que conectividad básica y acceso a las aplicaciones. La convergencia de los diferentes tipos de redes de comunicación en una plataforma representa la primera fase en la creación de la red inteligente de información. En el presente se está en una fase de evolución e implementación de la red en Smart Cities. El paso a seguir es consolidar no sólo los diferentes tipos de mensajes en una única red, sino también consolidar las aplicaciones que generan, transmiten y aseguran los mensajes en los dispositivos de red integrados. No sólo la voz, datos y videos se logran transmitir mediante estas redes, sino que los dispositivos que realizan la conmutación de teléfonos y el broadcast de videos serán los mismos dispositivos que enrutan los mensajes en la red. La plataforma de comunicaciones resultante proporcionará funcionalidad de aplicaciones de alta calidad a un costo reducido (Heo & Lee, 2019).

3. ARQUITECTURA DE RED DIGITAL DE CISCO SYSTEMS (DNA)

La DNA o también conocida como la red intuitiva de Cisco Systems, es una red convergente basada en la intención como se observa en la figura 4, que mediante sus innovadores componentes propician que los recursos de red aprendan, se adapten y evolucionen de manera automática. La DNA trata cada dispositivo de red (cableado o inalámbrico) como parte de una misma estructura de red unificada⁵, gestionando los miles de dispositivos conectados y eliminando la configuración manual. Cisco Systems ha incorporado tecnologías de machine learning, inteligencia artificial y un potente hardware abierto y programable, que garantiza cuestiones básicas como satisfacer la demanda de red y prevenir o evitar ciberataques (Cisco Systems, 2019).

Cisco Systems está logrando satisfacer las necesidades de extremo a extremo, y es que Cisco Systems DNA logra obtener el máximo provecho de los datos que circulan por las redes a nivel global. Y lo obtiene gracias a la capacidad de generar conocimiento predictivo útil y aplicable. Mediante la red intuitiva DNA, Cisco Systems está brindando tanto hardware como software avanzados, haciéndolos funcionar conjuntamente y permitiendo que los administradores de red

⁵ Estructura Unificada: Es la flexibilidad arquitectónica y conectividad de red uniforme entre los entornos físicos, virtuales y de nube.

y equipos de TI puedan centralizar y simplificar el manejo de todo el sistema de red. Con DNA Center en su núcleo, se proporciona la política, la automatización y el análisis necesarios para adaptarse al cambio, simplificar y escalar las operaciones, y proteger contra la degradación y las amenazas («Arquitectura de red digital de Cisco», 2017).

Figura 4. Red basada en intenciones.



Fuente: Adaptado de (Robb Boyd, 15:13:28 UTC)

Cisco Systems está aumentando el componente central (DNA Center) para admitir dispositivos IoT. DNA Center es un software de automatización de redes. Una parte clave es el Software Defined Access (Cisco Systems SD Access), que utiliza un enfoque centrado en la identidad para administrar a los usuarios y dispositivos que ingresan y operan dentro de la red.

Esta red se está empleando mucho en la industria, por lo que Cisco Systems está ampliando el SD-Access para empresas extendidas, como en centros de distribución, almacenes y plantas de fabricación donde los dispositivos, sensores y robots de IoT son comunes. La ampliación de SD-Access significa que se puede impulsar la política y automatizar las operaciones en la empresa, fabricación o entornos al aire libre, todo a través de DNA Center («Acceso definido por software», s. f.).

Las redes basadas en intención representan un cambio fundamental en la forma en que las redes se construyen y administran, al sustituir los métodos tradicionales con el que normalmente se administran las redes, que usualmente son manuales y que tardan mucho tiempo hacerlas. Estas redes modernas capturan la intención y la convierten en una política de red. Al llevar la red basada en la intención a entornos de IoT, las ciudades y/o comunidades tendrían la capacidad de escalar de manera automatizada y la flexible para conectar su infraestructura heredada y futura, como con 5G, y lo conectan todo de manera segura con protección integrada («Cisco Systems conecta de forma segura entornos complicados y ubicaciones remotas en el límite del IoT - Unipymes—Diplomados Virtuales Cursos Empresariales», s. f.).

Con la red intuitiva de Cisco Systems se emplea Machine Learning para analizar grandes cantidades de datos de red, desde telemetría hasta patrones de tráfico, y comprende anomalías y configuraciones óptimas de red. En última instancia, es una red basada en la intención, autodirigida y autocurativa. La red redirigirá el tráfico por sí misma y se curará de las perturbaciones internas, como el mal funcionamiento del dispositivo y las perturbaciones externas, como los ataques cibernéticos. DNA Center al ser una aplicación de administración centralizada. Incluye software Machine Learning que observa la configuración, la telemetría y los patrones de tráfico de las implementaciones de WAN y recomienda la

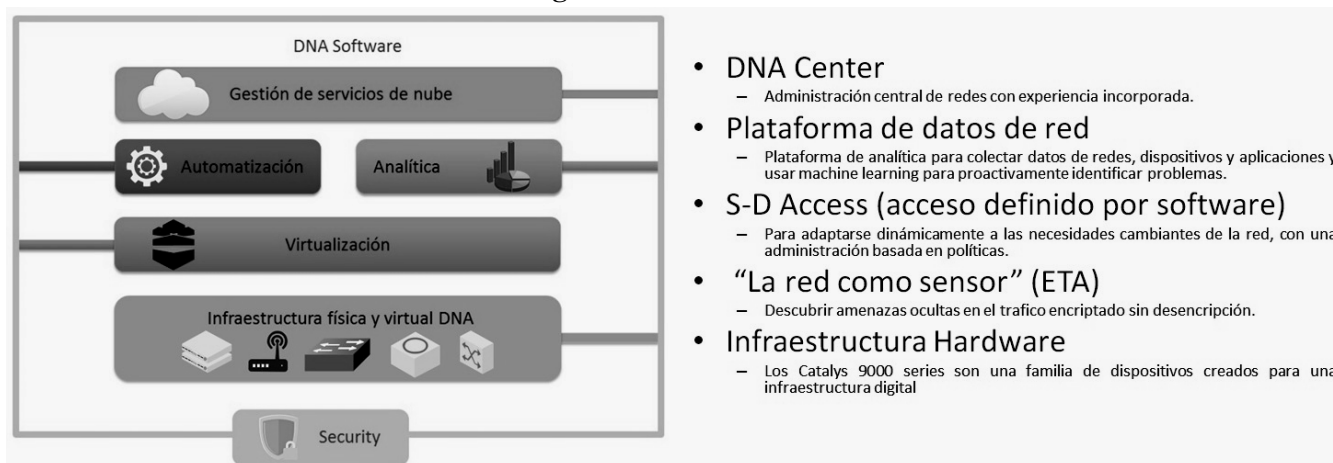
optimización y las medidas de seguridad basadas en ellos (*Transforming Businesses with Artificial Intelligence*, 2018).

3.1 Implementación e integración de redes DNA

Las ciudades actuales cada vez son más innovadoras y dinámicas al adoptar tecnologías para la movilidad, IoT, planificación urbana, seguridad pública, medio ambiente, administración y gobierno, además de, análisis de datos y nubes. Por eso se necesita contar con una red escalable, que cuente con buena velocidad y protección contra amenazas. La DNA brinda una red integral basada en la intención WAN con soluciones robustas de cableado, inalámbrica y enrutamiento. Con su enfoque entregado por software como se observa en la figura 5, tiene control y visibilidad en toda la red.

Además se puede crear y aplicar políticas en toda la red con unos pocos clics. También puede aislar y solucionar rápidamente problemas actuales y pasados. Además una de las cosas por desarrollar es implementar nuevas aplicaciones en su entorno de varias nubes sin comprometer la seguridad o el rendimiento. Con la infraestructura preparada para DNA de Cisco Systems, se tiene una base de conmutación, conexión inalámbrica y enrutamiento de última generación que permite una innovación continua.

Figura 5. DNA Software



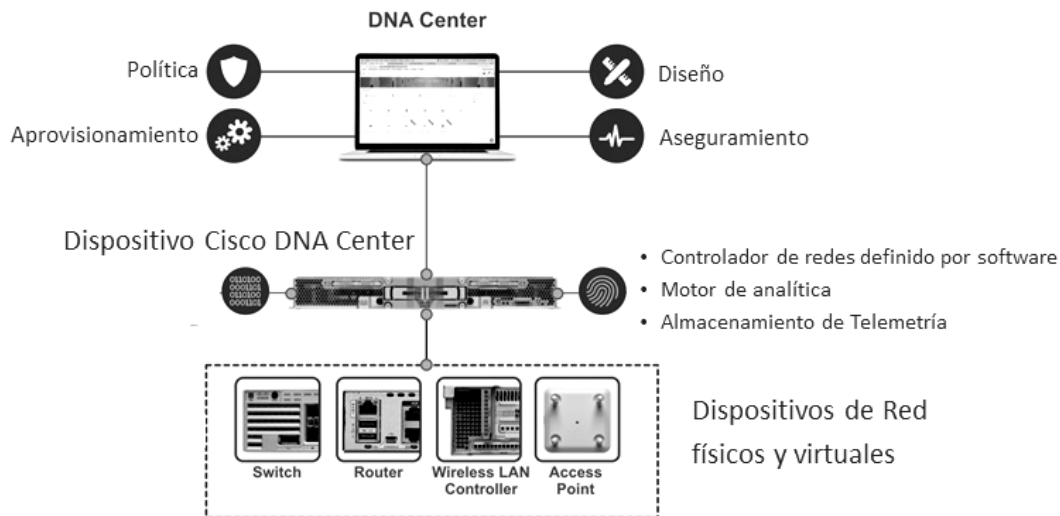
Fuente: Adaptado de (Cisco Systems)

La DNA Analytics and Assurance es una plataforma analítica capaz de resolver los problemas antes de que ocurran. De esta capacidad viene precisamente la característica de “intuitiva” de esta red. Se analizan todos los datos que pasan por la red y se los categoriza para que posteriormente se puedan utilizar para analíticas predictivas mediante machine learning. Mientras que el Encrypted Traffic Analytics (ETA) permite analizar el tráfico cifrado sin comprometer la privacidad. Se basa en Cisco Talos⁶ y usa herramientas de machine learning para analizar los datos en busca de cualquier tipo de amenaza o ataque, incluso cuando estos se encuentran encriptados (ARYSE Comunicaciones, 2018).

Estas redes deben estar preparadas para soportar la conexión de numerosos dispositivos de Internet de las Cosas de manera segura (muchos dispositivos tienen un software y un sistema operativo vulnerables a los ciberataques) y eficiente. Y, al mismo tiempo, es necesario emplear analíticas que ayuden a sostener la disponibilidad de los servicios y la seguridad de las conexiones. La red debe tener cierto nivel de inteligencia analítica que les permita reaccionar proactivamente a los eventuales problemas o incluso anticiparse a ellos (Alonso, 2018). Su infraestructura de red programable envía datos al dispositivo de Cisco DNA Center. El dispositivo activa las funciones y capacidades de los dispositivos de red con el software Cisco DNA como se puede visualizar en la figura 6. Todo se maneja desde el panel de Cisco DNA Center.

⁶ Cisco Talos: Es un grupo de investigación e inteligencia de ciberseguridad, Formada por 250 investigadores de seguridad y más de 600 ingenieros de software, Talos detecta, analiza y protege el software frente a amenazas.

Figura 6. Estructura Cisco DNA



Fuente: Adaptado de (Cisco Systems)

3.2 Wireless

Para la implementación de wireless inteligentes en ciudades y lograr la integración con la DNA, es necesario implementar tecnologías capaces de tener un análisis de tráfico cifrado, donde se identifique las comunicaciones de malware en el tráfico cifrado, la extracción de elementos de datos y el aprendizaje automático. También debe contar con una segmentación donde se reduzcan los gastos de operación y riesgos mientras se crea una infraestructura rápida con políticas y servicios consistentes en toda la red. Y por último debe garantizar la detección de puntos de acceso no autorizados, la localización de las amenazas de seguridad y minimizar las interferencias de RF.

3.2.1. Puntos de acceso inalámbricos para DNA

Los puntos de acceso deberán manejar los desafíos de la red de la próxima generación. Más allá del estándar Wi-Fi, los puntos de deben ser resistentes e inteligentes y proporcionar seguridad integrada para sus clientes móviles y sus dispositivos IoT. Cisco Systems para soportar lo dicho hasta ahora, tiene para ofrecer un producto como lo es el Catalyst 9100, el cual se considera como un punto de acceso más compatible con esta red, ya que más allá de ofrecer Wi-Fi 6 (802.11ax), el cual proporciona soporte multilingüe y alojamiento de aplicaciones de protocolos de IoT como Wi-Fi, BLE y Zigbee, Además, los dispositivos IoT (así como los dispositivos de usuario) pueden tener hasta tres veces menos consumo de energía y una mayor seguridad. El Catalyst 9100 puede alcanzar velocidades de hasta 10 Gbps y más de 100 dispositivos pueden conectarse con aplicaciones sensibles a la latencia, como voz sobre IP y videoconferencia. Esto es hasta tres veces más en comparación con los estándares anteriores («The Future is Now! Presenting the Cisco Catalyst 9100 Wi-Fi 6 Access Points», 2019).

3.2.2 Controladores inalámbricos

Los controladores inalámbricos inteligentes para DNA deben tener una alta disponibilidad y contar con actualizaciones de software integradas, que ayudan a mantener la red en funcionamiento. Deben ser seguros y proteger todos los dispositivos, usuarios e infraestructura de red, y que proporcione análisis mejorados o que se implemente en la infraestructura (incluida la nube) que se desee. Cisco Systems recomienda el controlador Catalyst 9800-80, que admite hasta 6000 puntos de acceso y 64.000 clientes. Admite un rendimiento de hasta 80 Gbps y ocupa un espacio de rack de 2RU y brinda protección de la inversión con una variedad de opciones de enlace ascendente modulares opcionales: GE, 10GE, 40GE y 100GE («Cisco Catalyst 9800 Wireless Controller Series Deployment Guide», s. f.)

3.3 Switching

Los switch inteligentes deben de reducir los ataques de seguridad con segmentación basada en políticas en todo el tejido de la red, implementar un cifrado de alto rendimiento para reducir las amenazas de intermediarios y reducir los ataques ocultos dentro del tráfico cifrado directamente en el switch. Debe permitir la actualización de código en dispositivos individuales y la reparación de problemas de hardware sin desconectar la red. Para soportar lo dicho anteriormente Cisco Systems sugiere el Switch Catalyst 9400, el cual tiene una función llamada “circuito integrado de aplicación específica del plano de datos de acceso unificado” (ASIC UADP) para la convergencia cableada e inalámbrica. Esta característica permite el acceso convergente por cable e inalámbrico para la simplicidad y escala operativa. Estos Switch de acceso modular están diseñados para la seguridad, IoT y la nube. Tienen alta disponibilidad de vanguardia, admiten hasta 9 Tbps, permite la automatización del aprovisionamiento, la segmentación y la gestión de políticas de la red para admitir IoT sin interrupción, al tiempo que limita la ubicación de los dispositivos IoT en la red. y forman uno de los componentes básicos de SD-Access («Cisco Catalyst 9400 Series Switches», s. f.).

3.4 Routing

Un Router inteligente en una ciudad debe ser de alto rendimiento y de bajo coste, su diseño debe soportar los datos de sensores, medidores y otros dispositivos en Smart Cities y para su posterior envío hacia la nube. En cuanto a seguridad debe identificar aplicaciones y bloquearlas según sea necesario. Debe evitar que todo tipo de usuarios accedan a malware, botnets, phishing y ataques en línea dirigidos mediante el acceso directo a Internet. Los Routers Cisco Systems DNA combinan dos características únicas que aceleran el tiempo que lleva desplegar una sucursal: TI y SD-WAN. TI puede automatizar el aprovisionamiento de varias sucursales con una programación y personalización mínima. La WAN definida por software (SD-WAN) ofrece una experiencia de usuario segura y consistente en cualquier conexión, independientemente de la conectividad subyacente. Estas capacidades simplificaran y racionalizaran sus operaciones de WAN, reduciendo costos, ahorrando tiempo y reduciendo el riesgo.

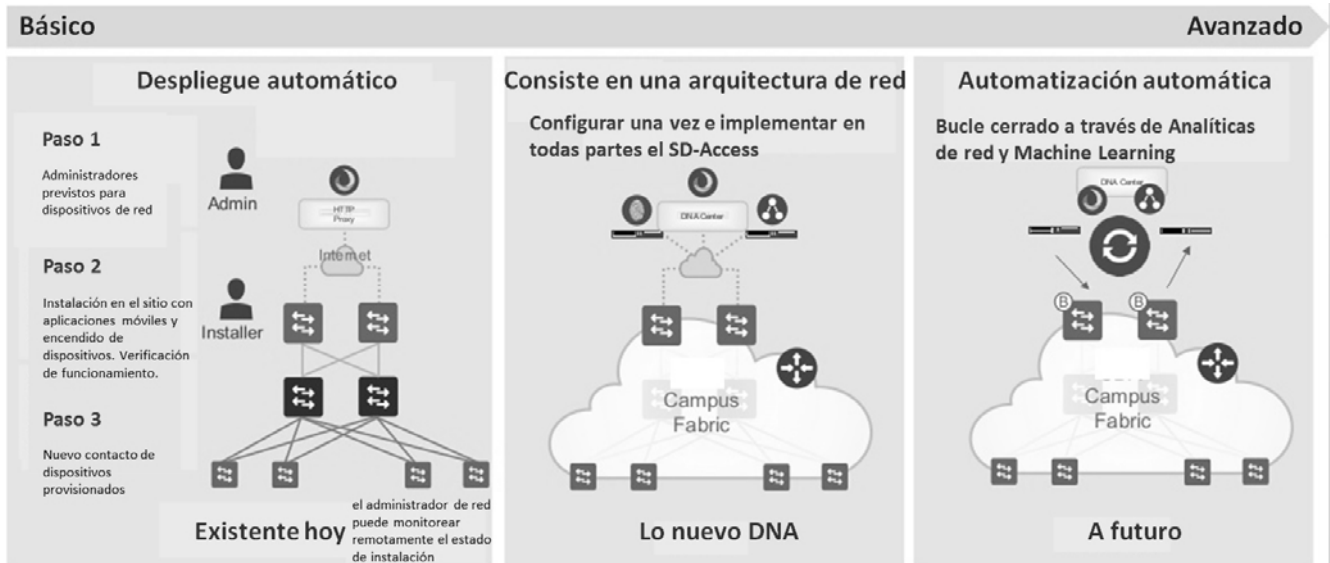
Los enrutadores deben brindar acceso a Internet, seguridad avanzada y servicios inalámbricos en un solo dispositivo. Para cumplir con dichas necesidades, Cisco Systems sugiere los enrutadores de servicios integrados (ISR) 1000, que son enrutadores fijos de alto rendimiento, fáciles de implementar y administrar. Son muy potentes y proporcionan conectividad de banda ancha, metro Ethernet y LAN inalámbrica altamente seguras. Tienen mayor movilidad y opciones de conectividad SD-WAN y LAN de próxima generación. Dan acceso a Ethernet, DSL, y opciones de conectividad más rápidas, como LTE Advanced y 802.11ac Wi-Fi. Al utilizar unas redes basadas en intenciones permite la administración y operación de la red WAN desde un centro de control, proporcionando acceso a Internet directo y altamente seguro («Cisco 1000 Series Integrated Services Routers (ISR)», s. f.).

Según el informe *Cisco VNI* («VNI Global Fixed and Mobile Internet Traffic Forecasts», s. f.), para 2021 el tráfico IP se habrá multiplicado por 3, alcanzando los 3 Zettabytes, habrá 27.100 millones de dispositivos conectados (siendo el 51% conexiones IoT) y 4.600 millones de internautas a escala global. En países europeos, el tráfico IP se multiplicará por tres entre 2016 y 2021, habrá hasta 7 dispositivos conectados por habitante en 2021 y las conexiones IoT representarán el 65% (Borja, 2017). Es por eso una ciudad inteligente como Copenhague, ha decidido proliferar el acceso Wi-Fi en busca de una digitalización de la ciudad con la arquitectura de red digital de Cisco Systems. Conecta personas, datos, dispositivos, procesos e incluso servicios de la ciudad de forma inalámbrica (*Copenhagen Drives City Carbon Footprint Reductions and Enriches Citizen Experiences through Converged Digital Solutions.pdf*, 2019).

Para la implementación de la DNA en ciudades colombianas, es necesario reemplazar los dispositivos de red actuales con los dispositivos compatibles con la DNA, sin embargo, se puede conservar los medios de transmisión guiados, ya que esta arquitectura es compatible con todos estos, lo que permite el ahorro de costos. Posteriormente se integran con el dispositivo DNA Center, permitiendo pasar de funciones básicas de red a más avanzadas como se observa en la figura 7.

Durante la transición de cambio de arquitectura de red, también es posible armar un núcleo de la red con las nuevas funcionalidades, manteniendo a los equipos legados en la red por fuera de núcleo, como funciona en la actualidad.

Figura 7. Red intuitiva, de lo básico a lo avanzado



Fuente: Adaptado de (Cisco Systems, 2019)

En cuanto al funcionamiento de la arquitectura, la capa de transporte es muy básica, SD-Access se basa en algunas opciones de conmutación, inalámbricas y controladores que se han desarrollado en la actualidad, que cuentan con toneladas de potencia y compatibilidad con ETA (Análisis de tráfico cifrado). Estos dispositivos realizan todo el transporte y la implementación de la política en el fondo de SD-Access y mueven los bits alrededor de la red. La red subyacente transportará el tráfico de un lugar a otro, conformando el Campus Fabric⁷ como se observa en la figura 8. La verdadera red virtual llega a los puntos finales a través de la encapsulación, ya no solo a través de las VLAN.

El Protocolo de separación de ID de localizador (LISP – *Locator ID Separation Protocol*) toma la IP y la ubicación y las separa para que la IP y la ubicación ya no estén atadas. LISP es como DNS⁸ para paquetes, cuando un conmutador necesita reenviar paquetes de un lugar a otro, LISP identifica las ubicaciones de los dispositivos de red y las rutas requeridas usando un servidor de mapas. LISP permite que un dispositivo esté en cualquier lugar de la red. Entrar y salir del entorno LISP es a través de un enrutador de túnel. Esto garantiza la movilidad de los dispositivos alrededor de la red, incluso si un dispositivo se traslada a otra ubicación geográfica la dirección IP de ese dispositivo no cambia, simplemente se mueve de un lugar a otro y el sistema de mapas maneja dónde está ese dispositivo.

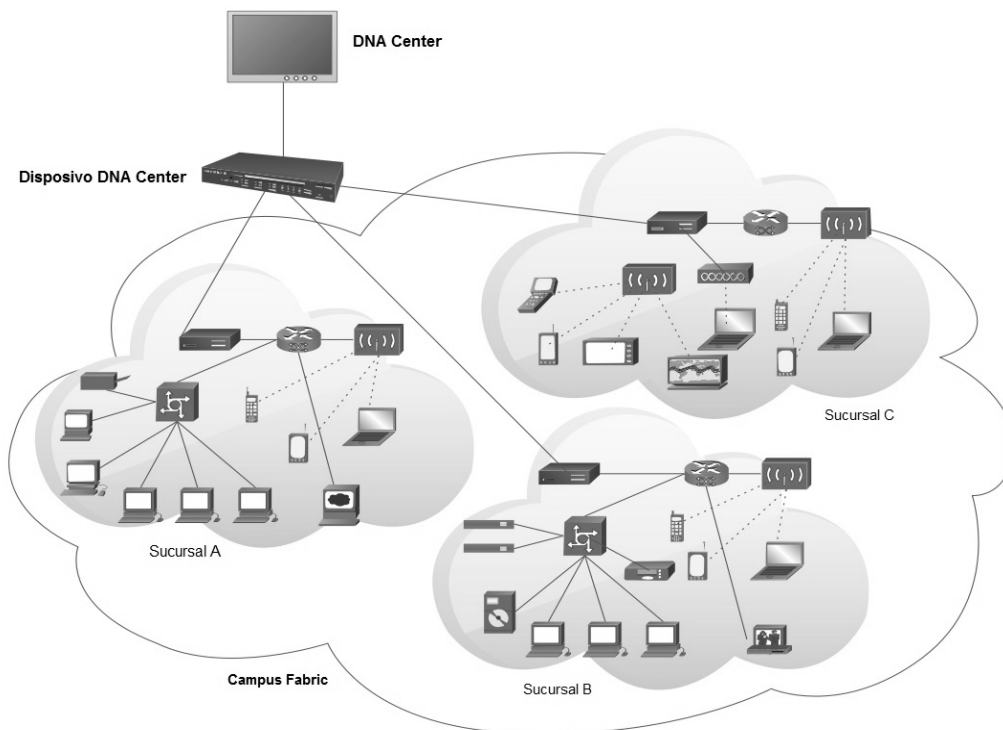
El protocolo VXLAN⁹ proporciona el transporte del tráfico en la capa de acceso a través del Campus Fabric. Se crea el contexto mediante ISE (Identity Services Engine) que sirve para crear identidad de red para objetos, usuarios y sistemas. una vez que se implementa ISE, todos los dispositivos de red comienzan a ver que las actividades son del usuario, los cortafuegos muestran los nombres de los usuarios y no los sistemas, se puede comenzar a implementar políticas contra grupos de objetos y la autenticación de la red se vuelve más fácil. La red inalámbrica se vuelve más fácil de administrar desde una perspectiva de seguridad.

⁷ Campus Fabric: Es la infraestructura básica para desarrollar redes virtuales basadas en construcciones de segmentación basadas en políticas.

⁸ DNS: Domain Name System

⁹ VXLAN: Es un protocolo de superposición de redes ideado para transportar tráfico de capa de enlace de datos sobre la capa de red.

Figura 8: Campus Fabric – Cisco DNA



Fuente: Propia

DNA Center es la interfaz de usuario para la red, allí es donde los grupos contextuales de ISE, como usuarios y servidores, se encontrarán con la política que se desea crear. Todos los componentes de SD-Access se encuentran en el DNA Center y luego se envían al resto de la red. DNA Center hará todo el trabajo de automatización de la red. Esta interfaz permite desde tratar con ISE hasta programar los dispositivos de red. Se establece la intención que se desea, y la DNA Center lo convertirá en acción en su capa de hardware.

4. CONCLUSIONES

Las ciudades inteligentes necesitan una infraestructura de telecomunicaciones que sea estable, segura, fiable e interoperable para dar soporte al enorme volumen de aplicaciones y servicios basados en TIC que existe en la actualidad. El concepto de IoT permite que miles de millones de dispositivos e instrumentos con sensores inteligentes utilizados en telemetría se conecten entre sí, adquieran datos en tiempo real, y envíen esta información a los sistemas de control centralizados. Las ciudades inteligentes y el IoT están creando una nueva era en la vida urbana, mejorando la seguridad, la habitabilidad y la comodidad de los ciudadanos, y a su vez, desarrollando una base para las empresas de alta tecnología y permitiendo servicios y administraciones de ciudades más eficientes e inteligentes. Para lograr la máxima funcionalidad de IoT, se necesita la implementación de ciertos sistemas operativos y protocolos de comunicación para permitir interacciones entre usuarios y dispositivos. En el futuro, habrá muchas aplicaciones de IoT para ciudades inteligentes, como el control inteligente de la red. Un sistema IoT debería poder conectar muchos dispositivos diferentes al mismo tiempo a través de Internet, lo que explica la necesidad de una arquitectura digital.

El mundo cada vez hay más conectividad entre dispositivos y, seguramente, en el futuro habrá muchos más. De acuerdo con el informe de *Redes Visuales de Cisco – Visual Networking Index (VNI)*, predice que serán 28,5 mil millones de dispositivos y conexiones de red en el mundo en 2022. Las empresas operadoras de telecomunicaciones deben tener la capacidad de soportar la gran cantidad de flujo de datos, generada por el desarrollo de tecnologías como nube,

inteligencia artificial, machine learning y big data. Si no se realizan mejoras en las redes actuales, las empresas están expuestas a sufrir operaciones lentas y propensas a fallos. Además, las redes están más expuestas, ya que el riesgo de ataques cibernéticos es mayor. Ese coctel de tecnologías ocasiona una fuerte demanda por conectividad, generando el nacimiento de una infraestructura: la red basada en la intención. En los últimos años, hubo una infinidad de cambios y conceptos, como híbrido, software-defined network, virtualización de las funciones de red o Software-Defined WAN, haciendo que de a poco la conectividad ya no sea tan dependiente del hardware.

La Red Intuitiva, es una red más sencilla de operar que las redes convergentes tradicionales. Se estima que el 95% de los cambios en la red aún se realizan manualmente. Esto deduce que con las redes tradicionales las empresas operadoras gastan hasta tres veces más recursos en operar la red que en la propia red. Con la Red Intuitiva, las organizaciones pueden afrontar todos los retos que le presenta la nueva era de la información.

Al contar con tecnologías de inteligencia artificial y Machine Learning, se obtiene redes aún más inteligentes y más seguras sin importar los tamaños y tipos de complejidad que tenga la red. Mientras se incrementa el uso de la telemetría, las estadísticas operativas e indicadores de amenazas de seguridad, más valor obtendrá la utilización de Cisco DNA Center por su capacidad intuitiva y generación de políticas de red. Los beneficios para las empresas al adoptar soluciones de red intuitiva son variados y se centran en una mayor comprensión de cómo se comporta la red. De esta manera es posible que las empresas tengan un mayor control de las necesidades y de las demandas de servicios, brindando la mejora continua y la adaptación que éstas necesitan.

DNA Center permite ver la red como un todo y agilizar el trabajo al momento de implementar nuevos dispositivos, establecer políticas o cambios de configuración. Ahora se puede administrar una amplia gama de dispositivos y procesos de red mediante un panel centralizado y simplificado. En cuanto a hardware, los dispositivos de red compatibles con la DNA tienen un control total diseñado para la seguridad, la movilidad, IoT y la nube. En el mundo actual, necesita una red que sea abierta, escalable y programable, de forma que pueda adaptarse e innovar con rapidez.

Al implementar e integrar una red intuitiva-convergente como DNA de Cisco Systems, se logra desde un único lugar (DNA Center) diseñar, definir y aprovisionar las políticas y gestionar la seguridad y comprobar que los dispositivos de red y la infraestructura de red cableada e inalámbrica, están funcionando correctamente. La red se vuelve más flexible y el tiempo de respuestas disminuye porque esta se adapta a las necesidades, programando y reprogramando sus modelos.

Hacer que la red sea intuitiva es un paso fundamental, y es de hecho la primera fase en lograr que la red sea inteligente, la fase siguiente será no solo consolidar los distintos tipos de mensajes que transitan la red sino los dispositivos que generan, transmiten y aseguran los mensajes en los dispositivos de red integrados. Eso quiere decir que los encargados de enrutar los mensajes serán los mismos dispositivos.

Al ritmo que avanza la tecnología se espera que haya un mundo donde cada objeto que se tenga a disposición va pertenecer a una red que permita generar, transmitir y recibir mensajes. Con una aproximación de 20.000 millones de elementos conectados en todo el mundo -de un total de 1.5 billones, hay mucho por conectar a través de Internet, dando paso no solo a admitir cambios sino a crecer, siempre buscando adaptarse a los requisitos de seguridad y de servicio de calidad.

REFERENCIAS

- Acceso definido por software. (s. f.). Recuperado 9 de septiembre de 2019, de Cisco website: https://www.cisco.com/c/es_mx/solutions/enterprise-networks/software-defined-access/index.html
- Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart Cities: Definitions, Dimensions, Performance, and Initiatives. *Journal of Urban Technology*, 22(1), 3-21. <https://doi.org/10.1080/10630732.2014.942092>
- Alonso, A. (2018, enero 15). ¿Qué es la Red Intuitiva de Cisco y por qué es importante para sus clientes empresariales? Recuperado 16 de septiembre de 2019, de ITSitio website: <https://www.itsitio.com/us/la-red-intuitiva-cisco-importante-clientes-empresariales/>
- Appio, F. P., Lima, M., & Paroutis, S. (2019). Understanding Smart Cities: Innovation ecosystems, technological advancements, and societal challenges. *Technological Forecasting and Social Change*, 142, 1-14. <https://doi.org/10.1016/j.techfore.2018.12.018>
- Arquitectura de red digital de Cisco: La Red Intuitiva. (2017, octubre 31). Recuperado 27 de agosto de 2019, de Datacom.Global website: <https://datacom.global/arquitectura-de-red-digital-cisco-red-intuitiva/>
- ARYSE Comunicaciones. (2018, julio 16). Red Intuitiva. Recuperado 17 de septiembre de 2019, de ARYSE COMUNICACIONES website: <https://www.aryse.net/red-intuitiva-que-es-la-nueva-red-digital-de-cisco/>
- Bedford, N., Hutchison, W., & Bedford, S. (2011). Ukraine's global strategy in the post-crisis economy: Developing an intelligent nation to achieve a competitive advantage. *Innovative Marketing*, 7(1), 8.
- Borja, M. (2017). ¿Qué es la red intuitiva? Recuperado 16 de septiembre de 2019, de <https://gblogs.cisco.com/es/2017/06/que-es-la-red-intuitiva/>
- Camero, A., & Alba, E. (2019). Smart City and information technology: A review. *Cities*, 93, 84-94. <https://doi.org/10.1016/j.cities.2019.04.014>
- Cisco 1000 Series Integrated Services Routers (ISR). (s. f.). Recuperado 4 de septiembre de 2019, de Cisco website: <https://www.cisco.com/c/en/us/products/routers/1000-series-integrated-services-routers-isr/index.html>
- Cisco Catalyst 9400 Series Switches. (s. f.). Recuperado 2 de septiembre de 2019, de Cisco website: <https://www.cisco.com/c/en/us/products/switches/catalyst-9400-series-switches/index.html>
- Cisco Catalyst 9800 Wireless Controller Series Deployment Guide. (s. f.). Recuperado 2 de septiembre de 2019,

- de Cisco website: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_cisco_catalyst_9800_wireless_controller_series_dg.html
- Cisco Systems. (2019). Cisco DNA para ciudades, comunidades e industrias. Recuperado 27 de agosto de 2019, de Cisco website: https://www.cisco.com/c/es_mx/solutions/industries/smart-connected-communities/dna-software.html
 - Cisco Systems. (s. f.). Cisco DNA Center—Network Management Automation. Recuperado 18 de septiembre de 2019, de Cisco website: <https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html>
 - *Copenhagen Drives City Carbon Footprint Reductions and Enriches Citizen Experiences through Converged Digital Solutions.pdf*. (s. f.).
 - De Maio, C., Fenza, G., Loia, V., & Orciuoli, F. (2017). Distributed online Temporal Fuzzy Concept Analysis for stream processing in smart cities. *Journal of Parallel and Distributed Computing*, 110, 31-41. <https://doi.org/10.1016/j.jpdc.2017.02.002>
 - El futuro de la conectividad está en la convergencia de redes—Noticias—Tendencias—Redes & Telecom. (s. f.). Recuperado 26 de agosto de 2019, de <https://www.redestelecom.es/tendencias/noticias/1099534003003/futuro-de-conectividad-convergencia-de-redes.1.html>
 - Hollands, R. G. (2015). Critical interventions into the corporate smart city. *Cambridge Journal of Regions, Economy and Society*, 8(1), 61-77. <https://doi.org/10.1093/cjres/rsu011>
 - Holm, P., & Travis, C. (2017). The New Human Condition and Climate Change: Humanities and Social Science Perceptions of Threat. *Global and Planetary Change*, 156, 112-114. <https://doi.org/10.1016/j.gloplacha.2017.08.013>
 - Internet de las Cosas: Nuevas políticas y sistemas de autodestrucción. (2017, abril 10). Recuperado 19 de agosto de 2019, de Pandora FMS - The Monitoring Blog website: <https://pandorafms.com/blog/es/internet-de-las-cosas/>
 - IoT: Origen, importancia en el presente y perspectiva de futuro. (s. f.). Recuperado 19 de agosto de 2019, de <http://www.itop.es/blog/item/iot-origen-importancia-en-el-presente-y-perspectiva-de-futuro.html>
 - Kim, T., Ramos, C., & Mohammed, S. (2017). Smart City and IoT. *Future Generation Computer Systems*, 76, 159-162.

<https://doi.org/10.1016/j.future.2017.03.034>

- Kummitha, R. K. R., & Crutzen, N. (2017). How do we understand smart cities? An evolutionary perspective. *Cities*, 67, 43-52. <https://doi.org/10.1016/j.cities.2017.04.010>
- Liu, L. (2018). IoT and A Sustainable City. *Energy Procedia*, 153, 342-346. <https://doi.org/10.1016/j.egypro.2018.10.080>
- No existirán ciudades inteligentes sin redes eficientes—Noticias—Infraestructuras—Redes & Telecom. (s. f.). Recuperado 19 de agosto de 2019, de <https://www.redestelecom.es/infraestructuras/noticias/1107908001803/no-existiran-ciudades-inteligentes-redes-eficientes.1.html>
- Robb Boyd. (15:13:28 UTC). *TechWiseTV Workshop: Cisco DNA Center Assurance*. Technology. Recuperado de <https://www.slideshare.net/robboyd/techwisetv-workshop-cisco-dna-center-assurance>
- Simplifique el desarrollo de sus soluciones de IoT con arquitecturas de IoT: Estrategias para crear soluciones de IoT escalables, flexibles y robustas. (2017, octubre 4). Recuperado 16 de septiembre de 2019, de <http://www.ibm.com/developerworks/ssa/library/iot-lp201-iot-architectures/index.html>
- Smart Cities Week San Diego, CA, 2019—Global Platform for Cities. (s. f.). Recuperado 19 de agosto de 2019, de Smart Cities Week San Diego, CA, 2019 website: <https://sandiego2019.smartcitiesweek.com/>
- Sutanta, H., Aditya, T., & Astrini, R. (2016). Smart City and Geospatial Information Availability, Current Status in Indonesian Cities. *Procedia - Social and Behavioral Sciences*, 227, 265-269. <https://doi.org/10.1016/j.sbspro.2016.06.070>
- The Future is Now! Presenting the Cisco Catalyst 9100 Wi-Fi 6 Access Points. (2019, mayo 1). Recuperado 2 de septiembre de 2019, de [blogs@Cisco—Cisco Blogs website: https://blogs.cisco.com/wireless/the-future-is-now-presenting-the-cisco-catalyst-9100-wi-fi-6-access-points](https://blogs.cisco.com/wireless/the-future-is-now-presenting-the-cisco-catalyst-9100-wi-fi-6-access-points)
- *Transforming Businesses with Artificial Intelligence*. (s. f.).
- Vélez, F., Marín, D., & Castillo, F. (2019). *Línea de investigación de Sistemas de Información y Automatización*. 77.
- VNI Global Fixed and Mobile Internet Traffic Forecasts. (s. f.). Recuperado 16 de septiembre de 2019, de Cisco website: <https://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html>