

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIONES

TESIS:

EL INTERNET DE LAS COSAS Y LAS CONSIDERACIONES DE SEGURIDAD

AUTOR:

CUZME RODRÍGUEZ FABIÁN GEOVANNY

Trabajo previo a la obtención del título de:

MAGISTER EN REDES DE COMUNICACIONES

Quito, Abril 2015

RESUMEN

La presente investigación se centra en el estudio de las consideraciones de seguridad en el Internet de las Cosas. Se analizan las debilidades y amenazas que tiene esta innovación tecnológica. Los costos de referencia asociados a adoptar seguridad a los objetos y desarrollo de esquemas a considerar para agregar seguridad a un objeto o en un entorno IoT.

Se investigó el marco general que abarca el Internet de las Cosas, la situación en que los objetos se vuelven cada vez más inteligentes, las capas básicas que están involucradas, el impacto que se impone en los negocios y en la sociedad y los factores determinantes en el futuro de esta tecnología.

Los mecanismos de seguridad que se plantean en este trabajo, parten de un análisis de información determinante en cuestiones de seguridad en diferentes niveles como hardware, software, red y nube, en donde cada uno forma un papel muy importante para los objetos o dispositivos conectados en un entorno IoT. Acompañado de un análisis de costos de referencia que incurren para adoptar seguridad en un objeto o entorno IoT, aquí se muestra claramente que debe existir un equilibrio entre los riesgos, costos de seguridad y costo del recurso o dispositivo a asegurar.

Luego de un exhaustivo análisis de los componentes, se presentan los esquemas para diseñar objetos con niveles de seguridad aceptables tanto para los entornos IoT, como para los dispositivos u objetos en sí.

Como parte final de nuestra investigación presentamos las conclusiones y recomendaciones, en las cuales exponemos los resultados obtenidos de toda la investigación, y recomendaciones para futuros estudios o implementaciones de esta tecnología prometedora.

Palabras Claves

Internet de las Cosas, IoT, Seguridad, Esquemas.

ABSTRACT

This research focuses on the study of the safety considerations in the Internet of Things. Weaknesses and threats that this technological innovation are analyzed. The reference costs associated with adopting security objects and schema development to consider to add security to an object or an IoT environment.

The general framework encompassing the Internet of Things investigated the situation in which objects become increasingly intelligent, basic layers that are involved, the impact is imposed on business and society and determinants in the future of this technology.

The security mechanisms that arise in this paper are based on an analysis of decisive information on security issues at different levels such as hardware, software, networking and cloud, where each forms a very important role for objects or devices connected one IoT environment. Accompanied by an analysis of reference costs incurred to adopt security IoT an object or environment, here clearly shows that there must be a balance between risks, security costs and cost of the resource or device to insure.

After a thorough analysis of the components, the schemes are presented for designing objects with acceptable safety levels for both IoT environments, such as for devices or objects themselves.

As a final part of our research we present the conclusions and recommendations, which present some results of all research, and recommendations for future studies or implementations of this promising technology.

Keywords

Internet of Things, IoT, Security, Schemes.

INDICE DE CONTENIDOS

RESUMEN ii

ABSTRACT iv

DEDICATORIA xi

AGRADECIMIENTO xii

CAPÍTULO I: INTRODUCCIÓN Y OBJETIVOS 13

1.1 INTRODUCCIÓN 13

1.2 JUSTIFICACIÓN 14

2.3 ANTECEDENTES 17

2.4 OBJETIVOS: 21

2.4.1 General: 21

2.4.2 Específicos: 21

CAPITULO II: MARCO TEÓRICO 22

2.1 ¿Qué es el internet de las cosas? 22

2.2 ¿Cómo de inteligentes son las cosas hoy día? Situación actual de una tecnología prometedora. 26

2.2.1 El Internet de las Cosas en los diferentes sectores 29

2.2.2 Teléfonos inteligentes: los ojos y oídos de las aplicaciones 39

2.3 Entendiendo las tres capas básicas del Internet de las Cosas 41

2.3.1 El hardware para conectar el mundo 43

2.3.2 Preparando la infraestructura del futuro 47

2.3.3 Software y datos al servicio de las personas 51

2.4 El impacto del Internet de las Cosas en los negocios y la sociedad 52

2.4.1 Servicios ubicuos para consumidores conectados 53

2.4.2 Open Source y modelos de negocio colaborativos 56

2.4.3 Optimizando las cosas: hacia un desarrollo realmente sostenible 58

2.5 Factores determinantes en el futuro del Internet de las Cosas 61
2.5.1 Principales barreras al IoT 64
2.6 Proyectos de ciudades inteligentes 66
2.7 Consideraciones de costos asociados a la implementación del internet de las cosas. 71
2.7.1 ¿Cuánto cuestan los tags RFID? 71
2.8 Sistema Operativo Contiki 72
CAPITULO III: MARCO METODOLÓGICO 77
3.1 Hipótesis 77
3.2 Variables 77
3.2.1 Variable independiente: 77
3.2.2 Variable dependiente: 77
3.3 Metodología 77
3.3.1. Tipo de investigación 77
3.3.2. Diseño de investigación 78
3.3.3 Métodos de investigación 78
3.3.4 Técnicas e instrumentos de recolección de datos 78
3.4 Plan recolección de la información 79
3.5 Plan de procesamiento y análisis de la información. 79
CAPITULO IV: MECANISMOS DE SEGURIDAD EN EL INTERNET DE LAS COSAS 81
4.1 Análisis de información determinante a la seguridad 81
4.1.1 Análisis FODA 88
4.2 Niveles de seguridad 89
4.2.1 Seguridad a nivel de hardware 90
4.2.2 Seguridad a nivel de software 92

4.2.3 Seguridad en la red 96
4.3.4 Seguridad en la nube 99
4.3 Costos asociados a la seguridad de los objetos 102
4.3.1 Análisis de costos 105
4.4 ESQUEMAS PARA DISEÑAR OBJETOS INTELIGENTES CON NIVELES DE SEGURIDAD ACEPTABLES. 108
4.4.1 Componentes IoT 108
4.4.2 Esquema de seguridad para un entorno de IoT 110
4.4.3 Análisis de los componentes del esquema 110
4.4.4 Componentes de un objeto inteligente 127
4.4.5 Esquema de seguridad de un dispositivo IoT 131
4.5 Beneficios del proyecto 140
CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES 142
5.1 Análisis de resultados 142
5.2 Validación de hipótesis 149
5.3 Conclusiones 153
5.4 Recomendaciones 155
BIBLIOGRAFÍA 157
GLOSARIO 167
ANEXOS 170

ÍNDICE DE FIGURAS

Figura 1: Índice de dispositivos conectados según estudio de CISCO 18

Figura 2:"La evolución de un objeto más inteligente"..... 28

Figura 3: Marco estándar de la industria para la visualización Mundial del M2M de servicios conectados conocidos como el Internet de las Cosas..... 30

Figura 4: Internet de la salud..... 35

Figura 5: Anatomía de una amenaza moderna..... 50

Figura 6: "5 cambios al futuro que producirá el internet de las cosas"..... 62

Figura 7: Interfaz del simulador de Contiki 74

Figura 8: Simulación de sensores en Contiki..... 76

Figura 9: Componentes para un proyecto de IoT..... 82

Figura 10: Objetos conectados..... 89

Figura 11: Marco conceptual IoT con Cloud Computing en el centro 100

Figura 12: Crecimiento del tráfico en la nube por regiones..... 101

Figura 13: Relación entre costo y seguridad de los objetos, costos altos. 103

Figura 14: Relación entre costo y seguridad de los objetos, costos bajos..... 104

Figura 15: Punto de Equilibrio: Costo/Seguridad/Riesgo 108

Figura 16: Componentes de un entorno IoT. 109

Figura 17: Esquema de seguridad para entorno IoT 110

Figura 18: Componentes de un objeto IoT..... 128

Figura 19: Esquema de seguridad para un objeto IoT..... 131

ÍNDICE DE TABLAS

Tabla 1: Análisis FODA 88

Tabla 2: Consideraciones de seguridad asignada a los componentes IoT 120

Tabla 3: Capa de seguridad omnipresente 123

Tabla 4: Protocolos de seguridad para dispositivos IoT 126

DEDICATORIA

Quiero dedicarle este trabajo.

A Dios que me ha dado la vida y fortaleza para terminar este proyecto de investigación.

A mis Padres por estar ahí cuando más los he necesitado y me han sabido formar con buenos sentimientos, hábitos y valores.

A mis hermanos que han estado junto a mi bríndame su apoyo en todo momento.

A mi novia Mariuxi por apoyarme y ayudarme en los momentos buenos y malos.

Fabián Geovanny Cuzme Rodríguez

AGRADECIMIENTO

El presente trabajo de tesis primeramente me gustaría agradecerle a ti Dios por bendecirme para llegar hasta donde he llegado.

A mi familia, en especial a mis padres que son parte importante de mi vida, que me han apoyado incondicionalmente en esta carrera profesional.

A mi novia Mariuxi, que con su apoyo desde el inicio hasta el final de este trayecto siempre me ha dado las fortalezas necesarias para no rendirme y seguir adelante en mi preparación personal y profesional.

A mi director de tesis, Dr. Gustavo Chafla por su dedicación, quien con sus conocimientos, su experiencia, su paciencia y su motivación pueda terminar mis estudios con éxito.

A mis revisores de tesis, Mtr. Francisco Balarezo y Mtr. Francisco Rodríguez, quienes con sus aportes ayudaron a que este trabajo fuera un éxito.

A todas las personas que han formado parte de mi vida personal y profesional les agradezco su amistad, consejos, apoyo, ánimo y compañía en algunos momentos de mi vida.

Fabián Geovanny Cuzme Rodríguez

CAPÍTULO I: INTRODUCCIÓN Y OBJETIVOS

1.1 INTRODUCCIÓN

En el presente trabajo se plantea, determinar los mecanismos de seguridad que se deben considerar al momento de implementar el IoT "Internet de las Cosas". El fin principal es establecer pautas de seguridad a nivel de hardware, software y red, que deberán tener los objetos que estarán conectados en el Internet enviando y recibiendo información de diferentes partes, además de considerar también los niveles de seguridad en la nube, ya que la tendencia es de almacenar la información en la nube también conocida Cloud Computing.

Se analizaran los costos asociados al implementar mecanismos de seguridad en cada uno de los objetos que estarán conectados a la red, plantear esquemas de diseño para los objetos inteligentes aceptables que permitan dar seguridad al usuario que los manipula, sin tener ningún perjuicio de confiabilidad en los datos que manejaran.

No existen estudios desarrollados sobre mecanismos de seguridad para los objetos inteligentes conectados a la red o el llamado IoT, lo que nos da la pauta para relacionarnos en base a artículos publicados sobre el tema, analizar e ir determinando esquemas de diseño para establecer los mecanismos que se requieren para que los objetos conectados a una red sean seguros.

1.2 JUSTIFICACIÓN

Las tecnologías de la Información y comunicación se han convertido en una herramienta indispensable para el intercambio de información ([1] Unión Internacional de Telecomunicaciones (UIT) - Ministerio de Ciencia y Tecnología), la convergencia de servicios televisión, telefonía, mensajería entre otros hacia una única red de comunicaciones hace que la Internet sea parte fundamental de nuestras vidas.

El internet de las cosas es una innovación tecnológica que nos permitirá transformar todos nuestros objetos en "Smart-objetos". Todas las cosas que nos rodean estarán conectadas en red transmitiendo y recibiendo información para facilitarnos la vida y volverla más eficiente, ya sea en consumos energéticos, en administración de finanzas e incluso en la utilización de nuestro tiempo ([2] Gutiérrez, 2013).

Esta innovación tecnológica IoT asume que permitirá:

Interactuar con las cosas*:* será la manera de relacionarnos con los objetos que nos rodean.

Monitorear cosas: Los objetos que utilizamos cotidianamente podrían entregarnos información de vuelta.

La búsqueda de cosas: Con el internet de las cosas podríamos saber en tiempo real donde está lo que queremos o necesitamos.

Administrar cosas: Las ciudades serían totalmente distintas. Esta nueva tecnología permitirá que las Smart-ciudades puedan administrar las congestiones vehiculares

habilitando rutas según la cantidad de personas que salen de su trabajo a la misma hora.

Cada vez más la población a nivel mundial, nacional y local utilizan las nuevas innovaciones tecnológicas para facilitar el vivir diario de alguna forma, donde el internet de las cosas encaja de una manera extraordinaria en ese contexto de necesidad, sin embargo las cuestiones de seguridad también se vuelven bastante relevantes al momento de utilizar este tipo de tecnologías y revolucionar la manera de comunicación entre los objetos y, más aun con el nuevo protocolo de comunicación IPV6 que garantiza direcciones IP para muchos años.

De igual manera así como hay beneficios, también existen desafíos. En el momento en que un objeto se vuelve parte de un entorno interconectado, es necesario considerar que estos dispositivos han perdido seguridad física o lógica, ya que posiblemente se encontrarán localizados en entornos inhóspitos y serán accesibles al instante por individuos con malas intenciones. Los atacantes podrían interceptar, leer o modificar información, y podrían manipular sistemas de control y modificar la funcionalidad.

Con el internet de las cosas, alguien podría hackear un juguete, controlarlo para encender una cámara, y poder espiar. Alguien podría intervenir el control del lavamanos y dejar corriendo el agua en tu ausencia, o controlar los termostatos de tu hogar. Podrían intervenir tu automóvil mientras vas conduciendo, en fin, las posibilidades son muchas ([2] Gutiérrez, 2013).

El aportar con un análisis del futuro del internet de las cosas y exponer las consideraciones sobre las seguridades que involucra que todos los dispositivos estén conectados en el internet. Dado que todos los objetos estarán conectados a la red, ¿Quién se preocupará de que no hackeen nuestros aparatos? Es difícil dimensionar la cantidad de situaciones a las cuales nos expondremos.

Se observa la necesidad y la importancia de realizar la investigación propuesta, ya que el internet de las cosas es una de las innovaciones tecnológicas que está en un proceso de incursión y que requiere de cuidado analizar las seguridades que brindara o que puede brindar esta tendencia tecnológica a los usuarios, instituciones o empresas.

Se considera que la investigación del tema es factible porque se cuenta con los conocimientos, recursos técnicos, materiales, metodología, para el análisis de los principios a considerar en relación a las seguridades que se deberán tomar en cuenta.

El resultado que se desea obtener con el desarrollo de la tesis propuesta es:

Establecer los mecanismos de seguridad que debe tener la innovación tecnológica del Internet de las Cosas.

2.3 ANTECEDENTES

Internet nació conectando personas a través de máquinas. Ahora una parte importante de su Red, un 12% del tráfico, conecta máquinas que hablan entre ellas para cumplir una tarea sin necesitar al hombre. El siguiente paso es el llamado Internet de las cosas. Se trata de que el actual Internet salte del universo en que se mueve al de los objetos, identificados y capaces de conectarse e intercambiar información. Las explicaciones sobre este futuro Internet de las cosas están llenas de metáforas y no es extraño que, junto a científicos, también hayan escrito sobre este futuro novelistas como Bruce Sterling ([3] Delclós, 2007).

A través de Internet, los ordenadores y equipos se conectan entre sí mediante sus respectivas direcciones IP. Bajo la versión IPv4 utilizada actualmente, sólo hay cabida para unas 4.300 millones de direcciones. Teniendo en cuenta que casi un tercio de la población mundial ya está conectada "aproximadamente 2.000 millones de personas", no queda mucho margen para seguir conectando todos los objetos del Internet de las Cosas. Este cuello de botella en nuestras infraestructuras tendría solución en la última iteración del protocolo IPv6 ([4] Díaz, Demasi, Robles, & Vodopivec), que permitiría alojar unos 340 billones de billones de billones de direcciones IP. Es decir, más que suficiente para todo lo que hay en el planeta y el resto del sistema solar también ([5] Fundación de la Innovación Bankinter, 2011).

Según Cisco Internet Business Solutions Group (IBSG), Internet de las Cosas surgió entre 2008 y 2009 como un simple momento en el tiempo en el que eran más las cosas conectadas a Internet que las personas ([6] Evans, 2011).

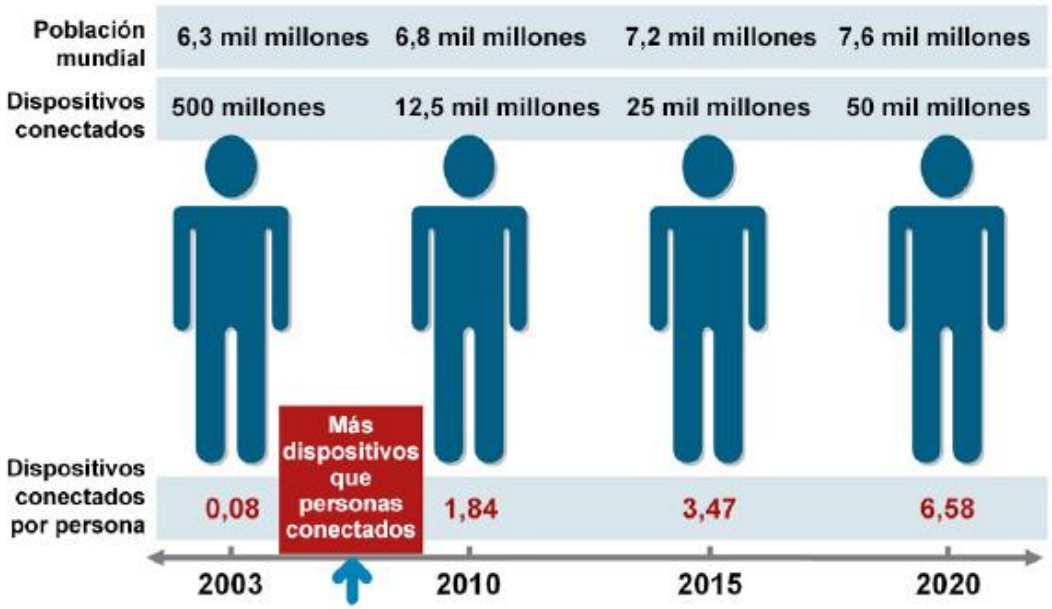


Figura 1: Índice de dispositivos conectados según estudio de CISCO ([6] Evans, 2011)
Fuente: Cisco IBSG, abril de 2011

Con miras al futuro, Cisco IBSG prevé que habrá 25 mil millones de dispositivos conectados a Internet para 2015, y 50 mil millones para 2020, Figura 1. Es importante destacar que estos cálculos no tienen en cuenta los rápidos avances en la tecnología de Internet o de los dispositivos; las cifras mostradas están basadas en datos actualmente válidos ([6] Evans, 2011).

Anteriormente los datos eran propiedad de las empresas "silos de datos" ahora disponemos de datos abiertos, lo dice Usman Haque, fundador de Pachube. Hace una década M2M era un diálogo entre máquinas, ahora Internet de las Cosas va sobre

conectar cosas dentro de la nube, lo dice Kristina Höök investigadora del Instituto Sueco de Ciencias de la Computación. Sin duda dos acontecimientos que nos sitúan en la realidad actual de IoT ([7] IBER GROUP IT). IoT está experimentando un desarrollo espectacular.

Una realidad que se fundamenta en hechos concretos como la adopción del nuevo protocolo de Internet (IPV6), la gran penetración de teléfonos inteligentes, el desarrollo de la nube, la aparición de los datos abiertos, el impulso del hardware libre o la extensión de RFID ([7] IBER GROUP IT). Pero, en ese camino aparecen también los nuevos desafíos como la necesidad de mantener la ingente cantidad de sensores que serán desplegados o la interoperatividad de los dispositivos. Por último y quizás lo más interesante, la inteligencia que se puede construir con los datos recogidos.

Internet de las Cosas está aquí, a nuestro alrededor, se ha hecho visible con la incorporación de los teléfonos inteligentes (Smartphone) a nuestra vida diaria. Internet de las Cosas tiene que ver sobre todo con sensores, esos diminutos dispositivos capaces de detectar todo lo que ocurre a nuestro alrededor, y con Internet. La nueva generación de hardware móvil viene repleta sensores: movimiento, ubicación, velocidad, humedad, luz ambiental, audio, imagen, entre otros. Con un Smartphone podemos medir nuestro pulso cardiaco, reconocer imágenes, geolocalizar objetos o personas, medir condiciones ambientales, saber cuánto hemos corrido, controlar todos los electrodomésticos del hogar y mil cosas

más. También se están incorporando sensores en ropa y accesorios como las gafas ([8] Paniagua, 2012).

La conectividad ya no se produce sólo desde un PC o un dispositivo móvil, cada vez hay más aparatos físicos cotidianos capaces de interactuar con la red y con otros sensores.

2.4 OBJETIVOS:

2.4.1 General:

- Establecer mecanismos de seguridad a considerar con la innovación tecnológica del Internet de las Cosas (IoT).

2.4.2 Específicos:

- Definir las debilidades y amenazas que presenta el Internet de las Cosas, en relación a la seguridad.
- Analizar los costos asociados al aplicar seguridad a los objetos.
- Determinar esquemas para diseñar objetos inteligentes con niveles de seguridad aceptables.

CAPITULO II: MARCO TEÓRICO

2.1 ¿Qué es el internet de las cosas?

Los avances tecnológicos se han convertido en un proceso imparable. Las innovaciones se van dando unas tras otras multiplicando sus efectos. En el campo de las Tecnologías de la Información y las Comunicaciones (TIC) hay que destacar varios momentos, como la digitalización de las señales, la transmisión de datos, la telefonía móvil, la fibra óptica o la banda ancha fija y móvil, que han transformado radicalmente el mundo de las comunicaciones. Gracias a todas estas tecnologías y aplicaciones disponemos hoy de un sistema de conexión universal como es Internet. Con el paso del tiempo, y gracias a la suma de innovaciones, la Red se ha ido transformando y ha pasado del concepto de Internet de las Personas al de Internet de las Cosas ([9] Redes de Telecomunicaciones y seguridad de la Información).

¿Qué es el Internet de las Cosas? Es la evolución de un primer Internet más centrado en las personas y cuyo potencial reside en la capacidad para combinar datos con personas, procesos y objetos. A partir de sensores, redes avanzadas de comunicaciones y procesos analíticos basados en el Big Data se están poniendo en marcha aplicaciones que harán más fácil la vida de las personas, mejorarán la sanidad y la educación, potenciarán las ciudades, los edificios y las redes eléctricas inteligentes, aumentarán la seguridad de la información e incrementarán el nivel de eficiencia de empresas y Administraciones Públicas.

Hasta ahora Internet era una red que permitía el acceso a portales, servicios, aplicaciones o diferentes opciones. El usuario, persona o negocio, entraba en ella y simplemente hacía lo que había ido a hacer, buscaba información o navegaba por las distintas posibilidades. Conforme la tecnología lo ha permitido, todo tipo de dispositivos, máquinas y objetos se han sumado a la red. Hablando de una gama de objetos infinita, desde el contador del consumo de agua que hay en los domicilios al sensor incorporado en una plaza de un aparcamiento público, pasando por una nevera, por una pulsera que lleva un enfermo o por un dispositivo asociado a una máquina en una fábrica. Todos ellos, al estar en permanente conexión con el resto del universo a través de Internet, pueden interactuar con personas, ordenadores u otros objetos, para dar información o avisos, recibir instrucciones, etc.

En esencia el Internet de las Cosas se basa en sensores, en redes de comunicaciones y en una inteligencia que maneja todo el proceso y los datos que se generan. Los sensores son los sentidos del sistema y, para que puedan ser empleados de forma masiva, deben tener bajo consumo y coste, un reducido tamaño y una gran flexibilidad para su uso en todo tipo de circunstancias. La evolución de Internet también precisa de potentes y seguras redes de comunicación inalámbrica M2M (máquina a máquina), que hagan posible la incorporación a las redes y a los sistemas de objetos totalmente fuera de ellos. Finalmente es necesario aplicar inteligencia a los sistemas y a los objetos, aprovechando los datos recogidos por los sensores, para procesarlos y convertirlos en información útil y en actuaciones. Aquí las técnicas de análisis asociadas al Big Data son vitales. En ocasiones hay que aplicar potentes sistemas de información y de software avanzado que hagan posible el tratamiento de

grandes volúmenes de datos de una naturaleza variada y a gran velocidad. Muchos de esos datos ya existían, pero hasta ahora la tecnología disponible no permitía su explotación y aprovechamiento.

Las ciudades inteligentes pueden ser un buen ejemplo de lo que es capaz de dar el Internet de las Cosas. En ellas, la combinación de dispositivos, sensores, redes de comunicaciones, capacidad de almacenamiento y de procesamiento y plataformas de gestión hacen posible que las ciudades en la que se facilitan servicios se lo hace de una forma más eficiente y sostenible, mejorando la vida de los ciudadanos, las posibilidades de los negocios y el atractivo de la propia ciudad para conseguir turismo, talento e inversiones. Entre los servicios que pueden mejorar significativamente se encuentran el suministro y consumo de energía o de agua, el transporte y la movilidad, la seguridad ciudadana y la protección civil, la creación de un entorno favorable para los negocios, el gobierno de la ciudad, la transparencia y participación ciudadana, el soporte al turismo y al comercio, la gestión de residuos, la gestión del mobiliario urbano, la eficiencia energética de los edificios o la gestión de los aparcamientos.

Además de las ciudades inteligentes, los campos de aplicación del Internet de las Cosas son muchos más variados. La sanidad, para monitorizar a los pacientes y conectarlos a los médicos y demás profesionales sanitarios; los sectores de la energía y del transporte, para conectar a proveedores y clientes; el sector del ventas al por menor, para predecir cuándo comprarán los consumidores; las telecomunicaciones y los servicios de información; los servicios financieros; o las fábricas inteligentes. En

estos y otros campos es posible encontrar también casos muy concretos de aplicación, como el marketing y la publicidad, la educación, los vehículos o los juegos y el entretenimiento conectado o las redes eléctricas inteligentes, en los que las nuevas posibilidades alcanzan rendimientos máximos.

El Internet de las Cosas requerirá de habilidades y conocimientos específicos combinados (tecnológicos, matemáticos o de funcionamiento de las organizaciones). Es decir, se abrirán nuevas e interesantes oportunidades de trabajo y se crearán empleos en este sector. Uno de los ejemplos más claros es el de los gestores de datos, esquema que se encuentra a mitad de camino entre la tecnología y la operación de los negocios y que requiere conocer y manejar las nuevas herramientas para la captura, el análisis y el aprovechamiento de los datos. La enseñanza, en sus diferentes niveles, también tendrá que hacerse eco de estas nuevas demandas ([9] Redes de Telecomunicaciones y seguridad de la Información).

Los desafíos y oportunidades son grandes y todas las actividades humanas en los diferentes sectores se verán afectadas por las posibilidades del Internet de las Cosas, que según diferentes análisis conectará varias decenas de miles de millones de dispositivos y objetos a corto plazo. Como ocurre con otras actuaciones asociadas a la evolución tecnológica, además de todos los temas de innovación hay también que analizar y valorar el impacto económico y social en las vidas de las personas, buscando su beneficio y cuidando al máximo los aspectos de seguridad y privacidad. Si todo ello se consigue, el Internet de las Cosas cambiará nuestras vidas radicalmente.

2.2 ¿Cómo de inteligentes son las cosas hoy día? Situación actual de una tecnología prometedora.

En el mismo modo que el siglo XIX fue el escenario de la Revolución Industrial, el siglo XX fue testigo de la Revolución de la Información. Con la aparición de las tecnologías TCP/IP, HTML y Wifi, aprendimos a navegar por la red y a utilizar contenidos web. Luego vimos nacer el comercio electrónico (e-commerce) y asistimos a la explosión de la colaboración abierta distribuida (crowdsourcing) y el concepto 2.0. Está claro que la popularización de Internet y los avances en las telecomunicaciones han facilitado que todo esté cada vez más conectado ([5] Fundación de la Innovación Bankinter, 2011).

Al fin y al cabo, los sensores y dispositivos colocados en todo tipo de objetos y conectados a Internet a través de redes fijas e inalámbricas son cada vez más pequeños y baratos. Las redes son capaces de extraer un gran volumen de datos capaces de ser analizados por un ordenador. Es un punto en el cual los objetos ya no sólo hablan con nosotros, sino que también están dotados de la inteligencia para hacerlo entre ellos. Estamos formando parte de una sociedad ubicua, en la que podemos estar en varios lugares simultáneamente.

En realidad, ¿cómo de inteligentes son estos dispositivos? A medida que se desarrolle la tecnología, la información recopilada será objeto de un análisis más exhaustivo, las decisiones que se tomen más acertadas y, de ser necesario, el

lanzamiento de un proceso automático más óptimo. Con ello, la intervención humana se irá minimizando. “Según la Fundación Francesa IDATE, en 2020 habrá en el mundo 80.000 millones de conexiones entre dispositivos de distinta naturaleza, que en su hipótesis corresponderían a tres categorías:

1) Los de comunicación, desde los móviles hasta los aparatos de Smart TV.
2) Los descritos como máquina a máquina (M2M) y
3) Los objetos en general.

En esta última categoría cabría incluir casi cualquier cosa aunque carezca de electrónica en su seno, pero que esté vinculada al resto de la realidad a través de dispositivos intermediarios” ([10] Gallego, 2013). Para entender esto, explicaremos la pirámide de la evolución de un objeto más inteligente de Accenture.

Empecemos por la base de la pirámide. En este nivel, el objeto cobra una identidad unívoca, por ejemplo, mediante una etiqueta RFID. En un segundo nivel, se utiliza la tecnología (GPS) para localizar la posición o trayectoria del objeto. Un nivel más arriba en la pirámide, se dota al objeto de estado, es decir, que sea capaz de comunicar su estado actual y sus propiedades. Por último, y en la cúspide, se dota al objeto de contexto para que sea consciente del entorno en el que se encuentra (véase la Figura 2).

El ejemplo más típico no requiere que nos remitamos al mundo del Internet de las Cosas, porque ya lo tenemos en muchos hogares. Los termostatos de calefacción regulan la temperatura del ambiente, dependiendo de los grados que registren. Pero la conexión de los sensores a Internet los hará aún más sofisticados. Por ejemplo, se podrán integrar en prendas de ropa para que mida lo que pesa una persona y le den consejos de adelgazamiento, o podrá colocarse en neveras para que comprueben las existencias y hagan pedidos de comida automáticamente.



Figura 2:"La evolución de un objeto más inteligente" ([11] Accenture 2005)
Fuente: Sensor Telemetry, Accenture 2005.

2.2.1 El Internet de las Cosas en los diferentes sectores

Imaginemos una ciudad del futuro. Una ciudad inteligente en la que los teléfonos móviles abren puertas, los sensores detectan fugas en las cañerías de agua y las vallas publicitarias cambian sus anuncios según el esquema de consumidor de las personas que pasan. Como veremos a continuación el IoT se ha aplicado a todo tipo de industrias, como la sanitaria, agrícola, logística o de suministros, permitiendo conectar todo tipo de máquinas para monitorizarlas y controlarlas de manera inteligente, como se muestra en la Figura 3, un arco de dispositivos que se conectan en los diferentes sectores que dan origen al Internet de las Cosas. Estas industrias han evolucionado en mayor o menor grado dentro del terreno del IoT, situándose en distintos niveles de la pirámide de Accenture explicada anteriormente. No obstante, el objetivo común de todas es el incremento en eficiencia, la reducción de costes, la mejora en la toma de decisiones, el ahorro energético y la protección medioambiental ([5] Fundación de la Innovación Bankinter, 2011).

A continuación aparte de la figura mostrada donde existe una gran variedad de sectores de aplicación del Internet de las Cosas, haremos referencia a ciertos sectores como: ventas, logística, gestión de cadenas de suministros, telecomunicaciones, tecnologías médicas de salud, fabricación, industrias petróleo y gas, y agricultura y ganadería.

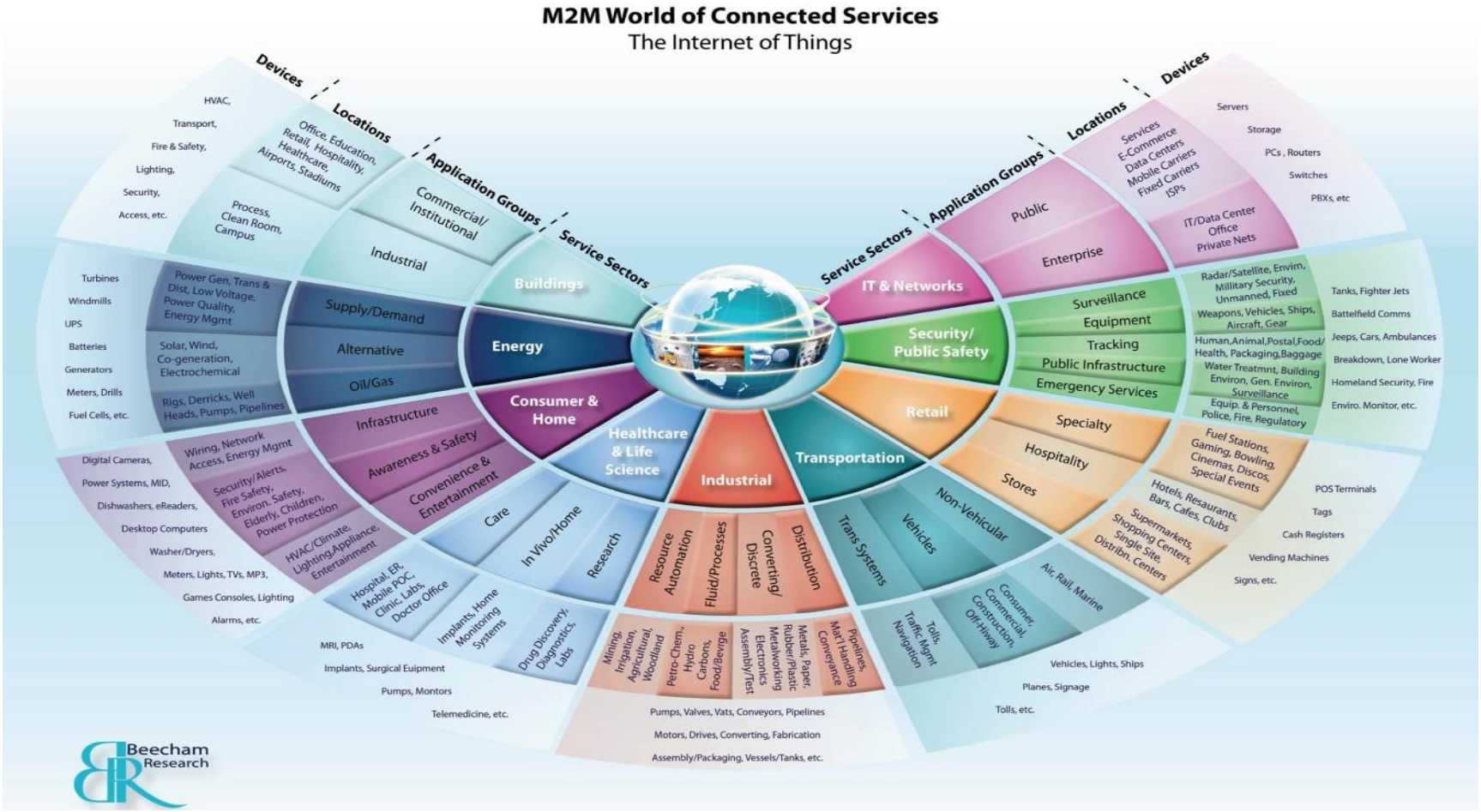


Figura 3: Marco estándar de la industria para la visualización Mundial del M2M de servicios conectados conocidos como el Internet de las Cosas. ([12] Beecham Research, 2011)
Fuente: Beecham Research 2011

2.2.1.1 Ventas, Logística, Gestión de Cadena de Suministros

La implementación del Internet de las cosas en Ventas por Menor/Gestión de Cadena de Suministros tiene muchas ventajas: artículos equipados con RFID y estantes inteligentes que rastrear los elementos presentes en tiempo real, un minorista puede optimizar muchas aplicaciones, como comprobar automáticamente la recepción de mercadería en tiempo real, control de stocks, seguimiento de falta de existencias o la detección de robo.

Los expertos del sector consideran que la integración inteligente de personas, procesos y datos a través de dispositivos electrónicos y sensores facilitará la automatización del proceso de fabricación y mejorará la visibilidad de los productos a lo largo de toda la cadena de suministro ([13] Jimenez, 2014).

El potencial de ahorro en una tienda minorista es grande. Además, los datos de la tienda minorista pueden utilizarse para optimizar la logística de la cadena de suministro: Si los fabricantes conocen las acciones y datos de ventas de los minoristas, pueden producir y enviar la cantidad correcta de productos, evitando el exceso de producción o producción insuficiente.

Los procesos logísticos de las cadenas de suministro en muchos sectores de la industria pueden beneficiarse del intercambio de datos por RFID, no sólo en el sector minorista. Además, se pueden abordar en circunstancias ambientales, por ejemplo se

puede optimizar la huella de carbono de las cadenas de suministro más generalmente procesos y logística basado en la disponibilidad de datos dinámicos, de grano fino, recogidos en el mundo real directamente por algunas de las "cosas" (por ejemplo, camiones, palets, artículos de productos individuales, etc., según el caso).

En la tienda misma se pueden ofrecer muchas aplicaciones como guía de acuerdo a las necesidades de los clientes como una lista de compras preseleccionada, soluciones de pago rápido, salida automática de las compras utilizando la biometría, la detección de alérgenos potenciales en un determinado producto, personalizado de marketing si aceptan, verificación de la cadena de frío, etc.. Edificios comerciales por supuesto se beneficiarán de las funcionalidades de edificio inteligente.

2.2.1.2 Telecomunicaciones

En el área de las telecomunicaciones muchos crearán la posibilidad de fusión de las tecnologías de telecomunicaciones diferente y crear nuevos servicios. Un ejemplo es el uso de GSM, NFC, Bluetooth de bajo consumo, WLAN, redes de múltiples saltos, GPS y sensor de redes junto con la tecnología de la tarjeta SIM. En estos tipos de aplicaciones del lector/etiqueta forma parte del teléfono móvil, y diferentes aplicaciones comparten la tarjeta SIM. NFC permite las comunicaciones entre objetos de una manera simple y segura a un rango de cercanía uno del otro ([14] Penalva, 2011). El teléfono móvil por lo tanto puede ser utilizado como un lector NFC y transmitir los datos leídos a un servidor central. Cuando se utiliza un teléfono móvil, la tarjeta SIM desempeña un papel importante como almacén para las

credenciales de los datos y autenticación de NFC (como números de boleto, las tarjetas de crédito, información del identificador etc.).

Las cosas pueden unirse a redes y facilitar la comunicación peer-to-peer para fines especializados para aumentar la robustez de redes y canales de comunicación. Las cosas pueden formar ad hoc, las redes Peer-to-peer en situaciones de desastre para mantener el flujo de información vital en caso de fallas de infraestructura de telecomunicaciones.

Grandes organismos internacionales de normalización también tienen en marcha iniciativas de normalización sobre Internet de las cosas, tales como la Organización Internacional de Normalización (ISO), la Comisión Electrotécnica Internacional (CEI) y el Grupo Especial sobre Ingeniería de Internet (IETF), que coopera estrechamente con el World Wide Web Consortium (W3C), la ISO y la CEI ([15] ITU News, 2013).

Los trabajos del IETF han dado lugar a una pila de protocolos que pueden soportar la implementación de una Internet de las cosas interoperable. Los protocolos correspondientes del IETF son, entre otros, IPv6 por redes de área personal inalámbricas de baja potencia, el protocolo IPv6 para redes de baja potencia y con pérdidas, y el protocolo de aplicación limitada.

2.2.1.3 Tecnología médica de salud, redes de área personal, monitoreo de parámetros, posicionamiento, sistemas de localización en tiempo real.

En el área sanitaria existen y se desarrollan muchas aplicaciones, con la posibilidad de utilizar el teléfono celular con capacidades de sensor RFID como una plataforma para el monitoreo de los parámetros médicos y fármacos. Las enormes ventajas deben ser consideradas en primer lugar en la prevención y fácil control, teniendo un impacto fundamental en nuestro sistema social, y en segundo lugar en caso de accidentes y la necesidad de diagnóstico ad hoc.

La combinación de sensores, RFID, NFC, Bluetooth, ZigBee, 6LoWPAN, WirelessHART, ISA100, WiFi permitirá significativamente mejor medición y control de métodos de funciones vitales (temperatura, presión arterial, frecuencia cardíaca, los niveles de colesterol, glucosa en la sangre etc.). Además, se espera que se convierta en la tecnología de sensor disponible a un costo mucho menor y con soporte incorporado para la conectividad de red y monitoreo remoto ([16] Jurado Pérez, Velásquez Vargas, & Vinueza Escobar, 2014).

Implantar identificables inalámbricos podrían utilizarse para almacenar registros de salud que podrían salvar la vida del paciente en situaciones de emergencia especialmente para personas con diabetes, cáncer, enfermedad cardíaca coronaria, accidente cerebrovascular, enfermedad pulmonar obstructiva crónica, debilitaciones cognoscitivas, trastornos convulsivos y enfermedad de Alzheimer, así como personas

con implantes de dispositivos médicos complejos, tales como marcapasos, endoprótesis vascular, reemplazo de articulaciones y trasplantes de órganos y que pueden estar inconsciente e incapaz de comunicarse por sí mismos, ver Figura 4.

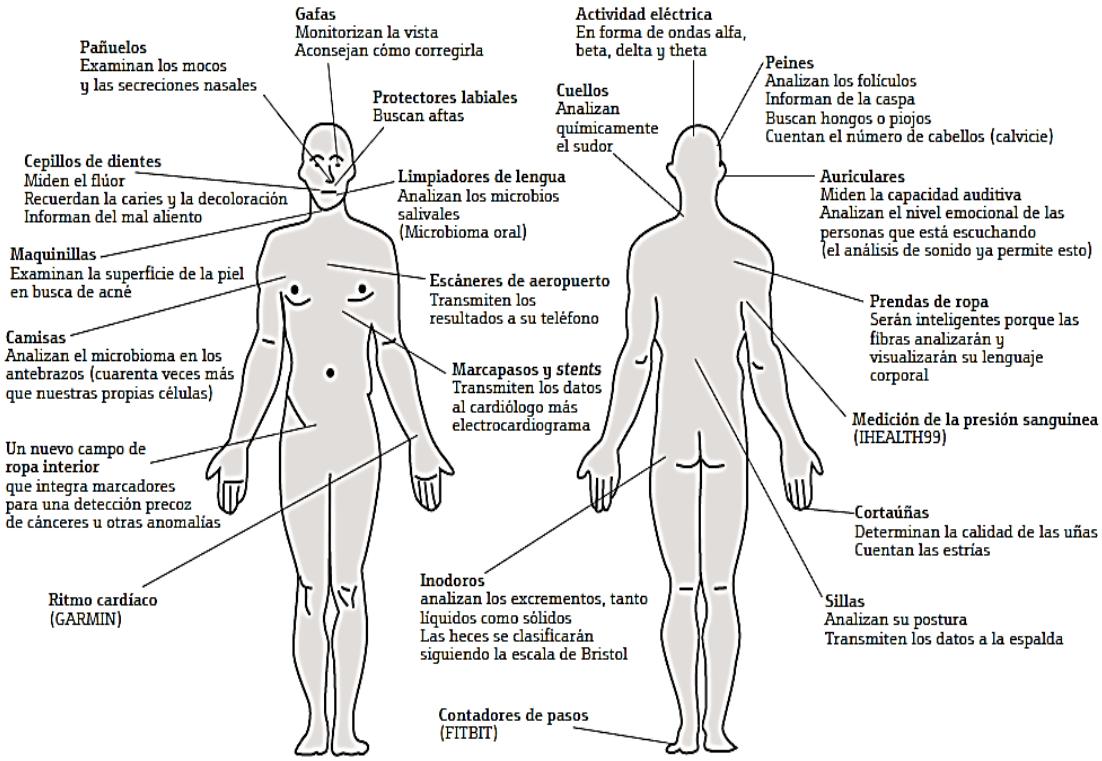


Figura 4: Internet de la salud ([5] Fundación de la Innovación Bankinter, 2011)
Fuente: http://quantifiedself.com/

Chips de comestibles, biodegradables podrían ser introducidos en el cuerpo y utilizados para acción guiada. Las personas parapléjicas podrían tener estímulos musculares entregados mediante el sistema de simulación eléctrico implantados, inteligentemente controlados con el fin de restaurar las funciones de movimiento.

Las cosas están cada vez más integradas dentro del cuerpo humano. Se espera que las redes de área corporal puedan ser formadas y que se comuniquen con tratamientos médicos, servicios de emergencia y los seres humanos cuidando ancianos.

2.2.1.4 Fabricación

Vinculando los artículos con tecnologías de la información, ya sea a través de dispositivos inteligentes embebidos o mediante el uso de identificadores únicos y portadores de datos que puedan tener interacciones con un inteligente apoyo de la infraestructura de red y sistemas de información, pueden optimizar los procesos de producción y el ciclo de vida completo de los objetos, desde la producción hasta la eliminación puede ser monitoreado. Por etiquetar artículos y contenedores, puede obtenerse una mayor transparencia sobre el estado de la planta, la localización y disposición de lotes y el estado de las máquinas de producción. La información de grano fino sirve como datos de entrada para programas de producción refinada y mejor logística. Auto-organización e inteligentes soluciones de fabricación pueden ser diseñadas alrededor de elementos identificables.

Como un objeto y el componente de procesamiento de la información adjunta pueden ser inseparables, desde la producción hasta el final del ciclo de vida, la historia de un elemento y su estado actual puede continuamente ser monitoreada y almacenarse en la etiqueta o en el sistema de información. Los datos reflejan un producto de la historia de uso que incluye valiosa información para el diseño de producto, marketing y el diseño de producto relacionadas con servicios, así como decisiones de

fin-de-vida de reciclaje ecológico y seguro, volver a fabricar o eliminación del producto ([16] Jurado Pérez, Velásquez Vargas, & Vinueza Escobar, 2014).

La implementación del IoT a la fabricación ofrece soluciones que están revolucionando la forma de producir definiendo lo que los expertos definen como fabricación avanzada. Las grandes empresas lo saben, no quieren quedarse atrás y están haciendo un gran esfuerzo de inversión en el sector. Según un estudio realizado por McKinsey entre el 80 y el 100 por ciento de todos los fabricantes utilizarán aplicaciones IoT en 2025, con un impacto económico potencial de 2,3 billones de dólares solo para el sector de fabricación global. El uso de IoT en fabricación lidera la lista de aplicaciones con más potencial ([17] LogicFin).

2.2.1.5 Industria - Petróleo y Gas

Industria del Gas y el petróleo está utilizando arquitecturas escalables que consideran la posibilidad de plug-and-play ID nuevos métodos combinados con detección/accionamiento integración con la infraestructura de Internet de las Cosas, e integran el monitoreo inalámbrico personal petrolero en situaciones críticas en tierra o mar adentro, seguimiento de contenedores, seguimiento de los tubos de perforación, cadena, componentes, monitoreo y manejo de equipo fijo ([16] Jurado Pérez, Velásquez Vargas, & Vinueza Escobar, 2014).

La Internet de las cosas puede ayudar a reducir accidentes en la industria de petróleo y gas. Por ejemplo, contenedores con mercancías peligrosas pueden ser un hecho inteligente equipándolas con nodos de sensores inalámbricos.

Un escenario posible es que estos nodos envían periódicamente mensajes de información sobre el producto químico que está dentro del contenedor se atan así como el límite máximo de almacenamiento de este producto químico en la ubicación actual. Como los nodos tienen acceso a una lista de sustancias químicas incompatibles, puede enviar mensajes de alerta en cuanto reciben un mensaje de información de otro nodo que está conectado a un recipiente con una sustancia química incompatible. Estos mensajes de alerta pueden enviarse luego a un sistema de backend que, por ejemplo, informa al Gerente de la planta sobre la crítica situación que se está generando en ese momento.

2.2.1.6 Agricultura y Ganadería

Las regulaciones para la trazabilidad de los animales de agricultura y sus movimientos requieren el uso de las tecnologías, como mucho, haciendo posible la detección de tiempo real de los animales, por ejemplo durante los brotes de enfermedades contagiosas ([16] Jurado Pérez, Velásquez Vargas, & Vinueza Escobar, 2014). Además, en muchos casos, los países dan subsidios dependiendo del número de animales en un rebaño y otros requisitos, a granjas con ganado, ovejas y cabras. Como la determinación de la cantidad es difícil, siempre hay la posibilidad de fraude. Sistemas de identificación bien implementados pueden ayudar a minimizar el

fraude. Por lo tanto, con la aplicación de sistemas de identificación, enfermedades de los animales pueden ser controladas, encuestadas y prevenidas. Identificación oficial de los animales en nacional, la comunidad y comercio internacional ya está en el lugar, mientras que al mismo tiempo, identificación del ganado vacunado o testado bajo control de las enfermedades oficiales o también es posible la erradicación. Las muestras de sangre y tejidos pueden ser identificadas con precisión, y el estado de salud de rebaños, regiones y países puede certificarse mediante el uso de muchos.

Con el Internet de las cosas, los agricultores individuales pueden ser capaces de entregar las cosechas directamente a los consumidores no sólo en una región pequeña como en marketing directo o tiendas, sino en una zona más amplia. Esto va a cambiar la cadena de suministro que está principalmente en manos de grandes empresas, ahora, pero puede cambiar a una cadena más corta, más directa entre productores y consumidores.

2.2.2 Teléfonos inteligentes: los ojos y oídos de las aplicaciones

Es algo notable y visible para todos como ver a la gente tecleando sin parar en los autobuses, consultando cómo llegar a los sitios con un solo clic o subiendo una foto a una red social en plena calle. Los teléfonos inteligentes o también conocidos como smartphones están de moda. Quienes creen que las funciones de su móvil se reducen a realizar llamadas, enviar mensajes de texto y, como mucho, despertarles por la mañana, están a punto de descubrir que los teléfonos móviles ofrecen mucho más que eso. El teléfono inteligente es el término comercial para denominar a un teléfono

móvil cuyo funcionamiento gira en torno a la conexión a Internet y al uso de un teclado similar al de un ordenador. A veces se presenta en formato de pantalla táctil y, en todo caso, viene provisto de menús y atajos como parte de un sistema operativo que facilita su uso.

Además de soportar el envío y recepción de correos electrónicos, los teléfonos inteligentes permiten la instalación de aplicaciones que realizan una función específica para el usuario, como procesadores de textos, bases de datos, programas de edición de imágenes o chats. La penetración de smartphones ya supera el 50% en los grandes mercados de todo el mundo ([18] Marketing Directo, 2013).

No obstante, ¿qué relación guardan los teléfonos inteligentes con el Internet de las Cosas? Muy sencillo: Nuestros móviles y cámaras se están convirtiendo en los ojos y oídos de las aplicaciones; sensores de movimiento y ubicación nos dicen dónde estamos, lo que estamos viendo y la velocidad a la que nos movemos. Los datos se están recopilando y se está actuando en tiempo real en base a ellos. La escala de participación se ha incrementado en órdenes de magnitud ([19] Tim & John, 2009). Los teléfonos inteligentes contienen multitud de sensores de sonido, luz o aceleración que recogen información y la envían a Internet. A medida que más usuarios entren a formar parte de la plataforma y se generen más datos, se desarrollarán más aplicaciones para aprovechar la ventaja de este dispositivo. Algunas de ellas no son más que puro entretenimiento, otras se presentan como soluciones efectivas a problemas reales. ¿Algunos de sus usos más insólitos? Una aplicación que sopla velas, otra que resuelve cubos de Rubik o sudokus, Trapster,

que permite a sus usuarios compartir los controles de velocidad de carretera con otros miembros, o WideNoise que mide la contaminación acústica.

En el otro extremo, existen aplicaciones para teléfonos inteligentes que van a revolucionar la logística y la sanidad. Tanto es así, que hasta febrero de 2010 había 5.805 aplicaciones médicas, de salud y fitness en la tienda de aplicaciones on-line de Apple. Si bien es verdad que sólo el 27% estaban dirigidas a profesionales y el resto a pacientes y usuarios finales ([20] Foundation California Healthcare, 2010), las aplicaciones pretenden cubrir cada vez más las carencias de nuestros saturados sistemas de sanidad en aspectos delegables a dispositivos que, por ejemplo, se encarguen de monitorizar enfermedades crónicas. Sin embargo, hay que tener en cuenta que descargarse una aplicación no te convierte automáticamente en licenciado en medicina.

2.3 Entendiendo las tres capas básicas del Internet de las Cosas

Hasta ahora hemos visto cómo el fenómeno del Internet de las Cosas ha irrumpido a nuestro alrededor, dando vida a objetos cotidianos que se interconectan gracias a Internet y constituyen fuentes inagotables de información. Para entender el Internet de las Cosas desde un punto de vista más técnico es necesario comprender las tres capas que lo hacen realidad hoy en día ([5] Fundación de la Innovación Bankinter, 2011).

- ✓ *La primera capa es el hardware*. Más de medio siglo después de los pesados ordenadores que ocupaban salas enteras, los componentes son cada vez más pequeños, lo que permite desarrollar ordenadores más potentes y rápidos que sus predecesores. Esta capa física ocupa menos espacio, lo que facilita que se pueda conectar prácticamente cualquier cosa, desde cualquier sitio, en cualquier momento. Dando paso al fenómeno de la miniaturización.

- ✓ *La segunda capa es la infraestructura*, o más bien sus limitaciones. Si miles de millones de nuevos dispositivos se conectan al IoT, ¿cómo lo soportará la tecnología actual? ¿Se va a convertir el espectro de Internet en el combustible del siglo XXI? Se hace necesario afrontar el problema del espectro como un recurso limitado.

- ✓ *La tercera y última capa la forman las aplicaciones y los servicios* que ponen en uso la gran cantidad de información creada a partir del IoT y donde se encuentra el mayor potencial de creación de valor. Estas aplicaciones conllevan a la creación de nuevos modelos de negocio e iniciativas empresariales muy interesantes desde el punto de vista de la innovación.

Estas tres capas la miniaturización del hardware, las necesidades de infraestructura y el desarrollo de software innovador son fundamentales para entender la expansión del Internet de las Cosas en el terreno de las tecnologías de la información y la comunicación.

2.3.1 El hardware para conectar el mundo

Los sensores y actuadores son piezas fundamentales que posibilitan el Internet de las Cosas. Al fin y al cabo, permiten que todos los objetos cotidianos interactúen con los ordenadores a través de Internet y recopilen valiosa información sobre el entorno en el que se encuentran. Es probable que en un futuro no muy lejano nos encontremos en un momento en el que se genere más información a partir de estos sensores que desde el teclado de los ordenadores. El motivo es sencillo: los sensores cada vez son más pequeños, lo que facilita que puedan ser integrados en cualquier objeto, bajo cualquier circunstancia ([5] Fundación de la Innovación Bankinter, 2011).

Para hacer esto posible, se pueden observar tres tendencias diferentes: la miniaturización de los dispositivos, el desarrollo de nuevas formas de computación como los ordenadores ADN o los ordenadores cuánticos y la creación de redes inteligentes de elementos simples.

La primera tendencia la miniaturización consiste en el proceso tecnológico mediante el cual se ha logrado reducir el tamaño de los dispositivos electrónicos, entre ellos los sensores. Junto a la nanotecnología, la miniaturización ha permitido que el tamaño de elementos como los microprocesadores algo así como el cerebro de los ordenadores sea mínimo sin disminución de la velocidad a la que funcionan.

Por lo tanto, parece que Moore no iba del todo descaminado con su predicción. Recordemos que corría el año 1975 cuando se postuló que el número de transistores en un chip se duplicaría cada dos años ([21] Reyes, 2012), haciendo posible la proliferación de la tecnología en todo el mundo. Con una mayor cantidad de transistores aumenta la velocidad de cálculo de los ordenadores. Moore también sugirió una disminución de costes, ya que los componentes con base de silicio utilizados en los ordenadores crecerían en rendimiento a la vez que se volverían más económicos de producir y abundantes en nuestra vida diaria. Unido a la Ley de Metcalf, que sostiene que el valor de una red de comunicaciones aumenta proporcionalmente al cuadrado del número de nodos del sistema ([22] EcuRed, 2013), es evidente que todos los factores económicos y tecnológicos apuntan a la computación ubicua.

Sin embargo, la reducción en tamaño no es perenne y pronto se presentará una limitación física a los componentes basados en el silicio. Algunos expertos intentan solventar este problema centrando sus líneas de investigación en los llamados ordenadores de ADN, que utilizan moléculas orgánicas para almacenar la información de partida y resolver problemas matemáticos a través de reacciones químicas, o los ordenadores cuánticos, que emplean elementos de mecánica cuántica para codificar y procesar la información. Gracias a esta característica, los componentes de los ordenadores cuánticos serán más pequeños, a la vez que podrán realizar enormes cálculos en un tiempo mucho más reducido ([23] Muy Interesante, 2006).

2.3.1.1 ¿Qué son capaces de hacer estos sensores?

Según el estudio realizado por la Fundación de la Innovación Bankinter indica que a medida que avanza la miniaturización de los componentes electrónicos, sus aplicaciones se multiplican. Cada vez más, sensores diminutos son integrados en los elementos del entorno, conectando el mundo físico con el mundo digital. ¿Qué son capaces de hacer los sensores que integramos en nuestro entorno? En gran medida, estos sensores tienen tres grandes aplicaciones ([5] Fundación de la Innovación Bankinter, 2011).

Primero, permiten capturar información tanto del entorno como del objeto en el que se encuentran integrado, para un análisis posterior. Por ejemplo, las compañías de seguros pueden utilizar sistemas de sensores para recuperar información de las formas de conducción de sus asegurados.

Segundo, los sensores pueden actuar como desencadenantes de una acción, permitiendo la automatización de determinadas funciones. Este puede ser el caso de la activación de una alarma por la detección de una persona no autorizada o el frenado automático de un coche ante la inminente colisión con otro vehículo, en esta parte intervienen los llamados actuadores que ejecutan una acción en base a su programación y a lo que el sensor recopila.

Por último, los sensores también podrán ser localizables en todo momento, con lo que se expande el rango de aplicaciones. Por ejemplo, la localización de los paquetes

en los sistemas de gestión de logística permite la determinación de su posición exacta a lo largo de un trayecto y la comunicación con las cintas transportadoras para establecer el destino de las mercancías. Pero las aplicaciones no acaban ahí, sino que el IoT añadiría la posibilidad de integrar el comportamiento del consumidor o las decisiones de la empresa contratante durante el proceso, pudiendo hacer cambios sobre la marcha para minimizar costes, evitar retrasos o, simplemente, adaptarse a las fluctuaciones en la oferta y la demanda de productos. Más allá de las grandes aplicaciones de los sensores, existen dos grandes retos a los que nos enfrentamos en su desarrollo: el consumo de energía y la interoperabilidad de sus componentes.

Los sensores consumen energía y, a medida que su tamaño disminuye, este consumo se convierte en un factor más limitador. De forma acorde con el tamaño del sensor, el tamaño de las fuentes de alimentación también disminuye y con ello el tiempo de funcionamiento del sensor. Por este motivo, se espera que los componentes sean capaces de generar su propia energía. De esta manera, los sensores podrán permanecer conectados a la red de forma autónoma durante más tiempo. Es más, en entornos en los que no haya ningún punto de acceso fijo ofreciendo una comunicación eficiente para las cosas, se formarán redes de información ad hoc extensas que dirijan la información hacia la infraestructura fija o su nodo de destino en la red formada. Esto permite que los sensores se coloquen en todas partes, aun cuando la infraestructura sea débil o ausente, e incluso si los sensores son móviles ([24] Continental Automated Buildings Association, 2008).

Sin embargo, el reto para promover la adopción del Internet de las Cosas no será el consumo de energía, sino la flexibilidad y modularidad de los componentes que asegure su fácil integración. Si no se promueve la interoperabilidad entre los componentes, existirán muchas trabas a la aceptación a gran escala del IoT.

2.3.2 Preparando la infraestructura del futuro

La capacidad de las infraestructuras de telefonía móvil es limitada y la proliferación de los teléfonos inteligentes está saturando la capacidad de las redes. Si a esto se suman millones de nuevos dispositivos conectados a Internet, la tecnología 3G o LTE ([25] Área Tecnología) no serán suficientes, y la combinación del uso del móvil, la conexión wifi y la fibra óptica cobran vital importancia para subsanar la saturación de las infraestructuras móviles. Aunque el negocio 3G y LTE está creciendo a nivel mundial, la capacidad de las redes móviles actúa como un cuello de botella para el buen despliegue del IoT, ya que las infraestructuras existentes pueden sufrir un colapso por el aumento de conexiones desmedidas que provocara el IoT.

Los gobiernos empiezan a abogar por compartir el espectro. Una tendencia actual son los llamados wifi hotspots o puntos calientes inalámbricos de conexión a internet. Estas zonas se encuentran en lugares públicos, como cafeterías, parques, terminales terrestres, aeropuertos y bibliotecas, donde se permite, a veces gratis y a veces a cambio de una suma de dinero, conectar ordenadores o teléfonos móviles, entre otros. Un ejemplo es lo que hace el Gobierno chino se ha propuesto transformar las cabinas de teléfono públicas en puntos de este tipo para hacer del país una red

gigante de acceso a conexión wifi ([26] ISon21, 2010), otro ejemplo seria lo que están haciendo los diferentes Gobiernos Autónomos Descentralizados de las diferentes provincias del Ecuador, como por ejemplo Portoviejo, Tosagua, Guayaquil que tienen puntos calientes de acceso a internet en lugares céntricos como parques, en el caso del Terminal Terrestre de Guayaquil que permite el acceso a los usuarios durante 30 minutos de manera gratuita. Con estas iniciativas se estaría creando una plataforma de conexión para una economía emergente que tiene todo el potencial de convertirse en el nuevo objetivo de la actividad on-line.

Spectrum Interactive, proveedor líder de acceso a Internet y servicios inalámbricos para los sectores de hostelería, viajes y medios de comunicación. La empresa, además de ofrecer soluciones de conexión wifi fiable desde cualquier localización y desde kioscos de Internet, ha desarrollado una cartera de servicios muy diversa y relacionada con el Internet de las Cosas: televisión a través de IP, herramientas de seguimiento remoto de las condiciones meteorológicas o soportes digitales de publicidad que pueden promocionar el producto adecuado en el momento y lugar apropiados ([5] Fundación de la Innovación Bankinter, 2011).

Para poder aprovechar estas oportunidades, es necesario que las redes de sensores se abran al gran público. De esta manera, muchos microproveedores podrán desarrollar modelos de negocio basados en la gestión de redes locales que capitalicen los activos susceptibles de conectarse al IoT y cubrir las necesidades de millones de consumidores.

Las infraestructuras deberán estar acorde a las exigencias del IoT y mantener su flexibilidad y escalabilidad, permitiendo un crecimiento sostenible de esta tendencia, generando confianza en los clientes y proveedores de servicio.

2.3.2.1 La nube y la complicación de la seguridad

El desafío que representa la seguridad de una amplia gama de aplicaciones, dispositivos y usuarios, ya sea en un contexto de "cualquiera con cualquiera" o de Internet de todo, se torna más complicado debido a la popularidad de la nube como medio para administración de los sistemas empresariales. Según los datos reunidos por Cisco, se prevé que el tráfico mundial de centros de datos se cuadriplique durante los próximos cinco años, y el componente de crecimiento más acelerado son los datos en la nube. Para 2016, el tráfico mundial en la nube representará aproximadamente dos tercios del tráfico total de centros de datos ([27] Cisco Systems, Inc., 2013).

Las soluciones de seguridad segmentadas, por ejemplo, la aplicación de firewalls en el perímetro de una red variable, no protegen los datos que ahora se encuentran en constante movimiento entre dispositivos, redes y nubes. Incluso entre los centros de datos, que ahora albergan información confidencial de las empresas (los datos masivos), la virtualización es la regla y no la excepción. Abordar los desafíos de seguridad que generan la virtualización y la nube exige el replanteo de los estados de seguridad, a fin de reflejar este nuevo paradigma: es necesario cambiar los controles

basados en el perímetro y los antiguos modelos de acceso y contención para proteger el nuevo modelo empresarial.

Anatomía de una amenaza moderna de acuerdo al informe de seguridad de Cisco 2014 ([28] Cisco Systems, Inc., 2014), ver Figura 5.

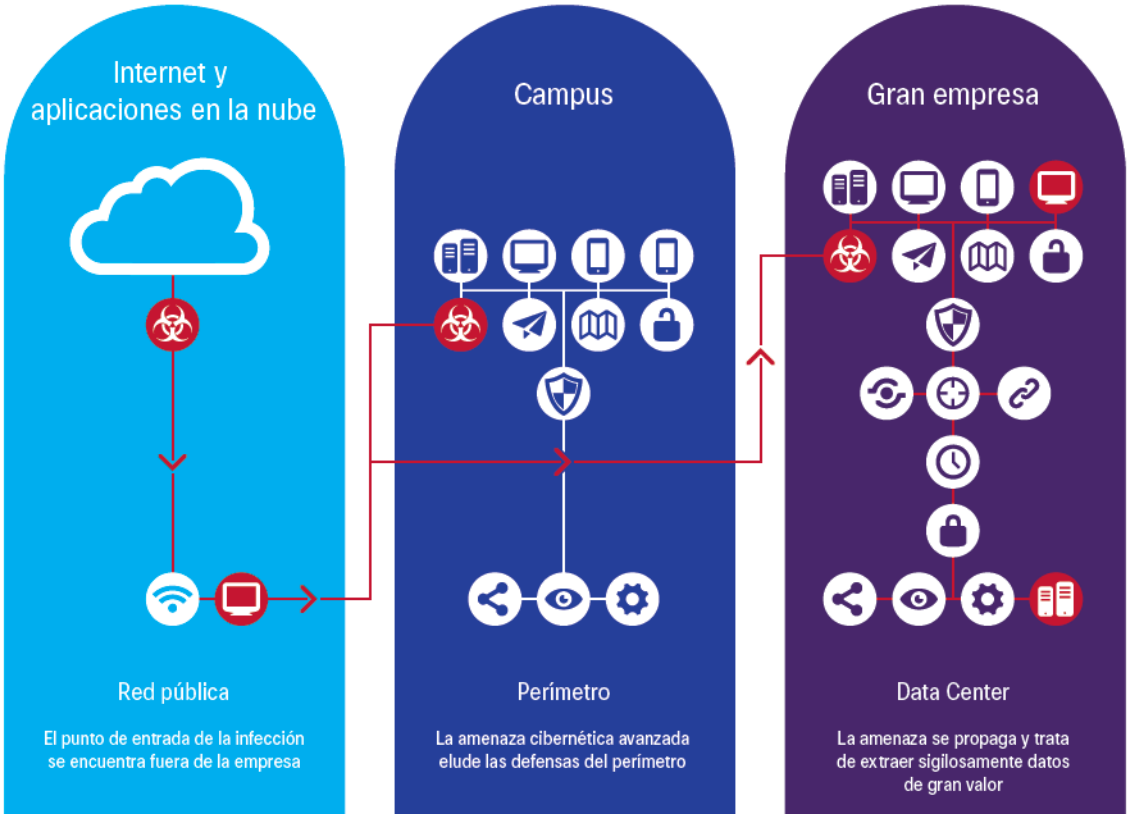


Figura 5: Anatomía de una amenaza moderna ([28] Cisco Systems, Inc., 2014)
Fuente: Cisco Systems, Inc., 2014

La figura 5 muestra claramente cómo se produce una acción malintencionada en un dispositivo que se encuentra fuera de la red corporativa, provocando una infección que se propaga a una red de campus y dicha red actúa como un trampolín para llegar a la red empresarial, para luego abrirse camino hasta el tesoro oculto que es el Data Center.

2.3.3 Software y datos al servicio de las personas

Con el desarrollo de aplicaciones de software, es posible producir respuestas rápidas a fenómenos físicos sobre la base de la información recogida o los patrones que siguen determinados objetos o personas. Se crean nuevas oportunidades para satisfacer los requerimientos del negocio, desarrollar nuevos servicios en tiempo real, adentrarse en procesos y relaciones complejas, gestionar incidencias, abordar la degradación del medio ambiente, supervisar las actividades humanas, mejorar la integridad de la infraestructura y tratar de resolver cuestiones de eficiencia energética ([29] Comisión Europea, 2009).

Grandes compañías como Microsoft que ha lanzado su programa de desarrolladores para el internet de las cosas, Microsoft quiere que Windows como plataforma también esté presente en dispositivos cotidianos, con el objetivo de recoger feedback y hacer una prueba de concepto de estas primeras herramientas y así lanzar nuevas herramientas en el futuro, las cuales estarán más pulidas y ofrecerán más funcionalidades ([30] Yirá, 2014).

MediaTek anuncio también la creación de MediaTek Labs, una iniciativa global que permite a los desarrolladores crear dispositivos y soluciones pertenecientes a ese futuro mundo de dispositivos conectados al que se ha dado en llamar Internet de las Cosas. Este programa ofrece un kit de desarrollo software (SDK), un kit de desarrollo hardware (HDK), y documentación técnica, con la idea de ofrecer a esa

nueva generación de emprendedores, desarrolladores y creadores las herramientas necesarias para que puedan llevar a buena escala sus ideas ([31] Pastor, 2014).

De esta forma muchas otras empresas también están con iniciativas para el desarrollo de software que permiten el análisis de la información que se generará con el Internet de la Cosas, el Open Source juega un papel muy importante en este desarrollo de software de manera colaborativa, conjugando ideas y mejorando las aplicaciones y herramientas de desarrollo.

El verdadero valor de negocio va a venir de la mano de estas aplicaciones y servicios que utilicen la nueva información que se está generando en el Internet de las Cosas. Van a surgir nuevos métodos de análisis inteligente de la información y las tareas manuales van a ser sustituidas por automatismos que operen en base a dicha información, prescindiendo de la intervención humana. El desarrollo de software óptimo para este tipo de tareas va a enfrentarse al elevado ritmo de las oportunidades. Emprendedores y empresas ya establecidas desarrollarán nuevas aplicaciones que exploten nuevas fuentes de información y cambien radicalmente los modelos de negocio.

2.4 El impacto del Internet de las Cosas en los negocios y la sociedad

Todos los negocios existentes deben comprender el impacto del IoT en sus operaciones y repensar sus modelos de negocio. Éstos están cambiando de las ventas de productos discretos, a los modelos de ingresos recurrentes. IoT ofrece la

oportunidad y una rápida evolución dentro de la necesidad, para monitorear y responder a los clientes casi en tiempo real ([32] Perea, 2014). Debido a que el internet se ha convertido en un factor fundamental de la economía global, la mayoría de usuarios a nivel mundial lo utilizan en su vida laboral y social.

Resulta interesante analizar cómo el Internet de las Cosas está cambiando el terreno de los modelos de negocio. Si bien es verdad que las grandes empresas suelen asentar las bases de la infraestructura tecnológica, los emprendedores son los agentes transformadores de nuestra sociedad que impulsan las tendencias más innovadoras. Son capaces de traducir costes en creación de valor.

El IoT y su impacto en las personas, los hogares, las ciudades y sobre todo en los negocios, estaría pasando de una industria 1.0 a una 4.0. Y lo que nos permitiría esta interconexión entre las cosas es monitorear, ubicar, gestionar y controlar de una manera más eficiente un negocio. Esto se ve reflejado en la obtención de precios dinámicos, facturación por consumo, autogestión, socialización, publicidad contextual, de esta manera lo manifestó Alejandro Girardotti, Product Manager Regional de Level 3 en el 6to. Foro Level 3 de Tecnología y Negocios ([33] TyN Megazine).

2.4.1 Servicios ubicuos para consumidores conectados

Estar permanentemente conectado y localizable ¿quién de nosotros no ha dicho alguna vez de no sé cómo me las arreglaba antes sin mi teléfono móvil?, está

surgiendo una nueva generación de consumidores, en paralelo a la aparición de la banda ancha móvil. Este segmento espera, o casi exige, que la red facilite todas las actividades que desea llevar a cabo y permanecer conectados allá donde vaya. Casi dan por hecho la conexión wifi y cualquier avance técnico que permita la movilidad. En otras palabras, el Internet de las Cosas comprende todo lo que pueda satisfacer sus necesidades ([5] Fundación de la Innovación Bankinter, 2011).

En muchos casos, los fabricantes sólo se tienen que limitar a reinventar objetos ya existentes para aumentar su utilidad gracias a la conectividad a la red. Por ejemplo, un bote de pastillas es un objeto cotidiano que, provisto de conexión a Internet, puede decirle al usuario, a sus familiares o a los médicos si se ha abierto o cerrado y a qué horas, para llevar un control de la toma de dosis por parte del paciente ([34] Penalva, 2013). Es sobre todo muy útil para el seguimiento de enfermedades crónicas, como la diabetes o la hipertensión. El inventor de este dispositivo acertó a la hora de trasladar este producto al mercado, al aliarse con las farmacéuticas que, obviamente, cuentan con grandes incentivos para procurar que los pacientes se tomen su medicación regularmente.

También el dispositivo Chumby ([35] Xataca), algo así como el reloj de mesilla 2.0. Consiste en una pantalla táctil con conexión wireless a Internet para acceder a una infinidad de aplicaciones de previsión meteorológica, redes sociales, chats, compras on-line, visualización de vídeos, etc. Es completamente personalizable de acuerdo con los intereses y aficiones de cada usuario. Con todo ello, se están descubriendo nuevos caminos hacia los consumidores. Muy probablemente la aplicación de

Internet a los objetos de uso cotidiano se asemejará al momento que se vivió hace más o menos un siglo, cuando se empezó a disponer de la versión eléctrica de muchos objetos caseros como la lavadora, la cafetera, la batidora, etc., que antes eran manuales.

Los comportamientos del consumidor a la hora de utilizar tecnología para sus compras se ve reflejada en el uso de su teléfono inteligente para realizar comparaciones de precios y observar las valoraciones de productos on-line antes de comprarlos. Con esa base la gran mayoría de ellos tomará una decisión de compra en función de la información consultada, comparar en el comercio donde se anunciaba más barato, pedir rebajas o de decidir no comprar el producto.

La posibilidad de consultar características, prestaciones y valoraciones de productos da al consumidor un poder sin precedentes. Las comparativas de mercado fomentan una bajada de precios y, sobre todo, un consumidor más informado y activo. Hoy día, es muy frecuente que un consumidor genere contenidos e interactúe con otros compradores on-line para intercambiar impresiones sobre productos. Los foros constituyen un punto de partida para muchas personas que se quieren informar acerca de una compra. Se busca información sobre un nuevo vecindario a la hora de comprar una casa, sobre el funcionamiento de dispositivos electrónicos o sobre los restaurantes con mejor servicio. Con un solo clic, es posible acceder a datos agregados que constituyen experiencias de primera mano, las más valoradas por los consumidores ([5] Fundación de la Innovación Bankinter, 2011).

Emily Green, Presidente de la Junta de Yankee Group y autora de ANYWHERE (en cualquier lugar) describe una nueva generación de consumidores, el segmento que se correlaciona con la emergencia a la banda ancha móvil, para usarla en todas las actividades que ellos quieren. Los consumidores no están seguros acerca de la conectividad, pero creen en ella, la quieren. Además, los comportamientos de los consumidores están cambiando rápidamente con consecuencias enormes para las marcas ([36] Green, 2011).

El desarrollo del Internet de las Cosas está llevando a que el consumidor sea cada vez más exigente, al estar conectados y localizables en todo momento facilita una mayor personalización de los servicios y objetos que nos rodean, así como una mayor información disponible en el momento de la toma de decisiones.

2.4.2 Open Source y modelos de negocio colaborativos

Con el nuevo entorno digital y las exigencias de los mercados, cada vez se crean más empresas con modelos de negocios del siglo XXI, como es el caso de los modelos de negocios colaborativos similar al Open Source en el mundo de software, y en vista que se tienen objetos permanentemente conectados generando modelos abiertos de colaboración.

Google y Microsoft son dos de las empresas líderes en desarrollo de software: Google es por su motor de búsqueda y Microsoft ha logrado que su sistema operativo Windows sea uno de los más utilizados por los usuarios de ordenadores de todo el

mundo. Pero existe una gran diferencia entre ambas empresas, mientras que Microsoft se limita a vender software y aplicaciones sin compartir su código fuente, Google se ha centrado en la venta de servicios. Es decir, Google ofrece todos sus productos de forma gratuita porque su modelo es más popular con usuarios que no quieren pagar por utilizar aplicaciones durante períodos cortos de tiempo. Estas aplicaciones quedan rápidamente obsoletas o son sometidas a mejoras por los propios usuarios. En esta línea, el Open Source es un movimiento que se centra en la premisa de que al compartir abiertamente el código fuente de los programas, las mejoras que pueden aportar terceras personas dan como resultado un programa infinitamente mejor. El apoyo que han mostrado empresas como Sun al desarrollo del Open Source está desplazando los modelos de negocio de formas tradicionales a otras más abiertas y colaborativas ([5] Fundación de la Innovación Bankinter, 2011).

Esto se debe a que hay cosas en los negocios que no cambian a menudo como por ejemplo las gasolineras venden gasolina, los restaurantes venden menús y los dentistas limpiezas bucales. Eso no va a cambiar. Son las funciones centrales de un negocio en las que se basa la actividad, la razón de ser de la empresa. Sin embargo, hay otra serie de factores que sí pueden cambiar frecuentemente: precios, tasas impositivas, nuevos productos, campañas de marketing o unidades de negocio. Por ello, los negocios deben ser capaces de cambiar rápidamente para adaptarse sin impactar de forma negativa en las funciones centrales. Los desarrolladores de software son conscientes de ello y son capaces de diferenciar las partes que cambian frecuentemente de las que permanecen iguales. Cuando esta práctica se aplica a la gestión de la información de una empresa, se llama SOA (Arquitectura Orientada a

Servicios). Es decir, SOA consiste en aislar las funciones de negocio en los servicios independientes que no cambian con frecuencia.

Muchas empresas se están apuntando a la web 2.0, 3.0 y las redes sociales con el objetivo claro de acercarse al consumidor y descubrir nuevas líneas de negocio. Sin embargo, el Smart Business o Inteligencia Empresarial consiste en llevar la interacción en la red al extremo. Es decir, el negocio no presenta ninguna jerarquía formal y se autogestiona gracias a la colaboración de personas motivadas o con algún interés en un determinado campo o aplicación. El mejor ejemplo es Wikipedia o el Open Source Linux, que sugiere que las empresas pueden aprovechar la especialización si ceden el control sobre el contenido de los productos a los colaboradores y participantes (proveedores, clientes, intermediarios, etc.).

Esta formas de negocios colaborativa tienen un gran potencial permitiendo descubrir, diseñar y desarrollar sistemas ubicuos en los que la innovación este presente ante todo.

2.4.3 Optimizando las cosas: hacia un desarrollo realmente sostenible

La optimización del consumo de recursos constituya uno de los campos más prometedores para el Internet de las Cosas. Los sensores y los sistemas de control automáticos integrados en objetos a nuestro alrededor permiten medir distintas variables que pueden llevar al cambio en los patrones de uso de recursos escasos.

Curiosamente, nos encontramos ante un círculo vicioso: mientras la aplicación del IoT en redes inteligentes permite realizar un consumo sensato de la energía, la propia industria de las tecnologías de la información y la comunicación (TIC) es una consumidora creciente de energía. Según la Universidad Técnica de Dresde, el 3% del consumo mundial de electricidad se atribuye actualmente a las granjas de servidores y a las infraestructuras de telecomunicaciones. Para el año 2030 se espera que el consumo eléctrico mundial se haya doblado, en parte por el aumento exponencial del consumo por parte de las TIC ([5] Fundación de la Innovación Bankinter, 2011).

Además de las redes inteligentes de energía, otras aplicaciones en torno a un consumo más responsable se suceden en la gestión del agua, el transporte inteligente y el control de tráfico, la gestión de residuos y reciclaje, el diseño de edificios, etc. El gigante de la electrónica Hewlett Packard ha construido una plataforma llamada CeNSE (Sistema Nervioso Central para la Tierra) que pretende establecer una red mundial de miles de millones de sensores que midan datos relacionados con objetos y personas ([37] DIARIO ABC, S.L, 2010). El objetivo es recabar información sobre variables como localización, temperatura, presión, sonido, luz, humedad y etc. Parte del reto consiste en lograr que los sensores sean, además de pequeños y resistentes, lo más baratos posible.

Como ya se ha dicho, toda esta información resulta fundamental para que las personas puedan tomar decisiones de consumo más acertadas. Las etiquetas RFID contribuyen ampliamente a que un comprador pueda consumir teniendo toda la

información necesaria en sus manos, literalmente. Imagine un producto en el supermercado con una etiqueta de este tipo que le puede indicar cuándo fue producido, cuándo fue empaquetado, cuánto tardó en llegar al supermercado, si la temperatura durante el viaje fue óptima, los precios históricos del producto, etc. ([38] Macmanus, 2009).

Cabe destacar Sourcemap, una red social y herramienta gratuita para acceder a información sobre el origen de los objetos más cotidianos con el fin de poder tomar decisiones de consumo sostenibles. ¿Sabía que un ordenador portátil está hecho de materiales como cobre, estaño, litio, rodio e indio? Algunos de ellos son procesados artesanalmente por familias en países en vías de desarrollo, otros se piensa que se agotarán en menos de diez años. Los fundadores de Sourcemap llaman la atención sobre la importancia de saber de dónde provienen las cosas, como en el caso de los ordenadores portátiles. Sólo de esta manera podremos evitar el consumo desmesurado de materiales básicos que pueden acabar por desaparecer ([39] Pomares, 2012).

Evidentemente, podemos pensar que antes de que se acaben determinados materiales, se encontrarán alternativas adecuadas para la fabricación, siguiendo con nuestro ejemplo, de ordenadores portátiles. Sin embargo, piense en el otro extremo del ciclo de vida, es decir, en su destrucción cuando dejan de tener uso. Los ordenadores portátiles suelen terminar en países con controles medioambientales débiles, donde se despiezan o funden para obtener materiales que, a su vez, son utilizados para fabricar nuevos objetos. El problema surge cuando estos nuevos objetos son, por

ejemplo, juguetes. Ya se ha dado algún caso de retirada del mercado de juguetes que contenían sustancias nocivas para la salud porque su fabricación en ciertos países no había pasado los controles de seguridad pertinentes. Una vez más, no saber de dónde vienen las cosas puede tener consecuencias graves ([5] Fundación de la Innovación Bankinter, 2011).

La colaboración de los consumidores a nivel global facilita la circulación de información que puede ayudar a mejorar la calidad de vida y reducir el impacto ecológico de nuestros hábitos en el planeta. Precisamente es el Internet de las Cosas la tecnología que permite realizar el seguimiento y recopilar información valiosa acerca de objetos provistos de sensores y dispositivos inteligentes. Otra muestra más de cómo la innovación a través de la tecnología se pone al servicio de las personas para retrasar los efectos perjudiciales que tiene nuestro modo de vida sobre el medio ambiente.

2.5 Factores determinantes en el futuro del Internet de las Cosas

El mundo del futuro será un mundo conectado, con miles de millones de dispositivos y sensores entre los que se encuentran los dispositivos personales compartiendo información, con capacidad para analizar, diagnosticar y tomar decisiones, haciendo posible la creación de nuevos servicios más inteligentes que contribuirán a la sostenibilidad del planeta, a un uso más eficiente de los recursos y, en definitiva, a un incremento de la calidad de vida de las personas ([40] Caminero, 2012). Figura 6.



Figura 6: "5 cambios al futuro que producirá el internet de las cosas" ([41] Gutierrez, 2013). Fuente: http://creascion.com/5-cambios-al-futuro-que-producir-el-internet-de-las-cosas/

El Internet de las Cosas será la estructura más compleja que la humanidad haya creado jamás. En una generación, es probable que exista un billón de nodos que midan cualquier cosa que se pueda medir sobre la faz de la Tierra y con la información extraída de esos datos controlaremos todos los aspectos del mundo que hemos construido ([42] Hirshberg, 2012).

Entonces, ¿qué podemos aprender del pasado y cómo nos puede orientar?

1. ¿Quiénes serán los arquitectos de todo esto? ¿Sería mejor de arriba abajo de forma ordenada, integrada, como corresponde a una corporación gigante o de abajo arriba de forma confusa, innovadora, resultado de reparaciones brillantes? No obstante, ¿cómo podría funcionar todo como un sistema?

La historia nos dice que algunas de nuestras estructuras más complejas y viables no son grandes redes integradas, sino que en realidad se trata de varias redes

heterogéneas, que se adaptan y aprenden. La planificación es más una aplicación sistemática de lo aprendido que un acto de preordenación. Las ciudades e Internet son, ambas, buenos ejemplos de ello y también dos de los mayores logros de la humanidad. Al mismo tiempo, con las comunidades de innovación global actuales y el crowdsourcing, es más que probable que algunas de las ideas más valiosas y perdurables vayan a surgir como sorpresas no planificadas.

2. El Internet de las Cosas tiene carácter político. Es algo digno del aprendiz de brujo, que va a afectar a toda nuestra vida, con grandes repercusiones sociales, económicas y sobre la privacidad. Por lo tanto, más vale que sea construida de forma inclusiva, ya que, de lo contrario, el temor puede superar sus beneficios. Los padres fundadores de Estados Unidos no prescribieron el modo en que se debería dirigir el país durante los siguientes doscientos años; diseñaron mecanismos para la participación y la manifestación de intereses discrepantes. En el caso del IoT existe una oportunidad similar de gobierno flexible.

3. Nadie sabe cuál será la aplicación determinante o killer application del IoT. En primer lugar, vamos a instrumentalizar las cosas obvias, las mismas cosas que hemos medido a lo largo del siglo XX: energía, transporte y procesos industriales. Sin embargo, las aplicaciones más profundas del Internet de las Cosas no existen en la actualidad y probablemente, si existieran, nos parecerían cosas sin sentido.

2.5.1 Principales barreras al IoT

Los principales obstáculos para la adopción del Internet de las Cosas se pueden encontrar infinidades de problemas viéndolos desde varios puntos de vista, pero se los puede enmarcar en asegurar la privacidad y seguridad de las nuevas soluciones, y conseguir estándares globalmente aceptados. Otras preocupaciones que amenazan con poner freno a su despegue son las limitaciones de la infraestructura actual, la falta de interoperabilidad entre sistemas, la fuerte inversión necesaria en equipos y las barreras psicológicas.

2.5.1.1 Privacidad y seguridad

Hay una necesidad de tener una solución técnicamente para garantizar la privacidad y la seguridad de los clientes y de las empresas para poder tener una adopción generalizada de cualquier sistema de identificación de objetos. Mientras que en muchos casos se ha hecho la seguridad como una característica adicional, es la sensación que la aceptación pública de Internet de las Cosas ocurrirá sólo cuando las soluciones de seguridad estén en su lugar. Estos podrían ser los mecanismos de seguridad híbrido que combina por ejemplo seguridad hardware con diversificación clave para proporcionar seguridad superior que hace ataques significativamente más difícil o incluso imposible. Continuará la selección de características de seguridad y los mecanismos que determine el impacto en los procesos de negocio; y las compensaciones se hará entre el tamaño del residuo, coste, funcionalidad, interoperabilidad, seguridad y privacidad.

La privacidad de la información juega un capítulo importante en las arquitecturas de IoT. La comisión Europea y países como Estados Unidos han debatido este tema en el pasado analizando las consecuencias que la privacidad y seguridad genera en la creciente demanda de conectividad de las "cosas". Las implicancias de no comprender la importancia en la seguridad o privacidad podría ser devastador en la arquitectura diseñada. Podrían verse afectados, por ejemplo, datos personales bancarios, de salud, etc. o información empresarial o de industrias, gobiernos, etc. El efecto o el riesgo dependen del contexto y la función que cumplen los datos generados por los sensores o dispositivos que están conectados a la red ([43] IOT SIMPLE S.A.).

Por las próximas normas que deben definir funciones de seguridad diferentes para proporcionar confidencialidad, integridad o servicios de disponibilidad deberían abordarse las cuestiones de seguridad y privacidad.

También hay una serie de cuestiones relacionadas con la identidad de las personas. Estas deben ser tratadas en la política y legislación, y que son de importancia crucial para las administraciones públicas eficientes del futuro.

2.5.1.2 Gobernanza

Una barrera importante para la adopción generalizada de la tecnología de Internet de las Cosas es la ausencia de gobernabilidad. Sin una autoridad, similar a la que

gobierna Internet, existen altas probabilidades que será imposible tener un verdaderamente global "Internet de las Cosas".

También existe la necesidad de mantener la gobernabilidad como genérico como sea posible, como tener una autoridad por campo llevará sin duda a superposición, la confusión y la competencia entre las normas. Arquitectura EPC Global tiene una arquitectura "punto único de falla y control" en una sola empresa, VeriSign, tiene los registros de todos los números y puede rastrear donde es cualquier objeto. Así, objetos pueden tener diferentes identidades en diferentes contextos para tener múltiples autoridades esto crearía una especie de multihoming, que puede conducir a resultados desastrosos.

¿Qué podría ser la gobernanza de la internet de las cosas, y cuán diferente sería de la gobernanza de la Internet de hoy? Sigue siendo una incógnita si debería ser una agencia dirigida por el estado o un grupo bajo la supervisión de las Naciones Unidas, o un consorcio industrial. Todas las partes deben convocar y trabajar juntos hacia una solución para evitar que eventualmente aparezca un estándar de facto, como lamentablemente en estos casos la solución ganadora a menudo no es el técnico más avanzado.

2.6 Proyectos de ciudades inteligentes

El crecimiento de las ciudades cada vez se va dando de una manera más acelerada y uno de los elementos que generan dicho crecimiento son los propios ciudadanos. Con

el vivir diario se van dando cuenta de las necesidades de su entorno siendo el motor principal para conseguir un lugar idóneo para desarrollar su proyecto de vida.

La tecnología vienen hacer el ingrediente principal para que las ciudades comunes y corrientes se conviertan en grandes Ciudades Inteligentes, que hace algunos años atrás solo se veía en películas de ciencia ficción. El empalme de la tecnología y las ciudades permiten gestionar el entorno que los rodeas en base a las necesidades de cada ciudadano haciéndolo más placentero para la vida.

A la hora de desarrollar este proyecto, en primer lugar es necesario llevar a cabo una estrategia que represente la idea de ciudad inteligente de futuro, un enfoque integral desde todas las perspectivas y áreas clave de la misma. Para tal efecto España cuenta con el apoyo de la multinacional de Tecnologías de la Información, Indra que presenta un proyecto de Ciudad 2020 que pretende lograr un avance en las áreas de eficiencia energética, Internet del futuro, Internet de las cosas, comportamiento humano, sostenibilidad medioambiental y movilidad y transporte, con el objetivo de diseñar la ciudad del futuro, sostenible, inteligente y eficiente ([44] Indra Sistemas S.A., 2011).

Para el desarrollo de una Ciudad Inteligente, Indra contempla desde el plano tecnológico hasta la gestión e integración de la información, qué decisiones serán automatizadas, pasando por el plano de interacción con los ciudadanos como la movilidad, los servicios urbanos, la energía, el medio ambiente o la seguridad.

Con el proyecto de Indra CIUDAD2020 logrará los objetivos 20-20-20: Reducción de un 20% de emisiones, producción de un 20% de energía renovable y mejora de un 20% de la eficiencia energética ([44] Indra Sistemas S.A., 2011).

Una "Ciudad Inteligente" es la respuesta a los retos del futuro, la respuesta que todo ciudadano busca, con una administración pública eficiente que genera nuevas respuestas sobre la base de la tecnología. En estas ciudades todo cobra importancia: desde la energía hasta los transportes, pasando por el mobiliario urbano. Todo ello ofrece una información al ciudadano y da respuesta a un nuevo entorno global ([45] Europa press, 2011).

Las Ciudades Inteligentes toman la figura de ciudades del futuro con el uso intensivo de las tecnologías de última generación. De esta manera se consigue una gestión eficiente de los recursos económicos en la planificación, gestión y operación de los diferentes servicios municipales a los ciudadanos.

Tienen como objetivo mejorar la calidad de vida de sus habitantes, aumentar la eficiencia de los servicios públicos, incrementar la participación de los ciudadanos en ellos, mejorar las condiciones de sostenibilidad medioambiental y aumentar las oportunidades que la ciudad ofrece a las personas y a las empresas ([45] Europa press, 2011).

La compañía Indra ya ha puesto en marcha este proyecto en España, en ciudades como Barcelona, Sant Cugat del Vallès y Lleida. La municipalidad de la ciudad

Barcelona, junto con Indra, ha presentado su modelo de Smart City para poder reducir el gasto público a través de tecnología inteligente y sostenible. El objetivo del proyecto de San Cugat se ha centrado en la reducción de las facturas del cabildo mediante una mejor gestión de los recursos ofreciendo servicios de valor añadido a través de la tecnología.

Gracias a este proyecto se ha podido reducir en el último año hasta en un 20 por ciento el gasto de agua gracias a la instalación de sensores inteligentes. Por su parte, el cabildo espera que esta cifra llegue hasta el 40 por ciento ([45] Europa press, 2011).

El desarrollo de Ciudades Inteligentes en Sant Cugat y Lleida permite un mejor aprovechamiento de los servicios municipales, llevando a cabo proyectos como la gestión eficiente del riego en parques y jardines en función de las condiciones ambientales, lectura remota de contadores, optimizar la recogida de basuras y el control del nivel de llenado de contenedores, gestión del alumbrado mediante la sincronización con las horas solares y gestión de la movilidad mediante el control de zonas de libre aparcamiento o limitar estancias en zonas de carga y descarga ([45] Europa press, 2011).

La información que se genera por parte de los ciudadanos y las empresas, mediante las infraestructuras inteligentes, permite el acceso a la Administración, creando nuevas oportunidades de negocios y personalización de los servicios.

Gracias a la tecnología, el bienestar social y medioambiental se convierte en realidad con este tipo de ciudades de la mano de la interacción. Ciudadano y medio ambiente convergen en un único actor gracias a la participación directa del primero en el mantenimiento y sostenibilidad del segundo.

En este punto todo gira alrededor del ciudadano, ya que es la propia persona quien decide qué quiere y cuándo lo quiere. Y gracias a esa participación ciudadana activa, se crea una verdadera consciencia del impacto ambiental.

Las Ciudades Inteligentes implican una Administración Pública más proactiva, flexible y adaptable, que mejora la capacidad de respuesta a las necesidades más complejas del ciudadano. Según las Naciones Unidades, el 70% de la población mundial vivirá en grandes ciudades en el 2050 ([46] Gonzalez, 2014).

La penetración de proyectos que se desarrollan en distintas ciudades de América Latina como Río de Janeiro (Brasil), Medellín, Bogotá, Barranquilla (Colombia) y Quito (Ecuador), están dando también pasos gigantescos hacia las ciudades inteligentes.

Aunque en Ecuador esta tendencia no está consolidada definitivamente Quito se encuentra entre las ciudades de América Latina consideradas de mayor crecimiento en la vinculación de la tecnología con la gestión pública, según el Smart Cities World Congress ([47] HOY digital, 2013).

Pilar Conesa, Directora de Smart Cities World Congress, indica que América Latina experimenta un boom de crecimiento de Ciudades Inteligentes en las que se conjuga el uso de la tecnología con temas de desarrollo sostenible.

2.7 Consideraciones de costos asociados a la implementación del internet de las cosas.

No se puede definir claramente un valor determinante para la implementación del IoT, ya que esta tendencia se define en diferentes sectores moviendo miles y miles de millones de dólares, aprovechando al máximo el sinnúmero de necesidades que se presentan diariamente por parte de los usuario quienes son los más beneficiados con las tecnologías que las grandes empresas desarrollan y entregan en un mercado consumido por la demanda tecnológica.

Los costos para la implementación del IoT, se pueden fijar de acuerdo a los alcances del mismo, ya que puede ir de dotarle de inteligencia a un determinado objeto que tiene un determinado fin, hasta la dotación de inteligencia a un sinnúmero de objetos dentro de un entorno que puede ser un cuarto, una vivienda, un barrio, una ciudad, una región o un país, con el fin de sacarles el mejor provecho posible.

2.7.1 ¿Cuánto cuestan los tags RFID?

El precio de un Tag es una función directa de sus prestaciones, características y el volumen a utilizar. Invengo ha estado ofreciendo inlays (UHF) basados en el

estándar General EPC 2 a menos de 10 centavos de dólar cada uno en Estados Unidos. El inlay puede ser usado para rastrear activos, o puede ser colocado dentro de una caja. Si es convertido en un tag, el costo se vería afectado en un aumento de aproximadamente el 100 por ciento.

Los inlays de alta frecuencia (HF) tienden a ser más caros, porque muchos tags HF tienen más complementos de avanzada y una estructura de antena más compleja. Los tags activos cuentas con una batería, por lo requieren de una carcasa plástica para contener sus componentes electrónicos y las batería. Es por ello que su costo parte alrededor de los USD5.00 cada uno.

El tipo de encapsulado aumentará el precio. Si se desea un tag activo que pueda soportar un horno en un proceso de manufactura durante un periodo de tiempo prolongado, o soportar químicos o materiales corrosivos, el alojamiento especial necesario para proteger el circuito y su batería incrementará el costo. Con los tags activos, otro factor de incremento en el costo es la duración requerida de la batería ([48] La Comunidad de RFID en Latinoamerica).

2.8 Sistema Operativo Contiki

El proyecto de Contiki OS se inició en el 2003, pero sus raíces se extienden al año 2000 cuando Dunkels como estudiante de informática en la Universidad de Mälardalen, trabajaba en un proyecto para utilizar sensores inalámbricos con el

objeto de rastrear los signos vitales de los jugadores de Hockey y mostrarlos en pantalla para que la multitud pudiera verlos ([49] TeknoPlof!, 2014).

Para hacer que todos aquellos sensores funcionaran correctamente, su mentor tuvo que escribir el software que les permitiera interactuar con una red informática. Denominó a aquel código resultante LwIP (que viene de pila Lightweight TCP/IP) y, aunque LwIP se sigue utilizando en muchos microcontroladores y otros productos actuales. Como LwIP no era lo bastante ligero en el 2003, creó microIP y, posteriormente, Contiki. El sistema operativo fue un éxito inmediato entre los investigadores y aficionados, y en los últimos años ha atraído a muchos usuarios comerciales con propuestas interesantes, como los instrumentos de detección de radiación Rad DX o los sistemas de monitorización del entorno Zolertia.

Contiki es un Sistema Operativo Open Source para para sistemas embebidos con escasa memoria, ver Figura 7. Cuenta con un núcleo orientado a eventos sobre el cual los programas pueden ser cargados y descargados de forma dinámica en tiempo de ejecución. Tiene un subsistema GUI opcional, con soporte de gráficos para terminales locales y para terminales virtuales en red mediante VNC o sobre Telnet. Incluye una pila ligera TCP/IP y una pila Rime, que está diseñada especialmente para comunicaciones inalámbricas de baja potencia, y cuenta con un amplio rango de primitivas de comunicación. También soporta IPv6, junto con protocolos como RPL4 y 6LoWPAN ([49] TeknoPlof!, 2014). Contiki permite a pequeños sistemas de baja potencia comunicarse con Internet.

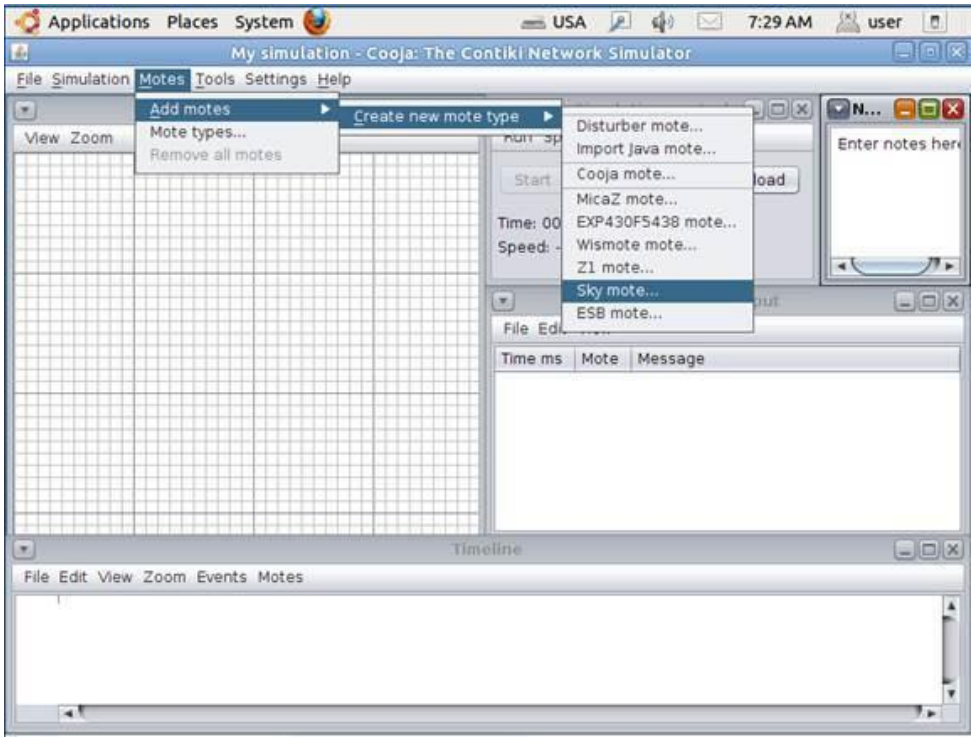


Figura 7: Interfaz del simulador de Contiki ([49] Préstamo, 2014)
Fuente: http://www.teknoplof.com

Contiki se utiliza actualmente en sistemas como sistemas de monitorización del nivel de ruido, medidores de energía eléctrica, control industrial, sistemas de alarma, sistemas de vigilancia remota de domótica, entre otros.

Entre sus principales alicientes como SO IoT:

- Basado en estándares:
  - Soporte IPv4 e IPv6
  - Soporte 6lowpan, RPL, CoAP

- Desarrollo sobre el OS muy rápido:
  - Aplicaciones escritas en C estándar.

- Simulador Cooja permite emular redes antes de desplegar en un Hardware.
- Instant Contiki ofrece un entorno de desarrollo completo.

- Soporte de hardware:
  - Brinda una tabla de plataformas de hardware en su árbol de código con los que se puede trabajar. Que se pueden encontrar en la página http://www.contiki-os.org/hardware.html

Contiki no es tan conocido como Windows, Linux o Mac OS, pero, desde hace más de una década, ha sido el sistema de referencia para hackers, académicos y empresas de dispositivos conectados a la red, como sensores, secuenciadores o sistemas de automatización basados en web. A los desarrolladores les encanta porque es ligero, muy maduro y, por supuesto, gratuito. Además, proporciona una base para programadores y emprendedores deseosos de traernos todos los aparatos conectados a la Red de redes, como el "Internet de las cosas" promete y sin tener que desarrollar un sistema operativo subyacente para esos gadgets en cuestión. Ver Figura 8.

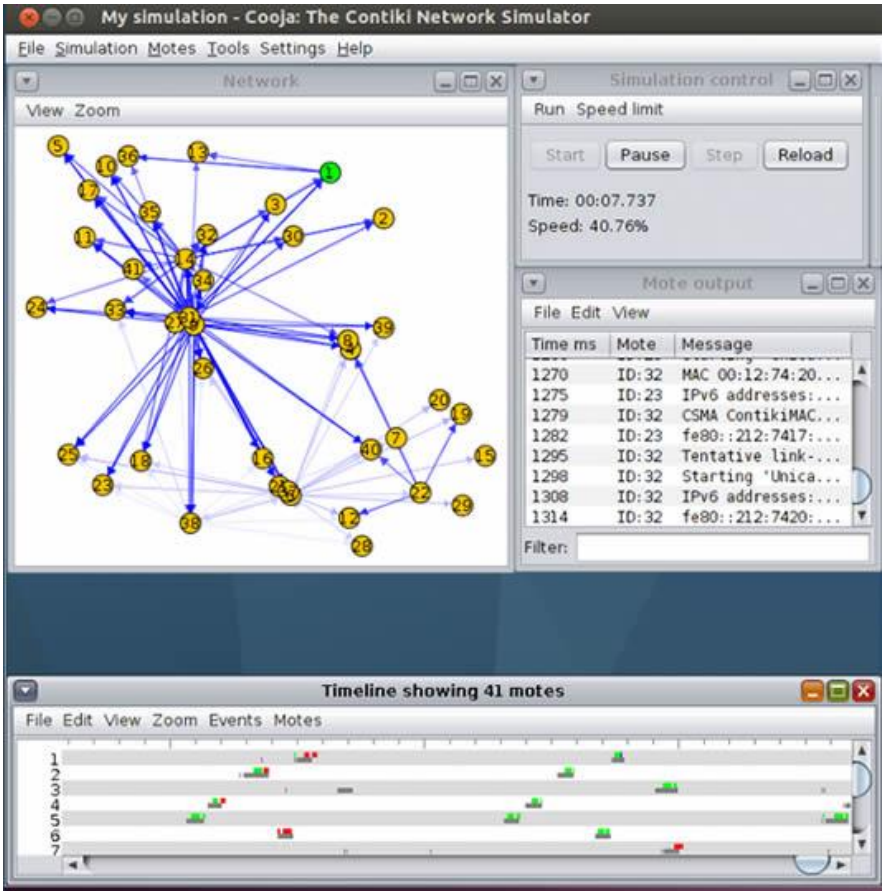


Figura 8: Simulación de sensores en Contiki ([50] Wikipedia)
Fuente: http://en.wikipedia.org/wiki/Contiki

CAPITULO III: MARCO METODOLÓGICO

3.1 Hipótesis

La hipótesis que se plantea en el presente trabajo es la siguiente:

- La seguridad y la privacidad serán factores favorables para la adopción del IoT.

3.2 Variables

3.2.1 Variable independiente:

- El Internet de la Cosas

3.2.2 Variable dependiente:

- Consideraciones de seguridad
- Esquemas de seguridad

3.3 Metodología

3.3.1. Tipo de investigación

El tipo de investigación asociado a este trabajo es la exploratoria por lo que permite examinar un tema poco estudiado y nos ayudará a familiarizarnos con fenómenos

desconocidos al mismo; y descriptivo porque nos permitirá analizar propiedades y características de los objetos para ser utilizados y mostrados en los esquemas.

3.3.2. Diseño de investigación

El diseño de la investigación se desarrollara en ciertas partes, análisis de la información, determinar niveles de seguridad en las diferentes capas, definir los costos asociados a la investigación, desarrollar esquemas para diseñar objetos inteligentes con niveles de seguridad aceptables y determinar los beneficios del proyecto.

3.3.3 Métodos de investigación

Los métodos utilizados en la investigación de este trabajo serán:

- Descriptivo
- Experimental

3.3.4 Técnicas e instrumentos de recolección de datos

Se utilizó las siguientes técnicas e instrumentos para la obtención de los datos:

- Investigación Bibliográfica.
- Investigación en Internet.
- Observación.
- Entrevistas

- Análisis.

3.4 Plan recolección de la información

Para la recolección de información se llevó a cabo una exhaustiva búsqueda de recursos bibliográficos (revistas, libros, artículos) de internet, además de la observación de videos sobre debates sobre temas de seguridad del Internet de las Cosas.

Además se desarrolló una entrevista con preguntas abiertas donde se plantearon temas sobre las seguridades en los objetos, las mismas que fueron realizadas a profesionales involucrados en el área tecnológica.

Se consideraron también entrevistas realizadas por algunos medios internacionales a profesionales de otros países que están directamente relacionados e investigando esta tendencia.

3.5 Plan de procesamiento y análisis de la información.

Se realizó un análisis de la información relevante en la adopción del IoT y los niveles de seguridad que se están considerando, con el fin de poder desarrollar la propuesta de la mejor manera posible.

Para ello se consideró realizar lo siguiente:

- ✓ Recolección de información
- ✓ Registrar las fuentes de información
- ✓ Procesamiento de la información recabada.

- ✓ Análisis e interpretación de las entrevistas realizadas.
- ✓ Plasmar los esquemas propuestos.
- ✓ Establecer las conclusiones y recomendaciones.

CAPITULO IV: MECANISMOS DE SEGURIDAD EN EL INTERNET DE LAS COSAS

4.1 Análisis de información determinante a la seguridad

Desde hace algún tiempo se ha venido hablando de ciertos puntos de lo que involucra el Internet de la cosas, en los cuales han dado como resultado la publicación de artículos, libros, ponencias, debates, entre otros, que han permitido a los involucrados con las nuevas corrientes tecnológicas aprovechar las oportunidades que brinda el Internet de las cosas.

Es cierto que el Internet de Todo como lo denomina Dave Evans en la página de Cisco es una nueva evolución del Internet de las Cosas ([51] Evans), es la reunión de personas, procesos, datos y cosas para hacer conexiones en red más relevantes y valiosas que nunca, convirtiendo la información en acciones que crean nuevas capacidades, experiencias más ricas, y oportunidades económicas sin precedentes para las empresas, los individuos y los países.

En una ponencia brindada por Jesús Ranz ([52] Centro Nacional de Tecnologías de la Accesibilidad - CENTAC, 2013), determina una combinación M2M + Internet = Internet de las Cosas. De esta unión nacen las granjas inteligentes, casas inteligentes, edificios inteligentes, ciudades inteligentes, autos inteligentes, etc. Pero así mismo expone los retos que se presentan para la adopción de esta tecnología son:

estandarización, redes de acceso de muy bajo costo, seguridad, recolección de energía para alimentar los sensores, privacidad, protocolos wireless más eficientes y un diseño nuevo de comunicación en el internet.

Alvaro Everlet y Javier Pastor de la empresa Carriots ([53] Universidad Rey Juan Carlos, 2014), definen que para que un objeto sea inteligente, se le debe de dotar de un poco de electrónica y conectarlo al internet, para explotar en si la definición de un objeto que solo esté conectado a internet, si no que aparte se pueda alimentar autónomamente con los datos recabados y pueda interactuar por sí mismo.

Para construir un proyecto de IoT se requiere lo siguiente:

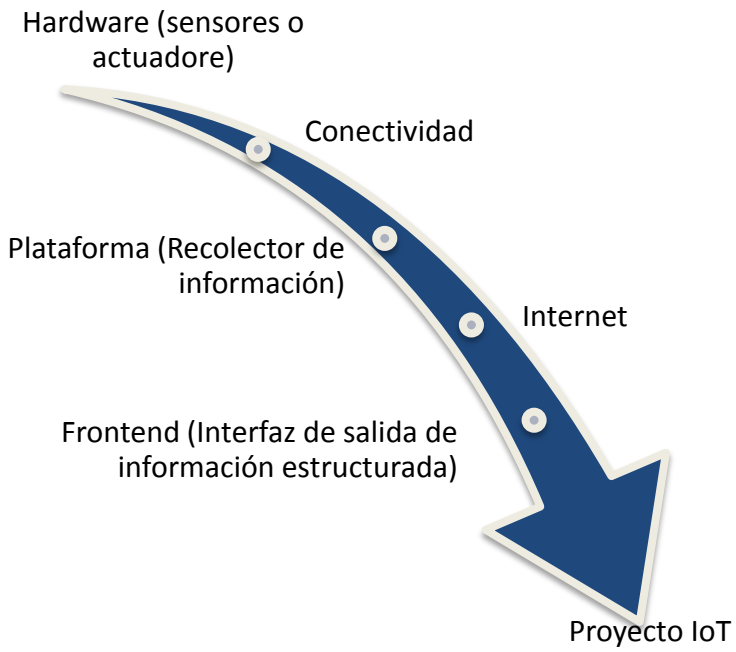


Figura 9: Componentes para un proyecto de IoT
Fuente: Diseño elaborado por Autor

Los dispositivos esta definidos por los sensores o actuadores, la conectividad que puede ser autónoma, dispositivo + pasarela y red de sensores, y los protocolos de comunicación. La plataforma donde se especifican las APIs Rest (aplicaciones orientadas a internet), almacenamiento Big Data, gestión de dispositivos, lógica de negocio, seguridad, logs y debugs.

En un debate realizado por HangoutON dirigido por Antonio Postigo y Yolanda Corral ([54] HangoutON, 2014), y en el cual reunieron a un selecto número de profesionales involucrados en este ámbito, se manifestó que en muy pocos años habrá millones y millones de objetos cotidianos conectados a Internet. Estamos hablando de objetos como electrodomésticos, vehículos, ropa, complementos. Que serán inteligentes y que estarán conectados entre sí, pudiendo ser controlados desde un dispositivo con conexión a Internet a miles de kilómetros, algo que cambiará nuestro día a día y que conllevará la ingente proliferación de datos y una vuelta más de tuerca al tema de la privacidad y la seguridad en red.

Se trataron temas referentes a la privacidad de las personas, en el cual hicieron énfasis en que cualquier persona puede desarrollar prototipos básicos con sensores accesibles a bajo costo y utilizando un sistema de desarrollo como Arduino para darle programación a las placas, el mayor reto de ello es desarrollar plataformas de administración que permitan gestionar dichos dispositivos de manera segura.

Javier Pastor hablo sobre la plataforma Carriot que fue diseñada para la administración de dispositivos inteligentes, el mismo que genera una API Key para cada usuario que le permite tener un único acceso a los datos gestionados por los sensores ([54] HangoutON, 2014).

Kevin Astón manifiesta que lo que se busca con el IoT es hacer las cosas más eficientes, traer el poder del internet al mundo real, que no solo las cosas se comuniquen maquina a máquina M2M sino también con las personas M2P ([55] Oppenheimer, 2014).

¿Qué pasaría si los sensores no hacen lo que el usuario desea? Fue una de las preguntas que lanzo Andrés Oppenheimer ([55] Oppenheimer, 2014), Astón manifestó que sucedería si no existiera el IoT, por lo que hay que determinar qué tipo de información se está recolectando para determinar los sistemas de información que van a manejar esos datos recolectados, los sensores se pueden romper en cierto momento, pero hay que preparar acciones para que esto no suceda, por lo general dice que en el lugar donde está el mayor riesgo de seguridad existe no es en el sensor si no que en el software que lo administra. Para preparase para esto se debe ahondar más en la parte del tratamiento de la información, la que se denomina Ciencia de la Información.

¿Qué sucede con los hacker?, Astón manifiesta que los nuevos problemas necesitan nuevas tecnologías para poderlos resolver, considerando las soluciones que se han dado en el pasado con otros fallos de seguridad. Nuestro mundo está cambiando,

debido a las pequeñas comodidades que se están dando en nuestro mundo en relación al IoT, lo que habrá una revolución.

Jordi Botifoll respondió sobre ¿Cómo va a mejorar nuestra vida el IoT?, indicó que la vida es tiempo y hay que saberla aprovechar. En relación a la seguridad dice que cada vez más se desarrollan software que va a gestionar y minimizar los errores, y que toda innovación tiene cosas positivas y negativas, por lo que las negativas a la larga se van a ir minimizando ([55] Oppenheimer, 2014).

Cito que la ciudad de Barcelona de España ha sido considerada como una de las ciudades más innovadoras de Europa, donde existe tecnología inteligente que permite tener un ahorro energético del 30%, al haber luminarias en las vías públicas que solo se encienden cuando existen circulación de personas en las horas nocturnas. También existen otros proyectos innovadores como lo son la gestión de tráfico (parque, semáforos, trasporte público), tratamiento de reciclaje de basura.

Silvina Moschini indicó que toda evolución va a tener un poquito de cada cosa, pero sin olvidar los riesgos asociados ([55] Oppenheimer, 2014).

Ariel Coro identifica un gran problema de seguridad las cuales crean desconfianza en la adopción de estas tecnologías, como es el caso de soporte para ciertos equipos que se descontinúan y dejan de sacar actualizaciones para parchar vulnerabilidades de los sistemas de los objetos ([55] Oppenheimer, 2014).

El Ing. Darwin Celorio Jefe de Sistemas de Banco Comercial de Manabí, en una entrevista realizada a él, manifiesta que las seguridades que se deben implementar son encriptación de los datos para protegerlos, manejo seguro de los certificados y claves, los objetos deben estar estandarizados para garantizar esto ([56] Celorio Lucas, 2014).

Las empresas tanto públicas como privadas actualmente se están interesando por ofrecer mejores servicios acompañados con la tecnología, por lo que en ciertas empresas o instituciones existen departamentos únicos encargados de investigar e implementar soluciones inteligentes que ayuden a mejorar los servicios.

El Ing. Vinicio Bucheli López Director de Informática del Gobierno Autónomo Descentralizado del Cantón Portoviejo, dice que las seguridades que se deben de considerar dependerán del objeto a administrar, y existe un sinnúmero de seguridades que se pueden implementar, como seguridades perimetrales, VPN, entre otros. Las empresas para generar confianza en los clientes dependerán de mucho del nivel de cultura que exista, además de que las empresas tengan una trayectoria y experiencia dentro de este campo ([57] Bucheli López, 2014).

Considerando el punto anterior el Ing. Rodney Castellanos, considera una conjugación de seguridad de hardware y software, hay que ver la criticidad del sensor que se está manejando, se ve a los dos niveles como muy importantes y de alta prioridad para aplicar niveles de seguridad aceptables ([58] Castellanos, 2014).

Se deben tener plataformas en las cuales se considere una seguridad de un 99,999%, que permitan tener confianza en la adopción del internet de las cosas, estas plataformas juegan un papel muy importante en esta adopción.

Más que las seguridades en las redes lo que considera en tener la disponibilidad de la red, las seguridades se deberían aplicar a nivel de hardware o software que permitan colocar equipos o sistemas de criptografía, de control de permisos, accesos, generación de claves. Esto permite asegurar los datos por la red y aunque los datos sean interceptados estos no sean descifrados.

Hemos revisado algunos puntos importantes, pero al igual de lo analizado partiremos de una base muy significativa que es un proyecto donde proponen las Consideraciones de seguridad para el Internet de las Cosas basada en IP, donde nos muestran una visión sobre la utilización de los protocolos IP para la comunicación entre las personas-objetos o de objetos-objetos ([59] Jayavardhana, Rajkumar, Slaven, & Marimuthu, 2013). Sin duda es un punto de partida para poder definir los esquemas específicos para la creación de objetos seguros.

4.1.1 Análisis FODA

FORTALEZAS	DEBILIDADES
❖ Detección Ubicua. ❖ Aumento de la productividad. ❖ Velocidad y precisión de la información. ❖ Capacidad de afectar objetivamente el entorno del mundo físico. ❖ Mejoramiento de la calidad de vida. ❖ Experiencias ya vividas de soluciones a problemas anteriores.	❖ Entorno amplio de ataque Ej.: datos, sensores, sistemas, dispositivos). ❖ Potencial introducción de incertidumbre debido al alto volumen de datos. ❖ Difusión de datos a través de múltiples dominios. ❖ Poca de concienciación sobre la falta de seguridad con objetos conectados.
OPORTUNIDADES	**AMENAZAS**
❖ Eficiencia operativa en tiempo real. ❖ Crecimiento de los ingresos económicos. ❖ Nuevas funcionalidades. ❖ Control constante para entornos en riesgo. ❖ Nuevos campos de desarrollo de tecnología. ❖ Crear soluciones a partir de problemas anteriores.	❖ Modalidad de ataques no anticipados. ❖ Inmaduro conocimiento sobre la seguridad en IoT. ❖ Robo o alteración de información confidencial. ❖ Falta de estándares y normativas para crear objetos IoT seguros.

Tabla 1: Análisis FODA
Fuente: Elaborado por Autor

4.2 Niveles de seguridad

Los objetos y los sistemas con los que el ser humano interacciona: su teléfono, el termostato de la calefacción, el coche, la llave de la puerta, la cámara de video, el receptor de TV, el sistema GPS, entre otros, ahora pueden ser controlados a través de la Web. El usuario podrá interrogar el estado de los sistemas y objetos y a su vez podrá recoger información de los eventos que estos objetos envíen a la red como consecuencia de una alteración o modificación de las variables físicas que están midiendo o controlando.

En este parte identificaremos los niveles de seguridad que existe en ciertos objetos más comúnmente que se encuentran conectados al internet, a nivel de hardware, software, red y la nube, ver Figura 10.



Figura 10: Objetos conectados ([60] Vargas, 2013)
Fuente: http://www.cabume.co.uk

4.2.1 Seguridad a nivel de hardware

Al hablar de seguridad a nivel de hardware estamos considerando el acceso físico a los equipos que comúnmente están conectados a Internet o red interna que genera algún tráfico de información y que de una u otra forma están enviando datos a un determinado repositorio que con una aplicación vinculada es el encargado de administrar la información recabada por los objetos, y ser utilizados para un fin correspondiente.

En el momento en que un objeto se vuelve parte de un entorno interconectado, es necesario considerar que estos dispositivos han perdido seguridad física, ya que posiblemente se encontrarán localizados en entornos inhóspitos y serán accesibles al instante por individuos con malas intenciones. Los atacantes podrían interceptar, leer o modificar información, y podrían manipular sistemas de control y modificar la funcionalidad ([61] CIO América Latina, 2013).

El mayor temor es que los usuarios de dispositivos IoT no tomarán en cuenta la seguridad de los objetos como una preocupación mayor. El problema es que el ancho de banda de un dispositivo comprometido puede ser utilizado para atacar a terceros, por lo que el IoT creará nuevos retos de seguridad para las empresas ([61] CIO América Latina, 2013).

La seguridad en este nivel se la considera como de una forma especial ya que no se puede comparar los niveles de seguridad a nivel de hardware en las pequeñas,

medianas, grandes empresas o a nivel de usuarios independientes no están al mismo nivel, ya que en base a la información que estos manejen, no aplican los mismos niveles de acceso a dichos objetos, pero sobre los cuales se deberá tener un control que permita que los mismos no sean manipulados por personas ajenas a los intereses de los usuarios o empresa.

Para el caso de las empresas la seguridad física se torna más ardua, puesto que los sistemas informáticos suelen estar cercanos al usuario final o al mismo administrador, por lo que están expuestos a un mayor peligro de mal uso o uso malintencionado. Aquí no podemos confiar plenamente en el cumplimiento de políticas o normativas de uso de las máquinas y como estas máquinas están más expuestas a intrusos ajenos al personal de la empresa que hayan superado los controles de acceso de niveles superiores debemos configurar estas máquinas y dispositivos de red de forma que sea lo más complicado posible el realizar manipulaciones sobre ellos, tanto a nivel físico como a nivel informático siempre que sea posible ([62] López Hernández, 2004).

Para el caso de los usuarios que utilizan dispositivos de uso personal por ejemplo un Smartphone para monitorear el estado de una vivienda inteligente por medio de acciones enviadas por el dispositivo, deberá considerar que en algún momento de pérdida o sustracción de dicho dispositivo de monitoreo y control las alternativas que permitan inmediatamente cambiar los accesos correspondientes para el control y monitoreo de los objetos de la vivienda.

La seguridad en el hardware para los objetos inteligentes se deberá considerar en la estructura del producto de una manera que permita la integridad del mismo y que no admita la manipulación directa en el caso de tener acceso a los mismos. Ejemplo una tarjeta inteligente deberá tener características físicas y un grado de protección contra agentes externos con el fin de que no sea fácilmente manipulable.

4.2.2 Seguridad a nivel de software

Una vez visto como el entorno de nuestro sistema puede verse comprometido por la falta de Seguridad Física, resulta significativo indicar que la gran parte de daños a un centro de datos, no será sobre la infraestructura física sino contra información que se almacena y se procesa en el mismo.

La Seguridad Física, sólo es una parte del amplio espectro que debe ser cubierto. Hay que tener claro que el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Por lo que es aquí donde entra la Seguridad Lógica a formar parte del amplio espectro que se tiene.

Es decir que la Seguridad Lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo ([63] Borghello).

Los objetivos que se plantean serán:

1. Restringir el acceso a los programas y archivos.
2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
3. Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
5. Que la información recibida sea la misma que ha sido transmitida.
6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
7. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Habitualmente los usuarios finales no tienen en consideración la seguridad cuando hacen uso de un sistema, ya que, frecuentemente se ignoran los aspectos relacionados con la seguridad. De igual forma, estos aspectos a veces pueden considerarse una molestia, ya que la seguridad suele ir en el platillo opuesto de la comodidad y facilidad de uso en la balanza del diseño de un sistema. Es por esto que los usuarios a veces puedan tener una imagen negativa de la seguridad, por considerarlo algo molesto y que interrumpe su capacidad de realización de un trabajo determinado. En un entorno seguro, un usuario se encuentra con tareas que le pueden resultar incómodas como por ejemplo, recordar contraseñas, cambiarlas periódicamente, etc.

y que pueden limitar las operaciones que puede realizar así como los recursos a los que se le permite acceder ([64] Ferrer & Fernández).

Sin embargo, la seguridad es fundamental a la hora de afrontar tareas que se realizan en sistemas informáticos ya que son las únicas medidas que pueden garantizar que éstas se realicen con una serie de garantías que se dan por sentado en el mundo físico. En el mundo intangible de la informática, tan cerca de un servidor están sus usuarios legítimos como los usuarios que hacen uso de la misma red de comunicaciones. Es más, estos usuarios, en el caso de una red global, se cuentan por millones. Algunos serán buenos vecinos pero otros serán agentes hostiles que trataran de causar el mayor daño posible violando la integridad del software ([64] Ferrer & Fernández).

4.2.2.1 Fallos de seguridad en la utilización del software

Los fallos de seguridad del software que se pueden dar en base al análisis realizado en el documento publicado por Jorge Ferrer y Javier Fernández sobre la Seguridad Informática y Software Libre ([64] Ferrer & Fernández). Se los agrupa de la siguiente manera:

1. Fallos debidos a errores desconocidos en el software, o conocidos sólo por terceras entidades hostiles.
2. Fallos debidos a errores conocidos pero no arreglados en la copia en uso del software.

3. Fallos debidos a una mala configuración del software, que introduce vulnerabilidades en el sistema.

Cada uno identifica un tipo de vulnerabilidad, el primero se puede atribuir a la calidad del código, el segundo a la capacidad y rapidez de arreglo de los errores descubiertos en el código por parte del proveedor del mismo y a la capacidad del administrador de recibir e instalar nuevas copias del software actualizado. El tercer tipo darse a una falta de documentación del software o una falta de formación adecuada de los administradores para hacer una adaptación correcta del mismo a sus necesidades.

Los fallos descritos anteriormente pueden producir un mal funcionamiento del programa, por lo que es necesario considerar lo siguiente:

- Pueden implementarse algoritmos de forma incorrecta lo que puede llevar a una pérdida de seguridad por ejemplo, un algoritmo de generación de claves que no se base en números totalmente aleatorios.
- Pueden diseñarse servicios que, en contra de sus especificaciones, ofrezcan funcionalidades no deseadas o que puedan vulnerar la seguridad del servidor que los ofrezca.
- Pueden no haberse tomado las medidas necesarias para asegurar el correcto tratamiento de los parámetros de entrada, lo que puede hacer que un atacante externo abuse de ellos para obligar al programa a realizar operaciones indeseadas.

4.2.3 Seguridad en la red

Las tecnologías de seguridad de red protegen su red contra el robo y el uso incorrecto de información confidencial de la empresa y ofrecen protección contra ataques maliciosos de virus y gusanos de Internet. Sin ningún tipo de seguridad en red, su empresa u objetos conectados se enfrenta a intrusiones no autorizadas, periodos de inactividad de red, interrupción del servicio, incumplimiento de las normativas e incluso a acciones legales.

Cómo funciona la seguridad.- La seguridad de red no se basa en un método concreto, sino que utiliza un conjunto de barreras que defienden a la empresa de diferentes formas. Incluso si falla una solución, se mantendrán otras que protegerán y en especial los datos de una gran variedad de ataques a la red ([65] Monzon, 2012).

Las capas de seguridad de su red garantizan que tenga a su disponibilidad la información importante en la que se basa para dirigir su negocio y que estará protegida de las diferentes amenazas. Específicamente, la seguridad de red:

- Ayuda a proteger la red de ataques internos y externos. Las amenazas se pueden originar tanto dentro como fuera del cortafuegos de una empresa. Un sistema de seguridad efectivo supervisa toda la actividad de la red, detecta el comportamiento malicioso y adopta la respuesta apropiada.

- Permite garantizar la privacidad de todas las comunicaciones. Los empleados o usuarios pueden acceder a la red desde cualquier lugar o mientras se desplazan con la garantía de que sus comunicaciones serán privadas y estarán protegidas.
- Controla el acceso a la información mediante la identificación exhaustiva de los usuarios y sus sistemas. Las empresas pueden establecer sus propias reglas de acceso. La denegación o la aprobación se puede otorgar según las identidades de los usuarios, la función del trabajo u otros criterios específicos de la empresa.
- Le hará más fiable. Puesto que las tecnologías de seguridad permiten a su sistema evitar ataques conocidos y adaptarse a las nuevas amenazas, los empleados, clientes y socios comerciales pueden confiar en que su información estará segura.

La seguridad a nivel de usuario final quien es el que hace uso de los objetos inteligentes no la tendrá muy en cuenta, pero la empresa que brinda el servicio con un determinado objeto o aplicación y que trasmitirá información por la red si deberá determinar las seguridades respectivas ya que por ese medio puede causar algún daño ya sea al usuario por alguna alteración de los datos enviados o a la empresa en general quien es la que administra y almacena toda la información.

Actualmente sólo el 1% de los dispositivos están conectados a Internet, por lo que los consumidores de igual forma deberán considerar los siguientes puntos para su seguridad en la red ([66] Alberca Jaquero, 2014):

- Todo dispositivo que esté conectado a Internet es susceptible de ser accedido, y por tanto, deberá ser protegido.
- Deberían desarrollarse estándares de seguridad de fabricación de dispositivos con conexión a internet para que todos los fabricantes puedan seguirlos.
- Cualquier dispositivo que venga configurado con una contraseña por defecto deberá ser cambiada siguiendo unas reglas de complejidad mínimas.
- El fabricante puede diseñar un dispositivo para ser seguro, pero en última instancia dependerá del usuario protegerlo y asegurarse de que es inaccesible; por ejemplo, accediendo a la web del fabricante para descargarse las actualizaciones del dispositivo que cubran vulnerabilidades detectadas.
- Conocer nuestros derechos y obligaciones en relación a la privacidad y protección de nuestros datos personales.

En la actualidad el perímetro de las redes crecen para dar paso a redes LTE y 4G de alta velocidad, puntos de acceso inalámbricos, sucursales, oficinas domésticas, usuarios itinerantes, servicios en la nube y terceros que acceden a las aplicaciones y a los datos para proporcionar servicios. Estos cambios en el tamaño, el alcance y la superficie de las redes pueden generar errores en las configuraciones y los controles que, a su vez, den lugar a infracciones de la seguridad. Por eso, es recomendable utilizar soluciones de seguridad que se puedan implementar de manera uniforme en todos los dispositivos y puntos de las infraestructuras. Así también, es necesario disponer de una administración centralizada para poder monitorear los cambios de

las infraestructuras elásticas y las diferentes capas de seguridad de las estaciones de trabajo.

4.3.4 Seguridad en la nube

Cada vez más empresas de todos los tamaños están empezando a adoptar servicios en la nube tales como software como servicios (SaaS), infraestructura como servicio (IaaS) y plataforma como servicio (PaaS). Un marco conceptual de integración de los dispositivos sensores ubicuos y las aplicaciones se muestra en la Figura 11. Con el fin de aprovechar todo el potencial de la computación en la nube, así como de detección en todas partes, un marco combinado con una nube en el centro parece ser más viable ([59] Jayavardhana, Rajkumar, Slaven, & Marimuthu, 2013).

Esta tendencia representa un gran reto para la seguridad de las redes, ya que el tráfico puede circunvalar los puntos de inspección tradicionales. Además, a medida que aumenta el número de aplicaciones disponibles en la nube, los controles de las políticas para las aplicaciones web y los servicios en la nube deberán experimentar la evolución correspondiente.

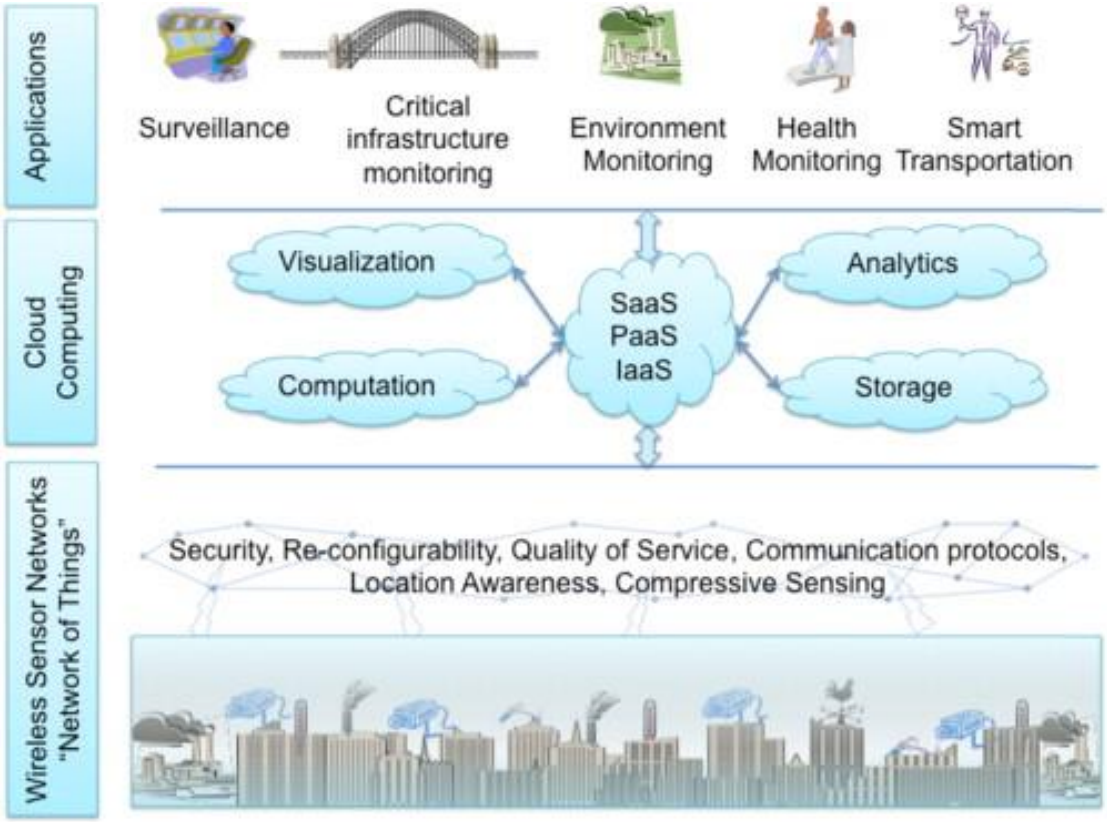


Figura 11: Marco conceptual IoT con Cloud Computing en el centro ([59] Jayavardhana, Rajkumar, Slaven, & Marimuthu, 2013)
Fuente: http://www.sciencedirect.com/science/article/pii/S0167739X13000241#

Las tecnologías de almacenamiento en la nube en los últimos años han experimentado un crecimiento considerable en lo que respecta al número de usuarios finales y empresas que la utilizan, actualmente hay un alto uso de la nube en comparación de medio tradicionales como el uso de DVD, CD, USB, entre otros; esto se debe a su gran ventaja que tiene la nube porque permite el fácil acceso a la información desde cualquier lugar, lo cual ha hecho de esta tecnología cada vez más popular. Gartner aseguró que sólo el 7% de contenido de los consumidores se almacena en la nube en 2011, pero esta cifra crecerá a 36% en 2016 ([67] Gartner, Inc., 2012).

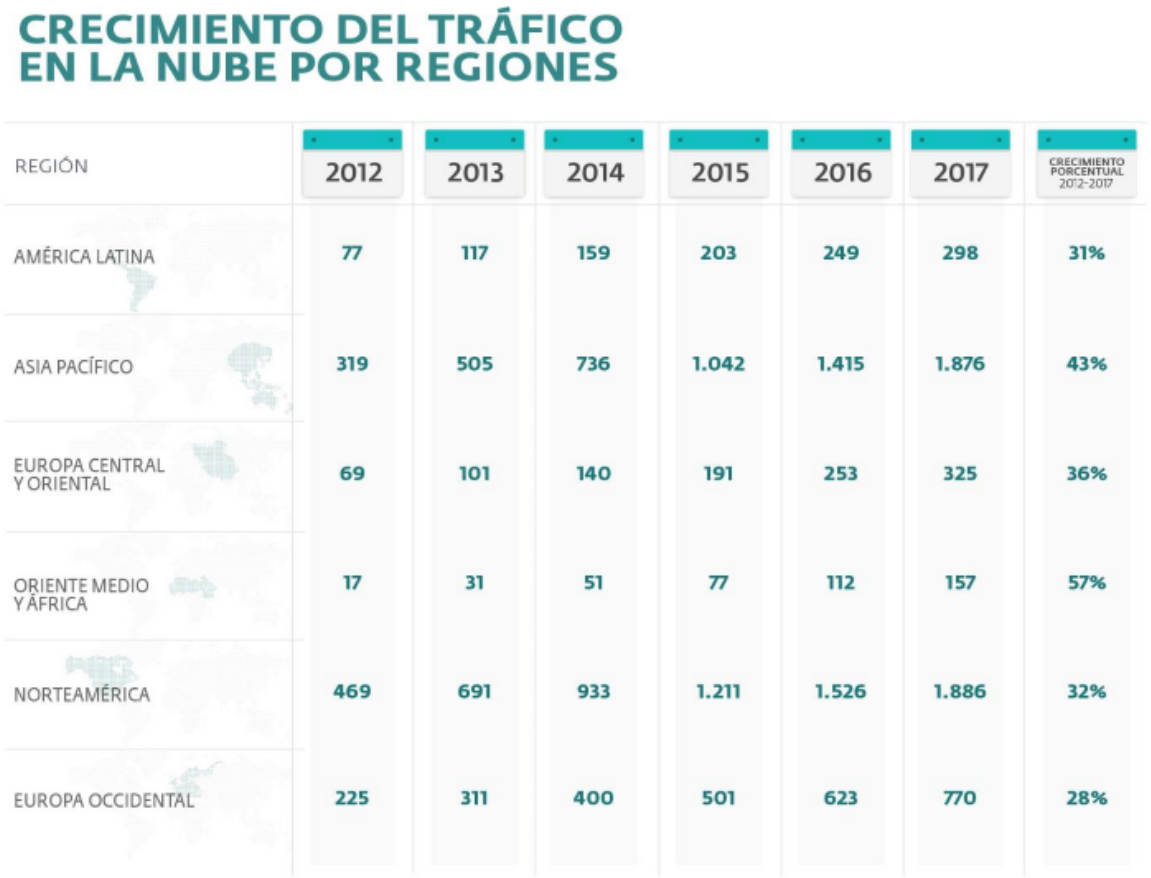


Figura 12: Crecimiento del tráfico en la nube por regiones (expresados en exabytes) ([68] ESET Latinoamérica, 2014)
Fuente: www.eset-la.com

En un informe realizado por el Laboratorio de Investigación de Eset Latinoamérica denominado Tendencias 2014: El desafío de la privacidad del internet, muestra una tabla donde se ve el crecimiento de tráfico en la nube por regiones, ver Figura 12; claramente determina un crecimiento de esta tendencia, más específicamente en América Latina donde se ve un crecimiento porcentual del 31% para el 2017. Pese al incremente y a las ventajas que le brinda a los usuarios es importante considerar que esta tecnología no está exenta de riesgos asociados a la seguridad de la información.

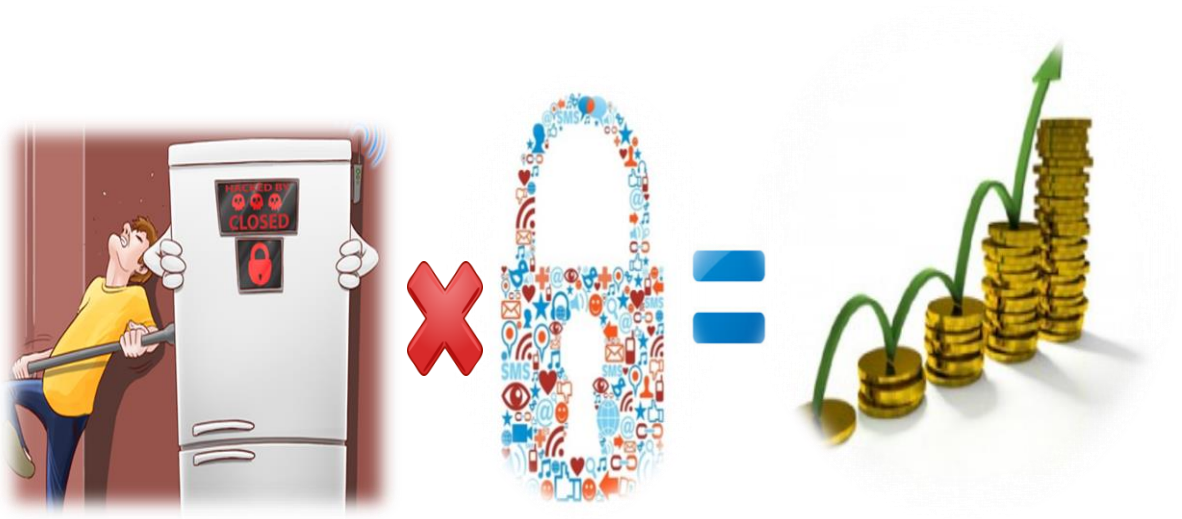
Se debe realizar un análisis cuidadoso sobre, ¿qué servicios puede utilizar cada usuario? ¿Quién debe tener permiso para publicar datos y quién puede leerlos

solamente? Aunque los servicios en la nube están desarrollando sus propios modelos de seguridad, deberán mantener cierta armonía con las estrategias de las empresas para evitar la proliferación de problemas con las contraseñas, los permisos y las infraestructuras de seguridad. La nube ofrece grandes oportunidades, pero la seguridad de las redes debe evolucionar al mismo ritmo ([69] Lyne, 2011).

4.3 Costos asociados a la seguridad de los objetos

Es difícil precisar los costes asociados a aportar seguridad a un objeto inteligente. Hay que partir de una base, es decir la seguridad debe incluirse en el proceso de diseño del mismo, por poner un ejemplo en el diseño, construcción y puesta en marcha de un vehículo, se consideran varios niveles de seguridad que la empresa considera y que permitirá al conductor y sus ocupantes andar seguros por las vías y protegerse en caso de cualquier accidente inesperado, esto lo realizan antes de sacar al mercado el producto, lo mismo se debe aplicar para los objetos que van a estar conectados a internet ([70] Medina, 2014).

Si creamos un dispositivo, pongamos otro ejemplo un televisor, sin tener en cuenta la seguridad del software y hardware incluidos, dar una solución de seguridad en base a una vulnerabilidad que se descubra posteriormente puede ser muy caro, porque puede suponer, en el mejor de los casos, una actualización de software, y en el peor el reemplazo de algún componente hardware e incluso el dispositivo completo. Ver Figura 13.



Vulnerabilidad de seguridad del objeto *Costo de seguridad* *Aumento de costos*

Figura 13: Relación entre costo y seguridad de los objetos, costos altos.
Fuente: Elaborado por Autor

La seguridad después de descubrir un fallo siempre es más cara, porque no afecta siempre a todos los dispositivos ni del mismo modo y puede repercutir en otros.

Si la seguridad se implementa en la fase de control de calidad, por ejemplo con herramientas de análisis de código seguro que impidan que el producto salga a la calle con vulnerabilidades conocidas, el coste es mínimo, porque un diseño del software para millones de dispositivos divide el coste entre estos con la fórmula:

Coste Seguridad / Nº Dispositivos

Si al mismo tiempo, en la fase de diseño, se diseña un sistema de actualizaciones sencillo y constante, será más fácil resolver vulnerabilidades que se descubran en el

futuro. En la Figura 14 se muestra como los costos se reducen en la fase de producción de los objetos.

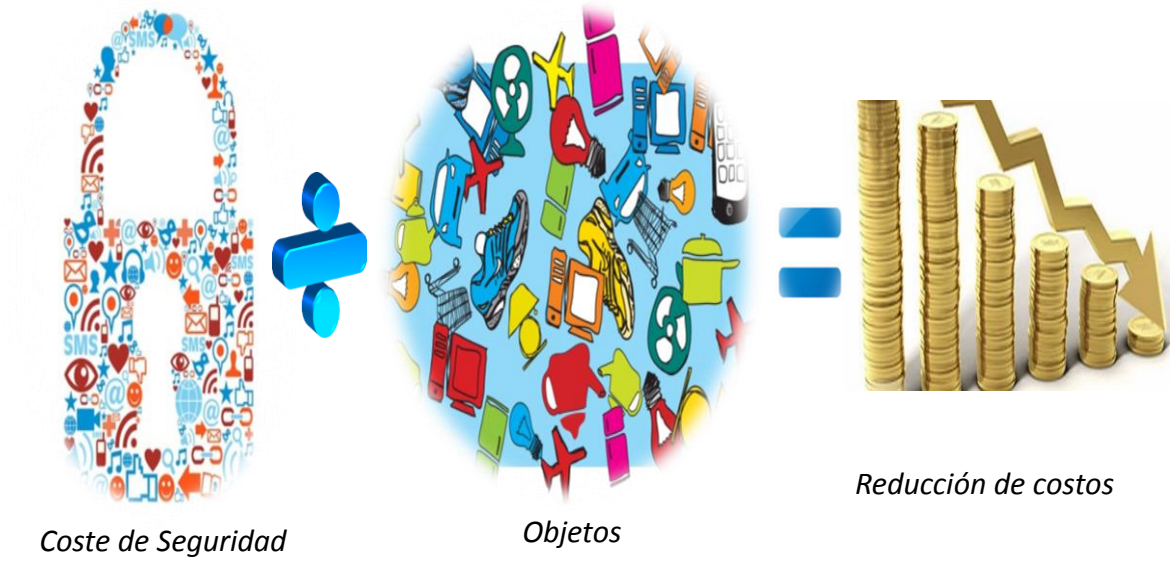


Figura 14: Relación entre costo y seguridad de los objetos, costos bajos.
Fuente: Elaborado por Autor

Eso sin olvidar la obsolescencia programada, y es que muchos fabricantes además de no diseñar estos dispositivos con la seguridad de serie, dejan de actualizarlos al poco tiempo de salir al mercado, o lo que es peor, los que se basan en sistemas operativos abiertos, como Android, no implementan las nuevas versiones hasta meses después de que estén liberadas.

En cualquier caso, la seguridad como diseño es más económica que la seguridad como reacción a un problema.

4.3.1 Análisis de costos

Para realizar un análisis de costos que implica dotar de seguridad a un objeto o a un entorno IoT, debemos partir de preguntas como ¿Qué recursos se quieren proteger?, ¿De qué personas necesita proteger los recursos?, ¿Qué tan reales son las amenazas?, ¿Qué tan importante es el recurso?, ¿Qué medidas se pueden implantar para proteger sus bienes de una manera económica y oportuna?, que permitan definir que recursos valen la pena proteger y justificar su costo ([71] Borghello).

Cristian Borghello Director de segu-info página web que brinda información de seguridad informática, define claramente en su blog tres costes fundamentales:

1. **CP:** Valor de los bienes y recursos protegidos.
2. **CR:** Costo de los medios necesarios para romper las medidas de seguridad establecidas.
3. **CS:** Costo de las medidas de seguridad aplicadas.

A partir de esto se representa con la siguiente relación:

$$\mathbf{CR > CP > CS}$$

En donde los costos para romper las medidas de seguridad establecidas en los objetos o en un entorno IoT deben ser mayores que el valor de los bienes y recursos

protegidos, esto conlleva a que los atacantes busquen formas menos costosas de romper las seguridades.

Así mismo el valor de los bienes y recursos protegidos debe ser mayor que los costos de las medidas de seguridad aplicadas, esto implica que los bienes o recursos a proteger su valor deben ser mucho más altos que los que implican establecer las medidas de seguridad.

Por poner un ejemplo, podemos definir a un objeto en este caso un sensor de proximidad de vehículo para evitar colisiones, si nos ponemos a analizar este caso está expuesto a muchos riegos, y los costos de las medidas de seguridad son altos.

Analizando el valor del bien o recurso a proteger, es decir no solo veamos al sensor como algo independiente sino que se ve como un conjunto acoplado a un vehículo con el fin de asegurar la vida de las personas que van dentro de él y las que se encuentran en su entorno, por lo que su valor seria alto. Basémonos en un rango del 1% al 15% para considerar los costos CR y CS.

Entonces si definimos el valor del bien o recurso a proteger es alto y sin omitir ningún costo se lo define con un valor de $1000, esto variara dependiendo del objeto o recurso y en el entorno donde estarán expuestos; ahora bien, considerando los costos de las medidas de seguridad que requiere el objeto para que no sea vulnerable se le asigna un valor de 10% ($100) considerando que tiene un nivel promedio de

seguridad de 27 puntos, y por último los costos que implican romper las seguridades implementadas por parte de los atacantes se le asignara el valor de 15% ($1150).

Aplicando la relación de costes tendríamos algo así:

CR=1150 > CP=1000 > CS=100

Podríamos considerar que el valor del bien justifica el costo que implica dotar de seguridad al objeto, y si la seguridad se aplica en conjunto a los dispositivos, los costes que incurren para asegurar el objeto serían menores.

En la Figura 15 se puede ver también el punto de equilibrio que debe existir, es decir, aplicando el ejemplo propuesto existe un nivel de seguridad de 27 puntos esto se define en base a los riesgos que existen para un determinado recurso, y el costo al aplicar medidas de seguridad es del 10% del valor del bien, y los costos de romper esas seguridades suman el 15% más del valor del bien.

Así mismo se observa que los riesgos disminuyen al aumentar la seguridad pero como es lógico los costos tenderán al infinito sin lograr el 100% de seguridad, por lo que nunca se logrará no correr algún tipo de riesgo.

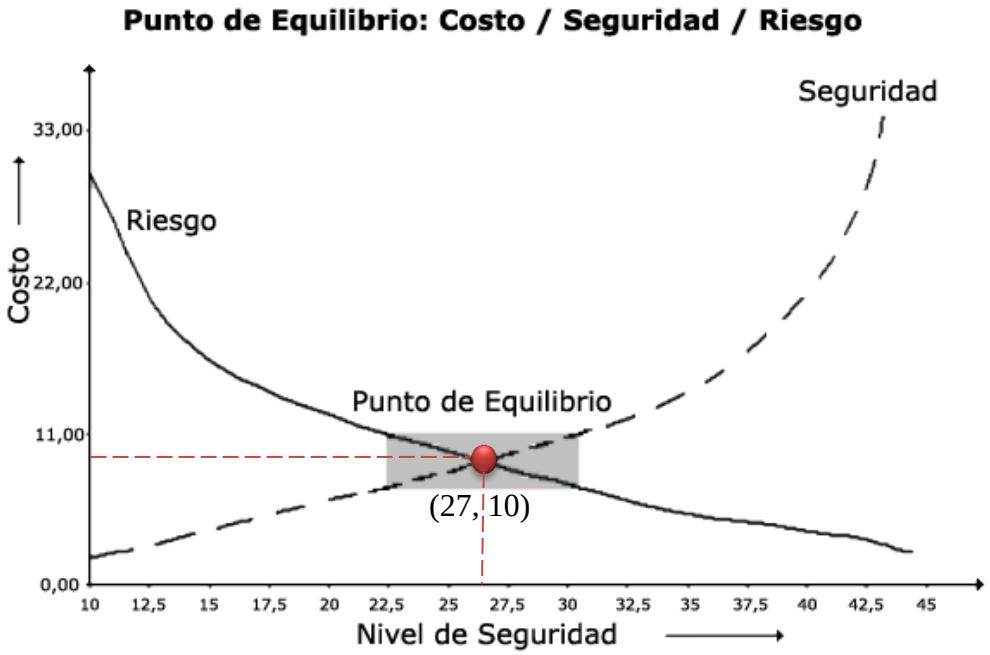


Figura 15: Punto de Equilibrio: Costo/Seguridad/Riesgo ([71] Borghello)
Fuente: https://www.segu-info.com.ar/politicas/costos.htm

El punto clave del análisis de costos que implican dotar de seguridad en un objeto o entorno IoT es conocer claramente los riesgos que se corren definirlos y asignarles un valor, los niveles de seguridad que se pueden aplicar y sus costos asociados, en el cual podemos llegar a un Punto de Equilibrio.

4.4 ESQUEMAS PARA DISEÑAR OBJETOS INTELIGENTES CON NIVELES DE SEGURIDAD ACEPTABLES.

4.4.1 Componentes IoT

Para una mejor comprensión y para definir los esquemas de seguridad en el Internet de las Cosas, es importante poner en consideración los componentes presentes, los mismos que deben estar integrados entre sí para lograr una seguridad integral. Estos

componentes se desglosan de la siguiente manera como lo muestra en la siguiente Figura 16.

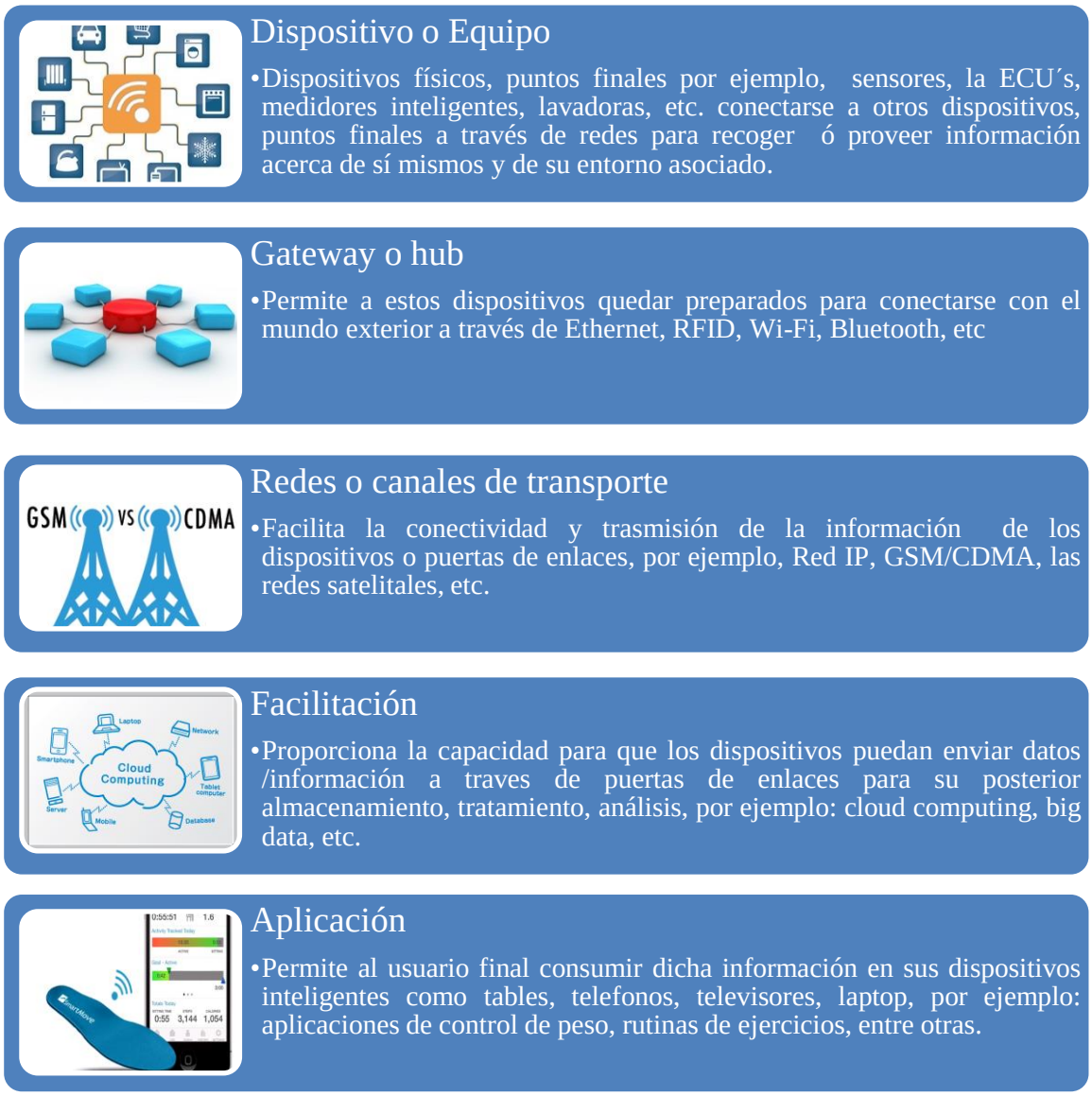


Figura 16: Componentes de un entorno IoT ([72] Ajit & Sunil).
Fuente: www.lnttechservices.com

4.4.2 Esquema de seguridad para un entorno de IoT

El siguiente esquema que se observa en la Figura 17 da un enfoque para la construcción de la seguridad desde sus niveles más bajos hasta sus niveles más altos, teniendo en cuenta la seguridad en todas las secciones del esquema.

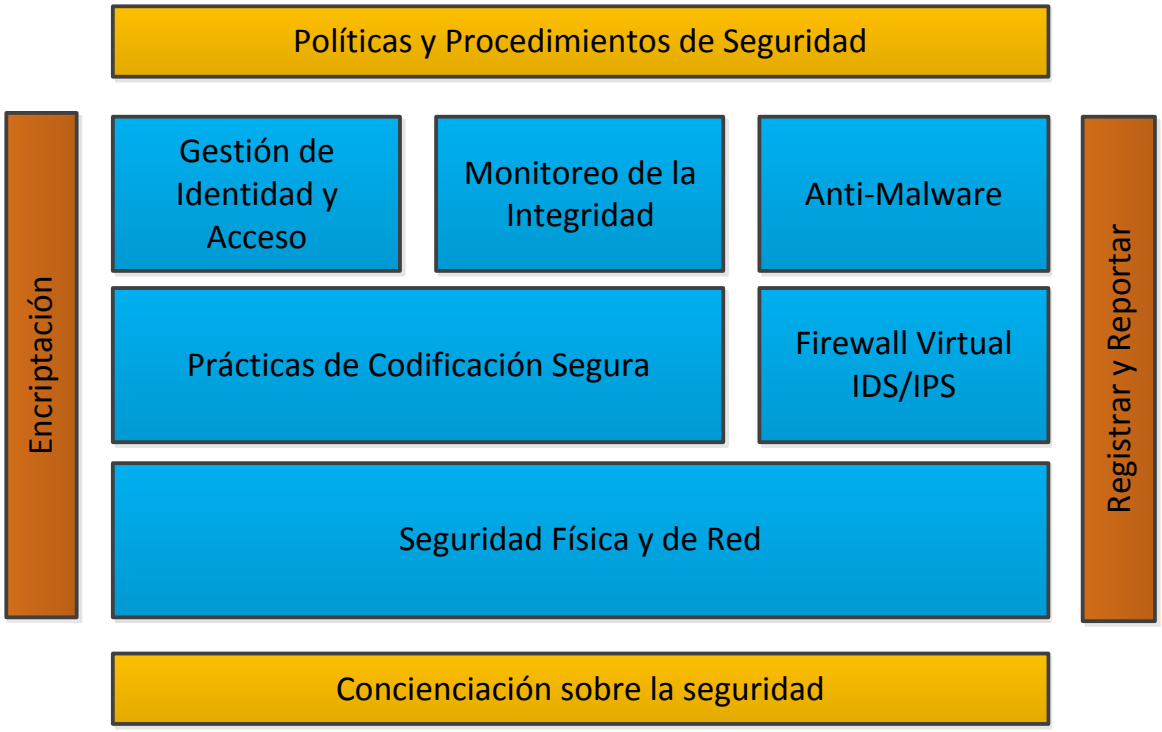


Figura 17: Esquema de seguridad para entorno IoT ([72] Ajit & Sunil)
Fuente: www.lnttechservices.com

4.4.3 Análisis de los componentes del esquema

4.4.3.1 Nivel 0: Concienciación sobre la seguridad

Es importante para empezar a crear un proyecto de IoT o claramente crear objetos que estarán conectados en una red donde van a transitar una gran cantidad de

información y entre esa parte información crítica que requiere de un tratamiento especial, esta debe empezar con el conocimiento sobre las seguridades que se requieren tener un determinado objeto conectado y a los peligros que este estará enfrentando día a día, dependiendo del entorno en el que se encuentre. Aunque esto podemos decir que no solo depende de un objeto ya que como hemos visto anteriormente intervienen otros componentes para asegurar que nuestro entorno IoT no se vea comprometido.

4.4.3.2 Nivel 1: Seguridad física y de red.

En este nivel se deberán considerar los accesos físicos de los dispositivos o puntos finales dándole la respectiva importancia dependiendo del entorno en el que se encuentren; así mismo la seguridad en la red en todas sus capas (acceso a la red, internet, transporte y aplicación), teniendo en cuenta las lecciones aprendas y adoptando los mecanismos apropiados para asegurar un entorno IoT.

4.4.3.3 Nivel 2: Prácticas de Codificación Segura & Firewall Virtual IDS/IPS

En este nivel se determinan aplicar para el desarrollo de aplicaciones para entornos IoT prácticas de codificación segura que permitan eliminar al mínimo vulnerabilidades conocidas y evitar ataques a las aplicaciones en base a los estándares de la industria como OWASP, SAFEcode, SANS/CWE, esto nos permite

considerar y exponer a las aplicaciones a pruebas de escaneo o fuzz para encontrar vulnerabilidades que comprometan las aplicaciones y los datos que manejen.

Así mismo encontramos en este nivel los Fierwall Virtuales IDS/IPS con sistemas de Detección de Intrusos y Prevención de Intrusos siendo un componente clave del sistema de detección de ataques y vulnerabilidades, que trabaja junto con otros controles en la seguridad que se consideren implementar.

4.4.3.4 Nivel 3: Gestión de Identidad y Acceso, Monitoreo de la Integridad & Anti-Malware.

En este nivel encontramos la gestión de identidad y acceso, debido a que el eslabón más débil de las redes son los usuarios y su identidad. Y a medida que datos y aplicaciones críticas de negocio migran a la nube, es necesario que los usuarios locales, remotos y móviles y su identidad accedan de forma sencilla sin poner en peligro la seguridad. Para lograrlo, se necesitan controles de acceso que extiendan la seguridad más allá del firewall. Esta parte representa una categoría de soluciones interrelacionadas que se utilizan para administrar autenticación de usuarios, derechos y restricciones de acceso, perfiles de cuentas, contraseñas y otros atributos necesarios para la administración de perfiles de usuario.

Otro punto es el monitoreo de la integridad, los archivos críticos requieren de bastante cuidado y se deben implementar fuertes controles para no permitir la

modificación o alteración de la información sin la autorización respectiva, un punto muy importante cuando se manejan archivos críticos.

El último punto de este nivel son los Anti-Malware, el software malicioso o malware es una amenaza que utiliza múltiples técnicas y vías de entrada: páginas web, correo electrónico, mensajería instantánea, redes P2P, dispositivos de almacenamiento externo y puertos abiertos en nuestro ordenador. Entre otras, estas vías, son utilizadas por el malware para infectar a los sistemas informáticos y propagarse por ellos, afectando de distintas formas (impidiendo acciones, vigilando usos, ralentizando sistemas, ejecutando acciones no permitidas, etc.), por este motivo una solución anti-malware permite tener una defensa frente a las amenazas, tanto dentro como fuera de la red.

4.4.3.5 Nivel 4: Políticas y procedimientos de seguridad

En este nivel las políticas de seguridad y los procedimientos de seguridad que se establezcan serán en base a las experiencias previas de lo que ya ha sucedido y como se ha actuado, así mismo tiene que permitir avizorar sobre posibles amenazas o problemas que pueden incurrir en un determinado momento. Se pueden considerar en este punto las RFC 2196 - Manual de Seguridad del Sitio, así como también la ISO 27001 – Sistema de Gestión de la Seguridad de la Información SGSI, que permiten proporcionar orientación práctica a los administradores tratando de asegurar su información y servicios en una red.

Como parte final de nuestro esquema encontramos la encriptación y el registro y reporte, estos se encuentran en los niveles 1, 2 y 3, en vista que la parte de encriptación lo que hace es hacer ilegible la información a personas no autorizadas en caso de que la misma este comprometida y se maneja dependiendo del entorno de aplicación, siendo consideradas o no en todos esos niveles o en algunos de ellos.

El registro y reporte lo que permite es registrar como bitácora todos los sucesos que se den en el entorno donde se encuentren los dispositivos ya sea en su periodo de pruebas o producción y al reportarlos se generan las debidas correcciones en caso de presentar alguna vulnerabilidad.

A continuación se presenta una tabla en la cual se asignaran las capas de seguridad a los componente de IoT, con las respectivas consideraciones de seguridad o estrategias de mitigación de riesgo que deben incorporarse, teniendo en cuenta en entorno de implementación donde van a funcionar y las experiencias de expertos.

No.	Capas de Seguridad	Consideraciones de Seguridad
Dispositivo o Equipo		
1	Seguridad en dispositivos físicos, puntos finales y equipos.	• La protección de los dispositivos es de suma importancia dependiendo del medio donde estén implementados, como es el caso de los dispositivos médicos que deben brindar una seguridad fuerte como:

		✓ Deshabilitar la conectividad de dispositivos por ejemplo USB, permitiendo solo el uso con la aprobación, revisión, escaneo con el debido consentimiento de la persona encargada. ✓ Deshabilitar el acceso directo a internet de dispositivos con información confidencial en los puntos finales si no se requiere. ✓ Asegurar que los servicios no utilizados son deshabilitados o bloqueados, como puertos abiertos, protocolos inseguros. ✓ Arranque seguro (usando claves cifradas) y firmware seguro. ✓ Soporte de autenticación de dispositivo cuando se conecta. ✓ Aplicación de parches regulares en el Sistema Operativo del dispositivo. ✓ Actualizaciones seguras y autenticadas. ✓ Conexiones seguras con listas blancas en lugar de listas negras. ✓ Intercambio de claves seguro.
Gateway & Red		
2	Seguridad en el Gateway	• Garantizar que la puerta de enlace que conecta

		el IoT/M2M con la parte exterior, este asegurada contra intrusiones y malware, mediante el uso de mecanismos adecuados como ACL, IPS, filtrado, etc.
3	Seguridad Física y de Red	• Las instalaciones deben tener seguridad física como guardias de seguridad, tarjetas de acceso, registro de visitantes, circuito cerrado de televisión, zonas seguras, etc. Para evitar los accesos no autorizados. • Mecanismos de seguridad apropiados deber ser aprovechados para el aislamiento de la información confidencial considerando los IDS/IPS, firewall, ACL de red, etc. • El proveedor de servicios debe tener certificaciones de seguridad, tales como la ISO 27001, sellos de privacidad, etc.
4	Seguridad de acceso remoto	• Permitir una sólida autenticación por ejemplo la Autenticación Multifactor (MFA), para el acceso remoto a los usuarios privilegiados como los administradores, médicos, personal de mantenimiento, para iniciar sesión de forma

		segura desde fuera de la red. • El uso de canales de comunicación seguros, tales como VPNs-S2S, C2S para acceso a empleados regulares a la red de la empresa desde las sucursales, y se deshabilita su acceso cuando ya no se requiera.
5	Seguridad en comunicaciones inalámbricas	• El uso de configuraciones seguras cuando se comunican a través de las redes inalámbricas; dispositivos/sensores por la puerta de enlace. • Cumplimiento de las autenticaciones y cifrados.
Facilitación		
6	Seguridad en la nube	• La seguridad y administración de la nube, es una parte importante y por lo tanto necesita una atención especial en lo referente a seguridad. Se pueden considerar las siguientes estrategias de mitigación de riesgos: ✓ Las Máquinas virtuales necesitan seguridad y cuidado, por ejemplo: dureza del Sistema Operativo huésped, parches, actualizaciones, etc. ✓ El acceso a las Máquinas Virtuales, las

		aplicaciones en ella necesitan tener fuerte mecanismos de control. ✓ La seguridad de datos en la nube con tecnologías apropiadas y algoritmos de cifrados apropiados incluyendo fuertes algoritmos de administración de claves. ✓ Soluciones BC/DR deben diseñarse como instantáneas para las Máquinas Virtuales y los datos de la misma, aprovechando las copias de seguridad fuera del sitio, teniendo máquinas virtuales en modo de espera en otros servicios de la nube, dentro de la misma región del proveedor. ✓ Protección Web frente a instancias en la nube con IDS/IPS, firewall basados en host, etc. Para el trafico malicioso detección/prevención. ✓ Monitoreo de inicio de sesión especialmente para usuarios con privilegios y administración de sesiones integrando los múltiples registros con soluciones SIEM (Información de Seguridad y administración de Eventos)

		para la correlación y análisis de incidentes de seguridad.
Aplicación		
7	Seguridad en las Aplicaciones	• Aplicaciones (pueden ser web, móvil, nube, etc.) deber ser desarrolladas con las prácticas seguras de codificaciones estándar de las industrias como OWASP, SAFEcode, SANS Institute/CWE, etc., para minimizar el riesgo de ataques a las aplicaciones. ✓ Ejemplo prevenir el SQL inyección, XSS, fuga de datos, sesión de repetición, ataques de desbordamiento de buffer, etc. ✓ Aprovechamiento de las mejores prácticas tales como restricción de archivo, validación de entrada, etc. ✓ Pruebas de escaneo o fuzz (dinámicas, estáticas, hibridas) para detectar vulnerabilidades en las aplicaciones y tomar acciones correctivas para solucionarlas. ✓ Emplear código firmado para asegurar a los clientes sobre la autenticidad del software, así como el no-repudio.

8	Monitoreo de la integridad	• Los archivos críticos deben ser monitoreados para detectar cualquier alteración o cambio no autorizado, por ejemplo: archivo de configuración, el tráfico debe ser monitoreado para detectar cualquier cambio deliberado o accidental. • Mecanismos apropiados como herramientas para monitorear la integridad deben ser implementados para prevenir o alertar lo indicado anteriormente. • Complementar además fuertes procesos de aprobación de cambios y revisión.

Tabla 2: Consideraciones de seguridad asignada a los componentes IoT ([72] Ajit & Sunil)
Fuente: www.lnttechservices.com

Otra capa que hay que considerar que es la ubicuidad u omnipresencia que se encuentra por encima de las capas e independientemente de cualquier componente del IoT, la misma que detallamos en la siguiente tabla.

No.	Capas de Seguridad	Consideraciones de Seguridad
Omnipresencia		
1	Identificar y comprender la necesidad del cliente.	❖ Trabajar con el negocio del cliente, Tecnologías de la Información y equipos de

		seguridad para entender las necesidades del negocio, sistema y medio ambiente: o Políticas del cliente (seguridad y privacidad). o Cumplimiento de normativas y requerimientos de la industria alineados con los objetivos del negocio (PCI DSS, NERC CIP, FDA, PIPEDA, etc.) o Evaluar los riesgos de seguridad.
2	Administración de Identidades y Accesos (IAM).	❖ Usuario, dispositivo, punto final se autentican como estaciones de trabajo, dispositivos médicos, contadores inteligentes, etc. ❖ Aprovisionamiento y des-aprovisionamiento seguro de dispositivos, usuarios, aplicaciones, etc. ❖ Integración con un sistema de administración de credenciales existente. ❖ Seguridad en las credenciales con hash. ❖ Roles basados en acceso a dispositivos, aplicación, base de datos, red, nube, etc.
3	Seguridad en los datos y	❖ Encriptación de datos en reposo para asegurar

	privacidad	la confidencialidad. ❖ Seguridad y privacidad de los datos en transito o Ejemplo transmisión segura de datos desde el dispositivo/Gateway a la nube, entre el móvil u la nube, etc. o Soporte a la seguridad en protocolos nuevos o emergentes como el MQTT que no disponen de seguridad básica incorporada. o Encriptación a nivel de canales o mensajes y administración de claves. o Adopción de protocolos seguros ligeros. o Integridad de la información sensible a ser almacenada, procesada y transmitida debe mantenerse, mitigación de riesgos de repudio, ejemplo mediante uso de firmas digitales.
4	Gestión de la Seguridad	❖ Asegurarse que las soluciones anti-malware se desplieguen y funcionen para proteger contra malware. ❖ Actualizaciones de parches, versiones del sistema operativo, deben ser empleados con

		frecuencia para evitar vulnerabilidades conocidas. ❖ Realizar análisis de vulnerabilidades y pruebas de seguridad en los puntos finales, estaciones de trabajo, dispositivos, aplicaciones, redes, etc., que formen parte del entrono IoT.
5	Registro y Auditoria	❖ Proveer para la rendición de cuentas permitiendo los registros de seguimiento de acceso a los dispositivos, aplicaciones, redes, etc., y los cambios no autorizados a los archivos ❖ La solución debe ser capaz de integrar los registros con soluciones SIEM para la correlación y análisis.

Tabla 3: Capa de seguridad omnipresente ([72] Ajit & Sunil)
Fuente: www.lnttechservices.com

Una parte fundamental en la seguridad viene de los sensores o dispositivos que tienen la capacidad de controlar directamente las cosas, estos están conectados a través de protocolos de comunicación diferentes que utilizan diferentes mecanismos para asegurarse a sí mismos. Algunos de estos mecanismos se enumeran en la siguiente tabla.

No.	Capas de Dispositivos de Sensores	Seguridad
Protocolos de comunicación		
1	Wi-fi	➢ Cifrado AES, TKIP y WEP ➢ WPA y WPA2 ➢ EAP-métodos de autenticación de la capa 2
2	Bluetooth / BLE	➢ Emparejamiento seguro ➢ Apagar el modo de detección cuando no es necesario, hacer cumplir la autenticación de dispositivos BT. ➢ Para BLE, el emparejamiento inicial es inseguro.
3	Zigbee (802.15.4)	➢ Enlace capa de cifrado con AES de 128 bits. ➢ Centro de confianza para la distribución de claves.
4	6LowPAN	➢ Modo seguro mediante el cifrado de capa de enlace 802.15.4. ➢ Lista de control de acceso (ACL).
5	Weightless	➢ Enlace de comunicación cifrada entre la estación base y el dispositivo.

6	GSM	➢ El algoritmo de autenticación (A3) para proteger contra el acceso no autorizado de servicio ➢ Cifrado algoritmo de generación de claves (A8) incrustado en la tarjeta SIM. ➢ Identidad del Suscriptor Móvil Temporal (TMSI) para evitar intrusiones.
7	3G	➢ Autenticación mutua - clave de cifrado e integridad de generación de claves. ➢ Integridad de datos. ➢ Autenticación de usuario-USIM.
Protocolos de seguridad IP		
1	IKEv2/IPsec	➢ Certificados X.509 para la autenticación ➢ Diffie-Hellman para sesión secreta compartida ➢ Generación de claves criptográficas utilizando secreto compartido ➢ Establece un túnel seguro.
2	TLS/SSL	➢ Certificado X.509 para la autenticación. ➢ Las claves asimétricas de X.509 utilizados para el intercambio de clave simétrica.

		➢ Clave simétrica utilizada para el cifrado de datos.
3	DTLS	➢ Datagramas de TLS (basado en TLS)
4	HIP	➢ Protocolo de Identidad de Host. ➢ La identidad del host basado en clave pública (en lugar de la popular dirección IP/DNS).
5	EAP	➢ Protocolo de autenticación extensible ➢ Un marco de autenticación que soporta múltiples métodos de autenticación. ➢ Funciona en la capa de Enlace. ➢ Utiliza diferentes protocolos de EAP mensajes transmisión. ➢ Compatible con los mecanismos de entrega y uso de claves.
6	SSH	➢ Un protocolo de red de cifrado. ➢ Utiliza la criptografía de clave pública para la autenticación mutua. ➢ Crea un canal seguro para los datos.

Tabla 4: Protocolos de seguridad para dispositivos IoT ([72] Ajit & Sunil).
Fuente: www.lnttechservices.com

En cada una de las capas de seguridad se hace referencia a un esquema general donde no solo interviene el objeto en sí, debido a que el entorno IoT está conformado por algunos componentes y cada uno juega un papel muy importante en la seguridad.

4.4.4 Componentes de un objeto inteligente

Una vez realizado un análisis general de los componentes de un entorno IoT y sus consideraciones de seguridad en sus distintos niveles y capas de sus componentes, definiremos los componentes específicos de un objeto inteligente, como se muestra en la siguiente Figura 18. Considerando que las primeras 5 capas de la Figura son obligatorias quedando de forma opcional las dos capas superiores, debido a que estas pueden ser manejadas desde otros dispositivos con mayores capacidades de procesamiento, memoria y energía.



Figura 18: Componentes de un objeto IoT.
Fuente: Elaborado por Autor

De estos componentes se define lo siguiente:

Un microcontrolador es un circuito integrado o chip que incluye en su interior las tres unidades funcionales de una computadora: CPU, Memoria y Unidades de E/S, es decir, se trata de un computador completo en un solo circuito integrado, estos cada vez son más pequeños y no tan notables.

El firmware es el bloque de instrucciones de máquina para propósitos específicos, grabado en una memoria, normalmente de lectura/escritura (ROM, EEPROM, flash, etc.), que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.

Los sensores recopilan información sobre el medio ambiente, el usuario, o ambos. Ejemplos de lo anterior incluyen la luz, temperatura, movimiento, ubicación (GPS), etc. Los actuadores trabajan en base a la información recabada por los sensores y actúan de acuerdo a las instrucciones programadas.

La parte de la alimentación se refiere a la batería que deben tener los objetos, aquí hay un serio problema que es que entre más pequeño el dispositivo los recursos de energía se limitan y se deben buscar mejores estrategias para que el dispositivo consuma menos energía o aprovechar energía que se pueda aprovechar del entorno.

La conectividad se enmarca en los protocolos de comunicación que se utilicen para que los dispositivos puedan interactuar con otros, así mismo se deben buscar protocolos de comunicación que permitan ahorrar los más posible la energía y además que brinden la seguridad en el entorno que se encuentren.

El sistema operativo es la parte que va a permitir manejar el dispositivo de acuerdo a las funciones para el que ha sido diseñado, en este nivel lo que me permitirá es poder instalar un mayor número de aplicaciones que permitan obtener una mayor funcionalidad en el objeto, el ejemplo más claro en este punto son los teléfonos inteligentes.

Cabe indicar que todos estos componentes están integrados, pero se puede omitir por ejemplo, que solo trabaje como sensor o solo como actuador, así mismo también se puede omitir la parte del Sistema Operativo y solo programar el dispositivo a nivel

de firmware para que ejecute las instrucciones respectivas, y la parte de administración se la realice desde otro dispositivo más robusto para manejar una mayor cantidad de dispositivos IoT.

Las aplicaciones también forman parte de los componentes de los objetos inteligentes IoT, aunque esto sería para dispositivos con mayores capacidades de procesamiento, memoria y energía, que le permitan tener un mayor rendimiento en base a los requisitos que fuesen diseñados.

Los componentes descritos en esta sección por lo general se integran en una sola placa, enmarcándolos en un solo dispositivo, además como se dijo anteriormente existirán componentes que se omitan en el diseño de un determinado dispositivo u objeto, esto con el fin de hacerlos menos notorios como es el caso de los Wearables que son dispositivos electrónicos que se incorporan en alguna parte de nuestro cuerpo interactuando continuamente con el usuario y con otros dispositivos con la finalidad de realizar alguna función específica, relojes inteligentes, zapatillas de deportes con GPS incorporado y pulseras que monitorizan nuestro estado de salud son ejemplos entre otros de este tipo tecnología que se encuentra cada vez más presente en nuestras vidas.

4.4.5 Esquema de seguridad de un dispositivo IoT

En este esquema en el cual nos centramos en el dispositivo y considerando el esquema general para entornos IoT, podemos determinar lo que es importante para que un objeto se considere con un nivel de seguridad aceptable, ver Figura 19.

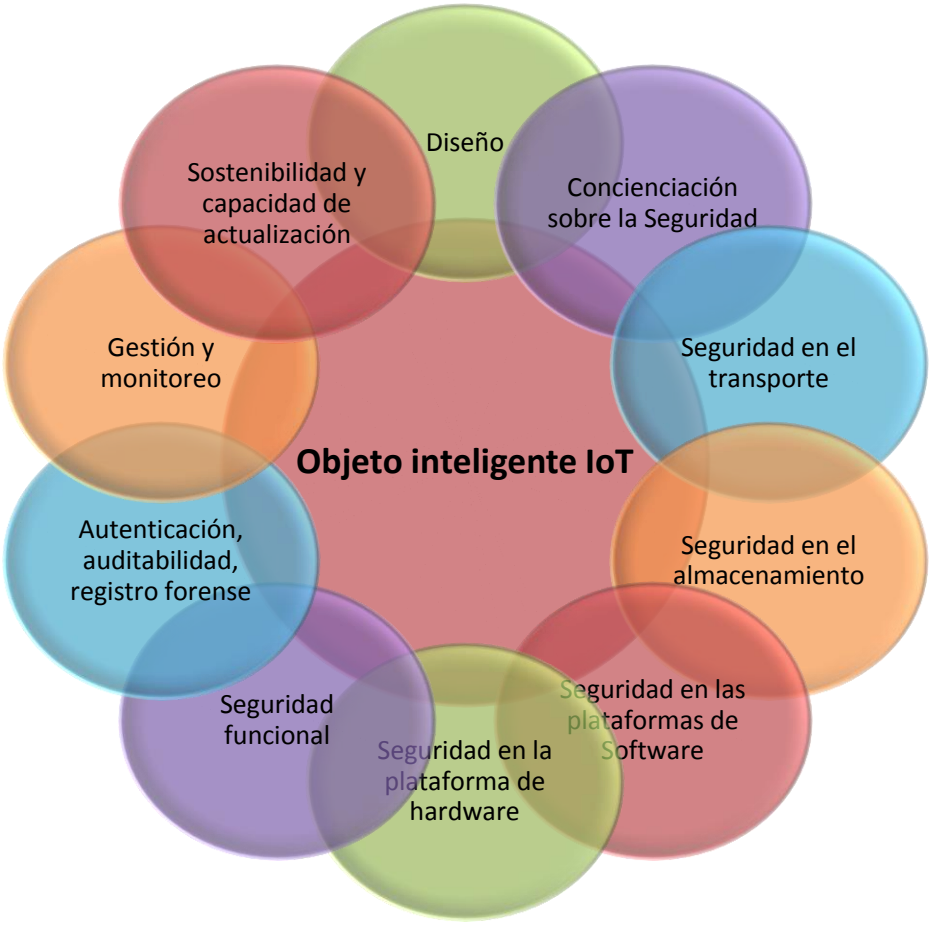


Figura 19: Esquema de seguridad para un objeto IoT.
Fuente: Elaborado por Autor

Al describir este ciclo continuo para el desarrollo de objetos inteligentes, el mismo que debe ser constante desde el principio del ciclo de vida de desarrollo del objeto

como es el diseño y arquitectura, implementación y pruebas, claramente se traduce en:

4.4.5.1 Diseño

En esta fase inicial de desarrollo del objeto puede haber una gran cantidad de concepto de diseño, análisis de mercado, análisis de la competencia, y el apoyo a la investigación. El papel de un individuo consciente de la seguridad es normalmente ligero, que ofrece consultoría, análisis y asesoramiento en torno a los conceptos de alto nivel, los componentes y las capacidades de seguridad de tecnología. También se puede tomar consejos de seguridad respecto a las capacidades de la competencia y la dirección esperada de mercado, regulaciones y de las fuerzas legislativas en lo que respecta a la seguridad cibernética.

Incluso en esta etapa temprana esta idea puede ser muy valiosa, ya que proporcionará insumos de muy alto nivel que ayudarán a determinar si los conceptos propuestos son viables y cuáles son las consideraciones deben ser durante la fase de requisitos.

4.4.5.2 Concienciación sobre la seguridad

Considerar experiencias vividas del pasado, registros tomados durante cada una de las fases, todo aquello que sirva para tomar conciencia de las seguridades que debe tener el objeto y tomar las acciones debidas minimizando los riesgos de vulnerabilidad en el objeto.

Se puede aplicar las normas ISO 27001, en la que hace referencia a la concienciación en una empresa sobre la seguridad de la información, esta puede ser tomada en cuenta también para el objeto físico y la información que esta maneje, la cultura de seguridad que debe tener cada componente del objeto para que se considere seguro.

Las políticas y procedimientos de seguridad que se consideren a partir de aquí, servirán de orientación durante el diseño e implementación de un objeto para un determinado entorno, además de avizorar posibles amenazas en los que se puedan ver comprometidos.

En este punto también se pueden considerar la facilidad de uso, factor de forma física, el consumo de energía, y otros requisitos tecnológicos que son importantes para asegurar la plataforma. Además de las personas con un mandato de seguridad deben ser parte de este equipo que participa en la formulación de los requisitos técnicos y de mercado, creando una mejor conciencia sobre la seguridad del objeto.

4.4.5.3 Seguridad en el transporte

Proporcionar un nivel adecuado de identificación, privacidad e integridad de la comunicación en red. La comprensión de cómo se produce la autenticación alámbrica o inalámbrica, las credenciales almacenadas y si pueden ser trasplantados en otros dispositivos son obviamente muy importante.

Se pueden aplicar Listas de Control de Acceso - ACL para dar privilegios a los a cierto tipo de información o determinados recursos; Sistemas de Prevención de Intrusos IPS, que permita la detección de ataques o abusos en una red; es importante en esta parte el uso de sistemas criptográficos que permitan que las conexiones y la información que se maneje entre determinados objetos este ilegible en caso de robo, existen varios métodos y técnicas de encriptación que se pueden utilizar las funciones hash como MD5, SHA-1 o SHA2, entre otras. Además de complementar utilizando canales de comunicación seguros como las VPN's, para la comunicación.

El manejo de protocolos de seguridad IP que forman parte del objeto como el IPsec, TLS/SSl, DTLS, HIP, EAP, SSH, compaginando con las seguridades que nos brinda los protocolos de comunicación Wi-fi, 6LowPAN, GSM, 3G.

4.4.5.4 Seguridad en el almacenamiento

Se debe proporcionar el nivel adecuado de protección de datos persistentes mantenidos en el dispositivo o en el sistema. Los datos deben estar asegurados en el caso de un ataque físico debido a la pérdida, o de otra manera la comprensión de cómo los datos sensibles serán asegurados, tanto desde una perspectiva de la integridad y la privacidad.

Podemos considerar como en el punto anterior la encriptación para datos en reposo, con esto aseguraremos que si en algún momento el objeto o plataforma que

almacena algún tipo de información confidencial no sea tan vulnerable a los ataques mal intencionados.

Es importante que se cuente con un almacenamiento redundante que permita tener disponible la información para ser accedida en momentos oportunos creando confianza en quienes utilizan el servicio.

4.4.5.5 Seguridad en las plataformas de software

Seleccionar e implementar plataformas y tecnologías de apoyo que proporcionan un entorno sólido y en capas sobre la cual construir la solución fácil y rápida.

La Selección de un sistema operativo moderno o plataforma que proporciona las propiedades de defensa en profundidad, incluyendo a ASLR que es una técnica de seguridad implicada en la protección de los ataques de desbordamiento de la pila, la memoria no ejecutable, la segregación de procesos, y la caja de arena.

Si las prácticas de codificación segura y protecciones compilador posteriores no logran mitigar una vulnerabilidad, un sistema operativo moderno o plataforma que proporciona una defensa en profundidad pueden ayudar a minimizar el impacto y facilitar la recuperación a un estado bueno conocido.

Es importante aplicar soluciones BC/DR para las plataformas de software que permitan aplicar políticas de continuidad del negocio y recuperación de desastres, así

como considerar practicas seguras de codificación estándar de las industrias tales como OWASP, SAFEcode, entre otras para minimizar el riego de ataques a las aplicaciones.

Implementación de Firewall, antivirus que ayuden también a la detención software malicioso evitando el robo de información confidencial.

4.4.5.6 Seguridad en la plataforma de hardware

Garantizar que la plataforma de hardware proporcione las características de seguridad necesarias. Esto implica algunos puntos como:

- ROM de arranque, permitiendo un arranque de confianza o verificado desde un nivel muy bajo, esto depende del entorno de ejecución de confianza en donde se implemente el objeto.
- Para los dispositivos que requieren un uso intensivo de la criptografía, las implementaciones de hardware pueden mejorar el rendimiento y prolongar la vida útil de la batería. Sin embargo, es importante entender que los cifrados son compatibles y sí que proporcionan una vida útil razonable para la longitud esperada del producto.
- En el diseño de circuitos se debe de considerar un posible ataque a la placa de circuito, es decir que su exposición debe ser considerado para mitigar posibles ataques. Siempre que sea posible, se debe dejar lo menos visible la placa del circuito del objeto.

- Las interfaces son las que proporcionan accesos a los componentes de la placa, el mismo que puede ser utilizado para alterar varias características de seguridad. Cualquier interfaz, sean consola o lógica, a través de USB o de serie, deben tenerse en cuenta en el contexto de la seguridad. La ROM de arranque a menudo proporcionan una manera de cargar el firmware o manipular el proceso de arranque, tanto de que los problemas de seguridad se encuentren potencialmente presentes.
- El embalaje de componentes, la facilidad de acceso a la memoria, flash, y la CPU. Al seleccionar ciertas opciones de sistema en chip de embalaje en el que, por ejemplo, la memoria se encuentra físicamente debajo de la CPU, puede complicar los ataques de hardware que de otro modo sería trivial.
- La administración de energía es un punto importante dentro de la seguridad de las plataformas de hardware, hay que considerar su resistencia dependiendo de la capacidad de procesamiento, almacenamiento que va a tener el objeto.

4.4.5.7 Seguridad funcional

Implementar la funcionalidad utilizando una tecnología de pila y herramientas que le permitan ser creado de una manera segura. Cada componente dele objeto aplicando los debidos mecanismos de autenticación, integridad, encriptación, identificación, no repudio, destrucción de datos, servicios, entre otros, deberán responder de forma adecuada a cualquier estimulo externo que comprometa de manera maliciosa al objeto.

4.4.5.8 Autenticación, auditabilidad y registro forense

Cada vez más dispositivos IoT se están comprometiendo y se utilizan como puntos de entrada o plataformas desde donde lanzar ataques. Ser capaz de investigar estos de una manera eficaz es fundamental, pero esto requiere el apoyo de los proveedores para proporcionar información de registro y auditoría robusta. Se pueden aplicar Sistemas de Detección de Intrusos o Sistemas de Prevención de Intrusos.

Conjuntamente con la necesidad de realizar auditorías de sistemas o análisis forenses según sea el caso, para determinar cómo se encuentran los objetos en un determinado momento y si es que ha sido comprometido de forma mal intencionado aplicar técnicas de análisis forenses para determinar el fallo. En este caso se pueden considerar distribuciones como Kali Linux específico para realizar auditorías de páginas web, redes y sistemas informáticos, GFI LanGuard orientado a redes y software, entre otros.

4.4.5.9 Gestión y monitoreo

Asegurar que los objetos IoT se pueden gestionar y supervisar de forma segura. En este caso se deben implementar sistemas de monitoreo de red para la conectividad de los objetos, integridad que permita detectar cualquier modificación o cambio no autorizado de la información o parámetros de los objetos.

Como por ejemplo podemos citar la herramienta PRTG Network Monitor que tiene funcionalidades como monitoreo de red compresivo, sistemas de alertas flexibles, clúster de alta disponibilidad para un monitoreo de red sin interrupciones, Monitoreo distribuido con sondas remotas, Publicación de datos y mapas. Cuanta con alrededor de 200 tipos de sensores que cubren varios aspectos de red.

La gestión y monitoreo permite conocer el estado de un determinado objeto, para que en caso de ruptura sea reemplazado oportunamente.

El registro de novedades es muy importante en esta fase para hacer la retroalimentación del sistema y mejorar las políticas y procedimientos de seguridad implementados inicialmente.

4.4.5.10 Sostenibilidad y la capacidad de actualización

Características que facilitan la posibilidad de actualizar de forma segura los dispositivos cuando se descubren vulnerabilidades después de la liberación, se puede considerar lo siguiente:

- Recibir y procesar los informes de problemas de seguridad de partes externas.
- Proactivamente monitorear los informes de problemas de seguridad en los componentes de terceros utilizados y trabajar con el desarrollo para integrarlos en su caso.

- Mantener contactos frecuentes con los proveedores de componentes utilizados para identificar si otros lanzamientos se han producido problemas de seguridad.
- Mantener una capacidad de selección, clasificación, resolución, pruebas, envíos y distribución de parches para problemas de seguridad detectados.
- Tener un plan en marcha para los peores casos, como retiro de productos o reparación generalizada.

Este último punto en particular, es de vital importancia. Vemos regularmente proveedores que no mantienen esas capacidades y como resultado no son capaces de tratar razonablemente parches de seguridad, incluso si hubiese una necesidad apremiante.

Cada una de estas fases o etapas a considerar al igual que el esquema general debe ser un ciclo en constante movimiento que permita la retroalimentación en base a los registros que se obtienen en pruebas durante su desarrollo o ya en un entorno real de funcionamiento, o también en base a algún fallo que se produzca por entes con malas intenciones provocando grandes pérdidas pero que deben ser solucionados de forma inmediata.

4.5 Beneficios del proyecto

Este Proyecto de Internet incluye una visión general de los requisitos operativos y de seguridad, tanto de los objetos conectados al internet, se refirió a los problemas

generales de modelo de amenaza y de seguridad, e introdujo una serie de posibles esquemas de seguridad ajustados diferentes tipos de despliegues de la IoT.

Se quiere lograr tener una base fundamentada para hacer de la seguridad una parte integral de los objetos inteligentes del IoT, para que los entornos donde estos sean desplegados exista la certeza de que su arquitectura de seguridad es muy sólida.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1 Análisis de resultados

Este análisis está basado en la comparación de los datos y resultados que se dieron en las entrevistas:

Entrevista al Director de tecnología del GAD-Portoviejo:

Se le realizaron 11 preguntas para analizar las consideraciones de seguridad de los objetos en el Internet de las Cosas.

- ¿Qué es el internet de las cosas?

VB: Es la definición de tener objetos comunes y corrientes conectados a internet realizando alguna actividad específica.

- ¿Qué beneficios consideras que traería la adopción del internet de las cosas?

VB: Importante en cuanto a la reducción de costos y tener una administración de dispositivos eficaz y eficiente.

- ¿Qué seguridades se deberían considerar en los objetos? (Hardware y software)

VB: Esto va a depender del objeto que se desea administrar, se pueden definir seguridades como VPN, seguridad perimetral, encriptación de información, entre otros.

- ¿Qué seguridades se deben tener en las redes de comunicación que interconectan los objetos?

VB: Las redes de comunicación deben asegurar que la comunicación permanezca estable siempre, para que los datos se puedan transmitir. Se pueden aplicar sistemas

de encriptación para que los datos que sean interceptados en la red no sean desencriptados por personas mal intencionadas.

- ¿Qué medidas se deberían tomar para que las empresas generen confianza en sus clientes para la adopción del Internet de las cosas?

VB: Depende del nivel cultural, que tenga experiencia y trayectoria de la misma, para el usuario tenga confianza en la adopción del IoT.

- ¿Las tecnologías existente en el Ecuador están preparadas para adopción del Internet de las cosas? (Infraestructura, conectividad, despliegue)

VB: En su totalidad si está preparando se está orientado y se está preparando en desarrollar soluciones con tecnologías en internet.

- ¿Qué mejoras implican estas innovaciones para todos?

VB: Entregar un mejor servicio a la ciudadanía, reducir costos dentro de la empresa y ser más eficaz y eficiente. Por ejemplo si un trabajo lo hacían 10 personas y con tecnología solo utilizo uno se está abaratando costos.

- ¿Cómo se pueden aprovechar las empresas Ecuatorianas del Internet de las Cosas?

VB: Desarrollando tecnología que sea útil para las personas y empresas que lo utilicen.

- ¿Cómo ves la participación de las empresas públicas y privadas en la adopción del Internet de las cosas?

VB: En Ecuador se han visto algunos proyectos innovadores de domótica con dispositivos móviles y aplicaciones para Smartphone.

- ¿Cuáles son los mayores retos a los que nos enfrentamos en el Internet de las cosas?

VB: Costos por los despliegues de las redes de comunicación que aún son altos y de las plataformas de administración, hay empresas o personas que no cuentan con los recursos para acceder a estas tecnologías innovadoras.

- En el campo que laboras conoces de alguna implementación con objetos inteligentes que se haya llevado a cabo. ¿Cuál? ¿Qué impacto tubo? ¿Qué proyectos se están planteando en el GAD?

VB: La implementación de la Smart City en la ciudad de Portoviejo que se desea llevar a cabo con la implementación de cámaras inteligentes, sistemas de parqueo inteligente y otras más que permitirán un mejor vivir a los ciudadanos de esta ciudad.

Entrevista al Jefe de Sistemas del Banco Comercial de Manabí

Se le realizaron 11 preguntas para analizar las consideraciones de seguridad de los objetos en el Internet de las Cosas.

- ¿Qué es el internet de las cosas?

DC: Medio de intercomunicación, relación, interacción de variedad de herramientas que tiene como objetivo facilitar las cosas a los usuarios finales.

- ¿Qué beneficios consideras que traería la adopción del internet de las cosas?

DC: Evolución para la aplicación de la tecnología.

- ¿Qué seguridades se deberían considerar en los objetos? (Hardware y software)

DC: Totalmente siempre se debe considerar la seguridad en informática en cual ambiente que este propiciando mejoras y avances tecnológicos.

- ¿Qué seguridades deberían tener las plataformas de almacenamiento, control, administración de los objetos inteligentes?

DC: Las plataforma de o debe implementar sistemas de encriptación, los de control manejo seguros de certificados y claves, y los de administración de objeto inteligentes debe estar bajo estándares que garantice las seguridades.

- ¿Qué seguridades se deben en las redes de comunicación que interconectan los objetos?

DC: Es crucial en sistema de red de cualquier topología manejar Firewall, certificados seguros.

- ¿Qué medidas se deberían tomar para que las empresas generen confianza en sus clientes para la adopción del Internet de las cosas?

DC: Debe implementar buenas prácticas de TI, aplicando estándares internacionales, ante todo certificarse. Esto lograra que se genere confianza en los clientes y atraerá más.

- ¿Las tecnologías existente en el Ecuador están preparadas para adopción del Internet de las cosas? (Infraestructura, conectividad, despliegue)

DC: Actualmente se ha notado que el Ecuador en materia de Tecnología está en proceso de cambio y esto es síntoma de que se está preparando para el avance y evolución tecnológica.

- ¿Qué mejoras implican estas innovaciones para todos?

DC: Aparecen nuevas formas de comunicarnos y estar más cercas de familias, amigos, etc. En fin aquello que antes era distante en la actualidad se acorta.

- ¿Cómo se pueden aprovechar las empresas Ecuatorianas del Internet de las Cosas?

DC: Creando nuevas herramientas y nuevos servicios para brindar a sus clientes. La oportunidad de invertir en tecnología y obtener nuevos ingresos.

- ¿Cómo ves la participación de las empresas públicas y privadas en la adopción del Internet de las cosas?

DC: Hoy en día todo lo que nos rodea tiene alguna relación con el Internet. La empresas cada vez se interesan más en el internet y su evolución e incluso ya existe dentro de las empresas departamentos solo dedicados a investigar esta tan fabulosa herramientas y sus bondades.

- ¿Cuáles son los mayores retos a los que nos enfrentamos en el Internet de las cosas?

DC: Uno de los mayores retos es el saberle darle buen uso aquellos componentes y herramientas que acompaña en el día. El no dejarnos dominar por aquellas cosas que parecen indispensables.

- En el campo que laboras conoces de alguna implementación con objetos inteligentes que se haya llevado a cabo. ¿Cuál? ¿Qué impacto tubo?

DC: Aún no hemos tenido la implementación de componentes inteligentes.

Entrevista al Jefe de Implementaciones de soluciones de software de la empresa BUPARTECH

Se le realizaron 11 preguntas para analizar las consideraciones de seguridad de los objetos en el Internet de las Cosas.

- ¿Qué es el internet de las cosas?

RC: Es lograr tener una conexión entre todas las cosas que nos rodea y lograr tener una comunicación basado en eso para nuestro beneficio, basado en las tecnologías y comunicaciones que actualmente tenemos.

- ¿Qué beneficios consideras que traería la adopción del internet de las cosas?

RC: El mayor beneficio que todos tendría es la optimización de tiempo en todas nuestras actividades, ósea minimizar los tiempos de respuesta en base a nuestras necesidades. Con estas conexiones vamos a tener más productividad en nuestras actividades diarias. Pero esto conlleva a tener una disponibilidad de los servicios, requiere que se tengan equipos de alto rendimiento de almacenamiento y procesamiento, y software que permita la administración de la información generada.

- ¿Qué seguridades se deberían considerar en los objetos? (Hardware y software)

RC: Considera una conjugación de seguridad de hardware y software, hay que ver la criticidad del sensor que se está manejando, se ve a los dos niveles como muy importantes y de alta prioridad para aplicar niveles de seguridad aceptables.

- ¿Qué seguridades deberían tener las plataformas de almacenamiento, control, administración de los objetos inteligentes?

RC: Se deben tener plataformas en las cuales se considere una seguridad de un 99,999% en diferentes niveles, que permitan tener confianza en la adopción del internet de las cosas, estas plataformas juegan un papel muy importante en esta adopción.

- ¿Qué seguridades se deben tener en las redes de comunicación que interconectan los objetos?

RC: Más que las seguridades en las redes lo que considera en tener la disponibilidad de la red, las seguridades se deberían aplicar a nivel de hardware o software que permitan colocar equipos o sistemas de criptografía, de control de permisos, accesos físicos y lógicos, generación de claves, accesos perimetrales. Esto permite asegurar los datos por la red y aunque los datos sean interceptados estos no sean descifrados.

- ¿Qué medidas se deberían tomar para que las empresas generen confianza en sus clientes para la adopción del Internet de las cosas?

RC: Las empresas deberán generar confianza a los clientes en base a los casos de éxito que la mayoría de empresas o personas van a pedir, esto es que a nuestro primer cliente mostrarle los beneficios y hacer que nuestro primer trabajo sea un trabajo exitoso.

- ¿Las tecnologías existente en el Ecuador están preparadas para adopción del Internet de las cosas? (Infraestructura, conectividad, despliegue)

RC: En este punto en el Ecuador quizás no se tenga una adopción rápida del IoT pero será algo que se ira introduciendo poco a poco, la infraestructura y conectividad que existe en el Ecuador deben mejorar mucho más para tener una adopción segura del IoT.

- ¿Qué mejoras implican estas innovaciones para todos?

RC: Las mejoras son muchas tanto en salud sensores que dan datos sobre nuestro estado de salud, administración pública para la gestión de semáforos y parqueos de las ciudades, entornos de hogares inteligentes automatizados, edificios que de alguna manera van a cambiar la forma de vida de todas las personas.

- ¿Cómo se pueden aprovechar las empresas Ecuatorianas del Internet de las Cosas?

RC: Es una nueva tecnología y deben aprovecharla de cierta manera para mejorar la calidad de vida y ser un poco más nobles con el medio ambiente, debido a que esta tecnología nos permite estar en contacto con todo lo que queramos y poder administrar de mejor manera los recursos.

- ¿Cómo ves la participación de las empresas públicas y privadas en la adopción del Internet de las cosas?

RC: Tanto para empresas vendedoras como las consumidoras de tecnología deben apuntar al cambio constante y adaptarse a ellos, siempre tomando las medidas de seguridad correspondiente para tener éxito.

- ¿Cuáles son los mayores retos a los que nos enfrentamos en el Internet de las cosas?

RC: Los mayores restos a los que nos enfrentamos con el Internet de las Cosas son la privacidad y la seguridad, ya que son partes fundamentales de la integridad de la información que se maneja.

- En el campo que laboras conoces de alguna implementación con objetos inteligentes que se haya llevado a cabo. ¿Cuál? ¿Qué impacto tubo? ¿Existe alguna en proyecto?

RC: No se ha realizado ninguna hasta el momento.

5.2 Validación de hipótesis

Según los resultados de estudio, se realiza la validación correspondiente de la hipótesis.

Se planteó esta hipótesis la cual es una posible respuesta al problema planteado y posee una íntima relación entre el problema y el objetivo.

Hipótesis

La seguridad y la privacidad serán factores favorables para la adopción del IoT.

Se realizó el análisis respectivo para validar esta hipótesis debido a que la seguridad y privacidad son factores que aún se deben madurar para asegurar al usuario que va hacer beneficiado ofreciendo el 99.999% de seguridad de cualquier fallo que incluya infiltración de datos, bloqueos del sistema o alteración de información confidencial, el cual se obtuvo los siguientes resultados.

- ✓ La investigación del Internet de las Cosas y las consideraciones de seguridad permitirán que las diferentes instituciones puedan hacer uso de esta tecnología en beneficio de determinadas actividades.
- ✓ Usando los diferentes mecanismos de seguridad del Internet de las Cosas se fomentará el desarrollo e implementación de esta tecnología en ambientes hostiles.
- ✓ Esta solución favorecería a los diferentes niveles de la sociedad, gobierno, empresas y ciudadanos, brindando niveles de seguridad de la información que se transportan por las redes y dispositivos dentro de un entorno IoT.
- ✓ Esta solución permitirá que las diferentes empresas, niveles de gobierno y usuarios finales estén a la vanguardia de la tecnología, y que los involucrados en este tipo de desarrollo tecnológico puedan consultar y controlar en línea los diferentes acontecimientos desde cualquier lugar remoto del mundo.
- ✓ Mediante un registro de incidencia la disponibilidad de entornos IoT críticos es alta debido a que se mantiene un control global de los objetos permitiendo tener redundancia entre ellos.

- ✓ Uno de los inconvenientes que se tiene en la adopción del Internet de las Cosas es la falta de una cultura de seguridad en los usuarios finales, al no comprender los riesgos sobre la manipulación de los dispositivos y datos, ocasionando perdida de información sensible y comprometimiento de dispositivos conectados a la red.
- ✓ Para que esta solución tenga una correcta adopción sociedad tecnológica se debe socializar y poner a disposición la información permitiendo a los grupos de interés brindar un mejor servicio.

Se cumplió con los tres objetivos ya que se investigó las debilidades y amenazas que presenta el Internet de las Cosas, costos asociados a integrar seguridad en los entornos y objetos IoT mediante entrevistas, análisis bibliográfico.

Para el cumplimiento del primer objetivo se realizó una investigación para definir las debilidades y amenazas que presenta el Internet de las Cosas, en relación a la seguridad.

- ➢ ¿Cómo de inteligentes son las cosas hoy día? Situación actual de una tecnología prometedora.
- ➢ El impacto del Internet de las Cosas en los negocios y la sociedad.
- ➢ Factores determinantes en el futuro del Internet de las Cosas.
- ➢ Análisis de información determinante a la seguridad.
- ➢ Niveles de seguridad.

Para el cumplimiento del segundo objetivo

- ➢ Entendiendo las tres capas básicas del Internet de las Cosas.
- ➢ Proyecto de seguridades inteligentes.

- Consideraciones de costos asociados a la implementación del internet de las cosas.
- Costos asociados a la seguridad de los objetos.

Para el cumplimiento del tercer objetivo

- ¿Cómo de inteligentes son las cosas hoy día? Situación actual de una tecnología prometedora.
- Entendiendo las tres capas básicas del Internet de las Cosas
- El impacto del Internet de las Cosas en los negocios y la sociedad
- Factores determinantes en el futuro del Internet de las Cosas
- Sistema Operativo Contiki
- Análisis de información determinante a la seguridad
- Niveles de seguridad
- Componentes IoT
- Esquema de seguridad para un entorno de IoT
- Análisis de los componentes del esquema
- Componentes de un objeto inteligente
- Esquema de seguridad de un dispositivo IoT

En la ejecución de este proyecto de tesis se pudo indicar las oportunidades y fortalezas que se tendrían en la ejecución del Internet de las Cosas y las consideraciones de seguridad.

5.3 Conclusiones

El Internet de las Cosas cambiara radicalmente la forma de comunicarnos con nuestro entorno y específicamente con los objetos, es una tecnología prometedora que ha llegado para mejorar la calidad de vida de los seres humanos en diferentes ámbitos, tales como conservación del ecosistema, administración y ahorro de recursos vitales (energía, agua, gas), equipamiento médico para el control de enfermedades, sistemas de parqueo para vehículos, sistemas de geo-localización de objetos, vehículos inteligentes, entre otros; todo conectado de forma que cada objeto brinde un beneficio importante a los grupos de interés que lo requieran.

La seguridad es un factor primordial para el Internet de las Cosas, debido a que no solo se habla de operaciones financieras que se pueden abordar a través de sanciones en caso de que exista una fuga de datos. Aquí estamos hablando de sistemas cuya infiltración podría conducir a la pérdida de vidas humanas o causar la interrupción masiva de la sociedad, es decir en los casos donde existan objetos de los cuales personas dependan de él y estos sean susceptibles a ataques, como los dispositivos médicos conectados a una persona que pueden ser vulnerables comprometiendo su vida, vehículos a los cuales se podrían infiltrar realizando alguna acción no controlada por el conductor provocando algún accidente, sistemas de control de tráfico terrestre, aéreo o marítimo que pueden generar caos o algún atentado de mayor magnitud. Todo esto tiene que ser considerado en un nivel básico como es el de la concienciación de la seguridad, para ser adoptados de manera sólida.

Este estudio claramente identifica que los desarrolladores de esta tecnología deben considerar la seguridad durante la concepción y desarrollo de productos IoT dependiendo del entorno en el que vayan hacer implementados. Si no se hace, existe el riesgo de que los futuros sistemas sean susceptibles y vulnerables a ataques cibernautas como los que existen hoy en día, debido a que la mayoría de objetos no fueron concebidos para estar en un entorno conectado al Internet.

Se identificó un esquema de seguridad para entornos IoT, donde están involucrados componentes como dispositivos/sensores, puertas de enlaces, canales de transporte, facilitación/plataformas de recolección de información y aplicaciones que permiten ver la información estructurada. El segundo esquema se lo propone con una visión más específica orientado al objeto o dispositivo, en este involucra componentes como microcontroladores, firmware, sensores/actuadores, alimentación, conectividad, sistema operativo y aplicaciones; cada uno de estos componentes en ambos esquemas juegan un papel muy importante en la seguridad del IoT, enmarcados en las respectivas capas de seguridad que se deben tener en cada nivel o etapa, de esta manera se puede lograr una seguridad integral tanto en el objeto como en un entorno IoT.

El Open Source Hardware/Software son comunidades online de colaboración donde se encuentran involucrados profesionales, estudiantes, usuarios, miembros de empresas de tecnologías, siendo el lugar propicio para compartir diferentes conocimientos en ámbitos de tecnología permitiendo integrar de manera variada experiencias sobre soluciones a problemas presentados y proponer temas de

discusión de los cuales sacar beneficio, todo esto crea una base de conocimiento compartido adecuado para desarrollar mejores alternativas de solución a ciertas vulnerabilidades detectadas en objetos, dispositivos o sistemas.

La investigación realizada sirve de aporte base para la adopción e implementación del Internet de las Cosas, en donde las empresas y grupos de interés puedan fomentar la confianza en los usuarios creando objetos y entornos IoT seguros inherentes al beneficio que aporta para mejorar su calidad de vida.

5.4 Recomendaciones

Se recomienda implementar dentro de la red de Internet de las Cosas sistemas de incidencias que envíen notificación de manera inmediata si un objeto sufrió algún desperfecto o avería para que se pueda pasar el control de forma automática a otro objeto redundante y mantener operativo todos los objetos con mayor nivel de importancia en ambientes donde se maneje información sensible.

Que las empresas ecuatorianas al incursionar en el desarrollo e implementación de entornos IoT, deberán generar confianza y seguridad en los clientes con la finalidad de garantizar la integridad, estabilidad, seguridad, privacidad y funcionabilidad de la información, orientándose a casos de éxito o enfocándose a la relación costo beneficio, que le permitan ganar prestigio generando confianza.

Que los organismos nacionales e internacionales reguladores de las telecomunicaciones como el MINTEL, IEEE, ITU, IETF, ISOC e ISO generen políticas y procedimientos de seguridad solidos que permitan salvaguardar la integridad física y lógica con fuertes estándares de cumplimiento.

Para que esta tecnología tenga éxito y de frutos es necesario, que los usuarios del Internet de las Cosas puedan permanecer siempre en control de sus datos y deben saber claramente cómo y para qué se van a utilizar los mismos. Dando su consentimiento expreso tras recibir la información de forma clara y transparente, lo que contribuirá a las bases del éxito de esta tecnología.

Los esquemas pueden ser mejorados en base a las experiencias que se generen en cada uno de los niveles o capas, por lo que una parte también importante es registrar y reportar, registro forense, auditorias donde se generan novedades que ayudan a mejorar los esquemas de seguridad, creando un ciclo retroalimentación constante de mejora.

BIBLIOGRAFÍA

[1] Unión Internacional de Telecomunicaciones (UIT) - Ministerio de Ciencia y Tecnología. (s.f.). La Sociedad de la Información en el siglo XXI: un requisito para el desarrollo. España.

[2] Gutiérrez, G. (13 de agosto de 2013). *creascion.com*. Recuperado el 02 de octubre de 2013, de http://creascion.com/los-problemas-que-enfrenta-el-internet-de-las-cosas/

[3] Delclós, T. (17 de Mayo de 2007). *elpais.com*. Recuperado el 03 de Octubre de 2013, de http://elpais.com/diario/2007/05/17/ciberpais/1179368665_850215.html

[4] Díaz, J., Demasi, M., Robles, M., & Vodopivec, G. (s.f.). *SEDICI Repositorio Digital de la UNLP*. Recuperado el 5 de Octubre de 2013, de http://sedici.unlp.edu.ar/bitstream/handle/10915/20873/Documento_completo.pdf?sequence=1

[5] Fundación de la Innovación Bankinter. (2011). *fundacionbankinter.org*. Recuperado el 3 de Octubre de 2013, de http://www.fundacionbankinter.org/system/documents/8168/original/XV_FTF_El_internet_de_las_cosas.pdf

[6] Evans, D. (2011). *Internet de las cosas.* San José, CA: Cisco Internet Business Solutions Group (IBSG).

[7] IBER GROUP IT. (s.f.). *http://iber-group.com/*. Recuperado el 05 de Octubre de 2013, de http://iber-group.com/Infraestructura/Tecnologias/RFID/

[8] Paniagua, S. (15 de Abril de 2012). *sorayapaniagua.com*. Recuperado el 03 de Octubre de 2013, de http://www.sorayapaniagua.com/2012/04/15/internet-de-las-cosas-nube-datos-ipv6-y-algoritmos/

[9] Redes de Telecomunicaciones y seguridad de la Información. (s.f.). *http://resdesycomunicaciones2.blogspot.com/*. Recuperado el 09 de 02 de 2013, de http://resdesycomunicaciones2.blogspot.com/2014/12/la-internet-de-las-cosas-no-necesitara.html

[10] Gallego, N. (28 de octubre de 2013). *http://www.norbertogallego.com/*. Recuperado el 01 de abril de 2014, de http://www.norbertogallego.com/internet-de-las-cosas-numeros-de-vertigo/2013/10/28/

[11] Accenture 2005. (s.f.). *http://www.accenture.com/SiteCollectionDocuments/pdf/sensortelemetry.pdf*. Recuperado el 04 de febrero de 2014, de http://www.accenture.com/SiteCollectionDocuments/pdf/sensortelemetry.pdf

[12] Beecham Research. (12 de julio de 2011). *http://www.beechamresearch.com/*. Recuperado el 10 de octubre de 2014, de http://blog.m2mapps.com/: http://blog.m2mapps.com/2011/07/12/welcome-to-our-new-blog-provided-in-association-with-m2mapps/

[13] Jimenez, M. (12 de agosto de 2014). *http://noticiaslogisticaytransporte.com/*. Recuperado el 30 de noviembre de 2014, de http://noticiaslogisticaytransporte.com/logistica/12/08/2014/expertos-creen-que-iot-mejorara-la-cadena-de-suministro/28572.html

[14] Penalva, J. (25 de enero de 2011). *http://www.xataka.com/*. Recuperado el 08 de septiembre de 2014, de http://www.xataka.com/moviles/nfc-que-es-y-para-que-sirve

[15] ITU News. (junio de 2013). *https://itunews.itu.int*. Recuperado el 13 de marzo de 2014, de https://itunews.itu.int/es/4503-Internet-de-las-cosas-Maquinas-empresas-personas-todo.note.aspx

[16] Jurado Pérez, L. A., Velásquez Vargas, W. A., & Vinueza Escobar, N. F. (2014). *http://www.academia.edu/.* Recuperado el 02 de noviembre de 2014, de http://www.academia.edu/7197061/Estado_del_Arte_de_las_Arquitecturas_de_Internet_de_las_Cosas_IoT_

[17] LogicFin. (s.f.). *http://logic-fin.com/*. Recuperado el 15 de noviembre de 2014, de http://logic-fin.com/analisis-del-sector-internet-de-las-cosas-en-la-fabricacion/

[18] Marketing Directo. (31 de mayo de 2013). *http://www.marketingdirecto.com/*. Recuperado el 25 de enero de 2014, de http://www.marketingdirecto.com/especiales/mobile-marketing-blog/la-penetracion-de-smartphones-ya-supera-el-50-en-los-grandes-mercados-de-todo-el-mundo/

[19] Tim, O., & John, B. (20 de octubre de 2009). *http://www.web2summit.com/.* Recuperado el 10 de abril de 2014, de http://www.web2summit.com/web2009/public/schedule/detail/10194

[20] Foundation California Healthcare. (2010). *How Smartphones Are Changing Health Care for Consumers and Providers.*

[21] Reyes, F. (30 de abril de 2012). *http://www.technologyreview.es/*. Recuperado el 10 de abril de 2014, de http://www.technologyreview.es/read_article.aspx?id=40314

[22] EcuRed. (28 de diciembre de 2013). *http://www.ecured.cu*. Recuperado el 12 de abril de 2014, de http://www.ecured.cu/index.php/Robert_Metcalfe

[23] Muy Interesante. (01 de junio de 2006). *http://www.muyinteresante.es*. Recuperado el 23 de agosto de 2014, de http://www.muyinteresante.es/tecnologia/preguntas-respuestas/icomo-seran-los-ordenadores-cuando-se-llegue-al-limite-de-miniaturizacion

[24] Continental Automated Buildings Association. (2008). *Internet of Things in 2020.*

[25] Área Tecnología. (s.f.). *http://www.areatecnologia.com*. Recuperado el 12 de abril de 2014, de http://www.areatecnologia.com/tecnologia/lte.html

[26] ISon21. (18 de diciembre de 2010). *http://www.ison21.es*. Recuperado el 13 de abril de 2014, de http://www.ison21.es/2010/12/18/china-cambiara-cabinas-telefonicas-por-puntos-de-acceso-wifi/

[27] Cisco Systems, Inc. (2013). *Informe Anual de Seguridad de Cisco 2013.*

[28] Cisco Systems, Inc. (2014). *Informe de Seguridad de Cisco 2014.*

[29] Comisión Europea. (2009). *Internet of Things Strategic Research Roadmap.*

[30] Yirá, F. (12 de julio de 2014). *http://www.xatakawindows.com*. Recuperado el 20 de agosto de 2014, de http://www.xatakawindows.com/windows/microsoft-lanza-su-programa-de-desarrolladores-para-el-internet-de-las-cosas

[31] Pastor, J. (22 de septiembre de 2014). *http://www.xataka.com*. Recuperado el 10 de octubre de 2014, de http://www.xataka.com/accesorios/mediatek-lanza-su-plataforma-para-el-desarrollo-des-wearables-y-de-la-internet-de-las-cosas

[32] Perea, C. (19 de diciembre de 2014). *http://americaeconomia.com*. Recuperado el 28 de diceimbre de 2014, de http://americaeconomia.com/analisis-opinion/las-empresas-deben-avanzar-al-ritmo-del-internet-de-las-cosas

[33] TyN Megazine. (s.f.). *http://www.tynmagazine.com*. Obtenido de http://www.tynmagazine.com/internet-of-things-y-su-impacto-en-los-negocios/

[34] Penalva, J. (01 de abril de 2013). *http://www.xataka.com*. Recuperado el 14 de abril de 2014, de http://www.xataka.com/hogar-digital/el-bote-de-tus-medicinas-se-chivara-a-tu-medico-si-no-las-tomas

[35] Xataca. (s.f.). *http://www.xataka.com*. Recuperado el 14 de abril de 2014, de http://www.xataka.com/gadgets/domotica/chumby

[36] Green, E. (2011). *http://www.fundacionbankinter.org*. Recuperado el 13 de abril de 2014, de http://www.fundacionbankinter.org/es/videos/what-is-anywhere

[37] DIARIO ABC, S.L. (05 de septiembre de 2010). *http://www.abc.es*. Recuperado el 12 de junio de 2014, de http://www.abc.es/20100826/tecnologia/puede-mundo-convertirse-gran-201008261244.html

[38] Macmanus, R. (11 de septiembre de 2009). *http://readwrite.com*. Recuperado el 14 de abril de 2014, de http://readwrite.com/2009/09/10/top_5_web_trends_of_2009_internet_of_things#awesm=~oAV0mpWZWYBKG9

[39] Pomares, R. (22 de marzo de 2012). *http://www.cienciasambientales.com*. Recuperado el 13 de abril de 2014, de http://www.cienciasambientales.com/es/noticias-ambientales/sourcemap-3626

[40] Caminero, D. (16 de marzo de 2012). *http://www.aunclicdelastic.com*. Recuperado el 05 de mayo de 2014, de http://www.aunclicdelastic.com/internet-de-las-cosas-en-el-sector-de-la-automocion/

[41] Gutierrez, G. (05 de Agosto de 2013). *http://creascion.com*. Recuperado el 02 de Octubre de 2013, de http://creascion.com/5-cambios-al-futuro-que-producir-el-internet-de-las-cosas/

[42] Hirshberg, P. (12 de junio de 2012). *http://tecnologia.elpais.com*. Recuperado el 13 de mayo de 2014, de http://tecnologia.elpais.com/tecnologia/2012/06/12/actualidad/1339513417_979445.html

[43] IOT SIMPLE S.A. (s.f.). *http://www.iotsimple.com*. Recuperado el 20 de octubre de 2014, de http://www.iotsimple.com/seguridad-en-iot/

[44] Indra Sistemas S.A. (2011). *http://www.indracompany.com*. Recuperado el 14 de abril de 2014, de http://www.indracompany.com/sostenibilidad-e-innovacion/proyectos-innovacion/ciudad-2020-hacia-un-nuevo-modelo-de-ciudad-intelig

[45] Europa press. (01 de junio de 2011). *http://www.europapress.es*. Recuperado el 20 de marzo de 2014, de

http://www.europapress.es/chance/tendencias/noticia-ciudades-inteligentes-tecnologia-servicio-ciudadano-20110601130049.html

[46] Gonzalez, A. (14 de julio de 2014). *http://lasproximasdecadas.blogspot.co*. Recuperado el 20 de julio de 2014, de http://lasproximasdecadas.blogspot.com/2012/01/2050-70-poblacion-vivira-en-ciudades.html

[47] HOY digital. (02 de mayo de 2013). *http://www.hoy.com.ec*. Recuperado el 16 de abril de 2014, de http://www.hoy.com.ec/noticias-ecuador/quito-en-mapa-de-ciudades-inteligentes-580207.html

[48] La Comunidad de RFID en Latinoamerica. (s.f.). *http://www.rfidpoint.com*. Recuperado el 17 de abril de 2014, de http://www.rfidpoint.com/consulte-al-experto/%C2%BFcuanto-cuestan-los-tags-rfid/

[49] Préstamo, J. (10 de junio de 2014). *http://www.teknoplof.com*. Recuperado el 30 de julio de 2014, de http://www.teknoplof.com/2014/06/10/el-sistema-operativo-contiki-ese-gran-desconocido-tan-cercano/

[49] TeknoPlof! (10 de junio de 2014). *http://www.teknoplof.com*. Recuperado el 23 de julio de 2014, de http://www.teknoplof.com/2014/06/10/el-sistema-operativo-contiki-ese-gran-desconocido-tan-cercano/

[50] Wikipedia. (s.f.). *http://en.wikipedia.or*. Obtenido de http://en.wikipedia.org/wiki/Contiki

[51] Evans, D. (s.f.). *http://www.cisco.com*. Recuperado el 20 de julio de 2014, de http://www.cisco.com/web/ES/campaigns/internet-de-las-cosas/index.html?CAMPAIGN=fy13-spain-internetofeverything&COUNTRY_SITE=us&REFERRING_SITE=cisco-

spain-website&POSITION=cisco+link&CREATIVE=cisco-spain-seo-page-tab3#~tab-tab1

[52] Centro Nacional de Tecnologías de la Accesibilidad - CENTAC. (05 de noviembre de 2013). *www.youtube.com*. Recuperado el 20 de julio de 2014, de https://www.youtube.com/watch?v=GYqgglLXhHM

[53] Universidad Rey Juan Carlos. (11 de novimbre de 2014). *www.youtube.com*. Recuperado el 21 de julio de 2014, de https://www.youtube.com/watch?v=IfbnDf1WD6s

[54] HangoutON. (29 de abril de 2014). *www.youtube.com/*. Recuperado el 24 de julio de 2014, de https://www.youtube.com/watch?v=ufQyuHTKs0Q

[55] Oppenheimer, A. (26 de junio de 2014). *www.youtube.com*. Recuperado el 27 de julio de 2014, de https://www.youtube.com/watch?v=QE64J7S3-eg

[56] Celorio Lucas, D. G. (6 de septiembre de 2014). El Internet de las cosas y las consideraciones de seguridad. (F. G. Cuzme Rodríguez, Entrevistador)

[57] Bucheli López, V. (12 de septiembre de 2014). El Internet de las cosas y las consideraciones de seguridad. (F. G. Cuzme Rodríguez, Entrevistador)

[58] Castellanos, R. (15 de septiembre de 2014). El Internet de las cosas y las consideraciones de seguridad. (F. G. Cuzme Rodríguez, Entrevistador)

[59] Jayavardhana, G., Rajkumar, B., Slaven, M., & Marimuthu, P. (24 de Febrero de 2013). *http://www.sciencedirect.com/.* Recuperado el 2015 de Enero de 28, de http://www.sciencedirect.com/science/article/pii/S0167739X13000241#

[60] Vargas, L. (16 de mayo de 2013). *http://www.cabume.co.uk*. Obtenido de http://www.cabume.co.uk/hardware/logmein-and-arm-offer-iot-innovation-starter-kits.html

[61] CIO América Latina. (24 de octubre de 2013). *http://www.cioal.com*. Obtenido de http://www.cioal.com/2013/10/24/lo-que-el-internet-de-las-cosas-representa-para-la-seguridad/

[62] López Hernández, J. M. (27 de agosto de 2004). *http://ibiblio.org*. Obtenido de http://ibiblio.org/pub/linux/docs/LuCaS/Manuales-LuCAS/doc-como-seguridad-fisica/html_out/laseguridadfisicadelhardwar.html

[63] Borghello, C. (s.f.). *https://www.segu-info.com.ar*. Obtenido de https://www.segu-info.com.ar/logica/seguridadlogica.htm

[64] Ferrer, J., & Fernández, J. (s.f.). *http://es.tldp.org/.* Obtenido de http://es.tldp.org/Informes/informe-seguridad-SL/informe-seguridad-SL.pdf

[65] Monzon, A. (15 de julio de 2012). *http://maestriainformaticamg.blogspot.com.* Obtenido de http://maestriainformaticamg.blogspot.com/2012/07/tema-2-necesidad-de-la-seguridad.html

[66] Alberca Jaquero, C. (17 de marzo de 2014). *https://www.incibe.es/.* Obtenido de https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/Internet_of_things_ciberseguridad

[67] Gartner, Inc. (25 de junio de 2012). *http://www.gartner.com/*. Recuperado el 17 de 10 de 2014, de http://www.gartner.com/newsroom/id/2060215

[68] ESET Latinoamérica. (2014). *http://www.eset-la.com/.* Obtenido de http://www.eset-la.com/pdf/tendencias_2014_el_desafio_de_la_privacidad_en_internet.pdf

[69] Lyne, J. (diciembre de 2011). *http://www.sophos.com/.* Obtenido de http://www.sophos.com/es-

es/medialibrary/gated%20assets/white%20papers/sophosnetworksecuritytoptrendswpna.pdf

[70] Medina, J. (04 de marzo de 2014). *http://asmarterplanet.com/*. Obtenido de http://asmarterplanet.com/es/seguridad-hasta-en-la-nevera/

[71] Borghello, C. (s.f.). *https://www.segu-info.com.ar*. Obtenido de https://www.segu-info.com.ar/politicas/costos.htm

[72] Ajit, J., & Sunil, M. C. (s.f.). *www.lnttechservices.com.* Obtenido de http://www.lnttechservices.com/media/30090/whitepaper_security-considerations-for-internet-of-things.pdf

GLOSARIO

ACL: Listas de Control de Acceso

BC: Continuidad en el Negocio

Backend: Plataforma de administración de sistemas.

CoAP: Protocolo de aplicación con restricciones.

C2S: Cliente a Sitio

DTLS: Seguridad en la capa de transporte de datagramas

DR: Recuperación de desastres

EPC: Ingeniería, Adquisición y Construcción

ECU: Unidad de Control Electrónico

Frontend: Interfaz donde se muestra el final de un proceso.

FDA: Administración de Alimentos y Medicamentos

GPS: Sistema de Posicionamiento Global

IaaS: Infraestructura como Servicio

IDS/IPS: Sistema de Detección de Intrusos/ Sistema de Prevención de Intrusos

ISO 27001: Organización Internacional de Normalización 27001 (Sistema de Gestión de Seguridad de la Información)

IoT: Internet de las Cosas

IKE: Intercambio de Claves en Internet

IPsec: Protocolo de Seguridad en Internet

MFA: Autenticación Multifactor

MULTIHOMING: Refiere a un dispositivo conectado a la red.

M2M: Maquina a Maquina

M2P: Maquina a Persona

NERC CIP: Corporación Norte Americana Confidencialidad Eléctrica Protección de Infraestructura Criticas

ONSHORE: Dentro de la línea de la costa o sobre ella.

OFFSHORE: Fuera de la línea de la costa, es decir mar adentro.

OWASP: Proyecto de Seguridad de Aplicaciones Web Abierta

PCI DSS: Industria de Tarjetas de Pago Estándar de Seguridad de Datos

PIPEDA: Ley de Protección de Información y Documentos Electrónicos Personal

PaaS: Plataforma como Servicio

RPL: Carga remota de programa inicial.

RFID: Identificación de Radio Frecuencia

SaaS: Software como Servicio

SAFEcode: Foro de Aseguramiento del Software para la Excelencia del Código

SANS/CWE: Instituto Administración de Sistemas, Auditoria, Redes y Seguridad/Enumeración de debilidad común

SSL: Capa de conexión segura

S2S: Sitio a Sitio

SIEM: Información de Seguridad y Administración de Eventos

SQL: Lenguaje de Consulta Estructurado

SSH: Interprete de Órdenes Seguras

TLS: Seguridad de la capa de transporte

UHF: Frecuencia Ultra alta

VNC: Computación Virtual en Red

VPN: Red Privada Virtual

WEP: Privacidad Equivalente a Cableado

WPA/WPA2: Acceso Wi-Fi Protegido / Acceso Wi-Fi Protegido versión 2

XSS: Secuencias de comandos en sitios cruzados

6LoWpan: Redes Inalámbricas de Área personal de baja potencia con protocolo IPV6.

6LBR: 6LoWPAN Border Router basado en Contiki, proyecto dedicado al IoT.

ANEXOS

ANEXO A

MODELO DE PREGUNTAS DE ENTREVISTA

Entrevistador: Fabián Geovanny Cuzme Rodríguez

Entrevistado:

Fecha de realización:

- ¿Qué es el internet de las cosas?
- ¿Qué beneficios consideras que traería la adopción del internet de las cosas?
- ¿Qué seguridades se deberían considerar en los objetos? (Hardware y software)
- ¿Qué seguridades deberían tener las plataformas de almacenamiento, control, administración de los objetos inteligentes?
- ¿Qué seguridades se deben tener en las redes de comunicación que interconectan los objetos?
- ¿Qué medidas se deberían tomar para que las empresas generen confianza en sus clientes para la adopción del Internet de las cosas?
- ¿Las tecnologías existente en el Ecuador están preparadas para adopción del Internet de las cosas? (Infraestructura, conectividad, despliegue)
- ¿Qué mejoras implican estas innovaciones para todos?
- ¿Cómo se pueden aprovechar las empresas Ecuatorianas del Internet de las Cosas?
- ¿Cómo ves la participación de las empresas públicas y privadas en la adopción del Internet de las cosas?

- ¿Cuáles son los mayores retos a los que nos enfrentamos en el Internet de las cosas?
- En el campo que laboras conoces de alguna implementación con objetos inteligentes que se haya llevado a cabo. ¿Cuál? ¿Qué impacto tubo? ¿Existe alguna en proyecto?

Firma del Entrevistador ***Firma de Entrevistado***

ANEXO B

OFICIO DIRIGIDO AL ALCALDE DE PORTOVIEJO

T 144478

Directo de informatica
Buchelly Lopez Carlos
Mendoza Kewin
PS2301.

Portoviejo, 09 de septiembre de 2014

Ingeniero
Agustín Casanova Cedeño
ALCALDE DE LA GAD PORTOVIEJO
Ciudad.-

De mi consideración

Reciba usted un cordial saludo y deseándole éxitos en las funciones que usted acertadamente dirige, la presente es para solicitar su autorización y disposición al Jefe del Dpto. de Tecnologías para realizar una entrevista sobre temas relacionados al Internet de los Objetos.

Le comento un poquito de lo que estoy realizado, soy egresado de la Universidad Pontificia Católica del Ecuador de la Maestría de Redes de Comunicación y como proyecto de titulación he presentado como tema "El Internet de las Cosas y las Consideraciones de Seguridad".

Como esto involucra también las ciudades inteligentes o smart city, quisiera saber si como GAD llevan algún provecto de este tipo o si tienen pensando hacerlo.

Por tal motivo quisiera la apertura para realizar la entrevista, para el día Jueves 11 de septiembre de 2014, en el horario que ustedes consideren.

Esperando que mi petición tenga una respuesta favorable, le quedo de antemano muy agradecido.

Atentamente,

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN PORTOVIEJO
09 SEP 2014
Hora: 12:10
Recibido por:

Fabián Geovanny Cuzme Rodríguez
C.C. 1311527012
Email: fabiancuzme@gmail.com; fabiancuzme@hotmail.es
Twitter: @farcu26
Celular: 0994564714

ANEXO C

ENTREVISTA AL ING. DARWIN CELORIO, JEFE DE SISTEMAS DEL BANCO COMERCIAL DE MANABÍ

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

ENTREVISTA

Entrevistador: Fabián Geovanny Cuzme Rodríguez

Entrevistado: Ing. Darwin Geovanny Celorio Lucas

Ingeniero en Sistemas – Jefe de Sistemas del Banco Comercial de Manabí

Fecha: 06/09/2014

1. **¿Qué es el internet de las cosas?**

   DC: Medio de intercomunicación, relación, interacción de variedad de herramientas que tiene como objetivo facilitar las cosas a los usuarios finales.

2. **¿Qué beneficios consideras que traería la adopción del internet de las cosas?**

   DC: Evolución para la aplicación de la tecnología.

3. **¿Qué seguridades se deberían considerar en los objetos? (Hardware y software)**

   DC: Totalmente siempre se debe considerar la seguridad en informática en cual ambiente que este propiciando mejoras y avances tecnológicos.

4. **¿Qué seguridades deberían tener las plataformas de almacenamiento, control, administración de los objetos inteligentes?**

   DC: Las plataforma de o debe implementar sistemas de encriptación, los de control manejo seguros de certificados y claves, y los de administración de objeto inteligentes debe estar bajo estándares que garantice las seguridades.

5. **¿Qué seguridades se deben en las redes de comunicación que interconectan los objetos?**

   DC: Es crucial en sistema de red de cualquier topología manejar Firewall, certificados seguros.

6. **¿Qué medidas se deberían tomar para que las empresas generen confianza en sus clientes para la adopción del Internet de las cosas?**

   DC: Debe implementar buenas prácticas de TI, aplicando estándares internacionales, ante todo certificarse. Esto lograra que se genere confianza en los clientes y atraerá más.

ENTREVISTA

7. **¿Las tecnologías existente en el Ecuador están preparadas para adopción del Internet de las cosas? (Infraestructura, conectividad, despliegue)**

   DC: Actualmente se ha notado que el Ecuador en materia de Tecnología está en proceso de cambio y esto es síntoma de que se está preparando para el avance y evolución tecnológica.

8. **¿Qué mejoras implican estas innovaciones para todos?**

   DC: Aparecen nuevas formas de comunicarnos y estar más cercas de familias, amigos, etc. En fin aquello que antes era distante en la actualidad se acorta.

9. **¿Cómo se pueden aprovechar las empresas Ecuatorianas del Internet de las Cosas?**

   DC: Creando nuevas herramientas y nuevos servicios para brindar a sus clientes. La oportunidad de invertir en tecnología y obtener nuevos ingresos.

10. **¿Cómo ves la participación de las empresas públicas y privadas en la adopción del Internet de las cosas?**

    DC: Hoy en día todo lo que nos rodea tiene alguna relación con el Internet. La empresas cada vez se interesan más en el internet y su evolución e incluso ya existe dentro de las empresas departamentos solo dedicados a investigar esta tan fabulosa herramientas y sus bondades.

11. **¿Cuáles son los mayores retos a los que nos enfrentamos en el Internet de las cosas?**

    DC: Uno de los mayores retos es el saberle darle buen uso aquellos componentes y herramientas que acompaña en el día. El no dejarnos dominar por aquellas cosas que parecen indispensables.

12. **En el campo que laboras conoces de alguna implementación con objetos inteligentes que se haya llevado a cabo. ¿Cuál? ¿Qué impacto tubo?**

    DC: Aún no hemos tenido la implementación de componentes inteligentes.

Firma del Entrevistador ***Firma de entrevistado***

ENTREVISTA AL ING. VINICIO BUCHELI, DIRECTOR DE SISTEMAS DEL GAD-PORTOVIEJO

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

ENTREVISTA

Entrevistador: Fabián Geovanny Cuzme Rodríguez

Entrevistado: Ing. Vinicio Bucheli López – Director de Informática del GAD-Portoviejo

Ingeniero en Sistemas Informáticos

Diplomado en Seguridades Informática en Instituto Tecnológico de Monterrey.

Realizado Maestría en Gestión de Sistemas en la ESPE

Certificaciones:

Informática Forense REDLIFE

ISO 27001 Fundación UNED

Seguridad ISACA

Realizando una certificación en COBIT

Fecha de realización: 12/09/2014 **Hora:** 08H00

1. ¿Qué es el internet de las cosas?
   VB: Es la definición de tener objetos comunes y corrientes conectados a internet realizando alguna actividad específica.
2. ¿Qué beneficios consideras que traería la adopción del internet de las cosas?
   VB: Importante en cuanto a la reducción de costos y tener una administración de dispositivos eficaz y eficiente.
3. ¿Qué seguridades se deberían considerar en los objetos? (Hardware y software)
   VB: Esto va a depender del objeto que se desea administrar, se pueden definir seguridades como VPN, seguridad perimetral, encriptación de información, entre otros.
4. ¿Qué seguridades se deben tener en las redes de comunicación que interconectan los objetos?
   VB: Las redes de comunicación deben asegurar que la comunicación permanezca estable siempre, para que los datos se puedan transmitir. Se pueden aplicar sistemas de encriptación para que los datos que sean interceptados en la red no sean desencriptados por personas mal intencionadas.
5. ¿Qué medidas se deberían tomar para que las empresas generen confianza en sus clientes para la adopción del Internet de las cosas?
   VB: Depende del nivel cultural, que tenga experiencia y trayectoria de la misma, para el usuario tenga confianza en la adopción del IoT.
6. ¿Las tecnologías existente en el Ecuador están preparadas para adopción del Internet de las cosas? (Infraestructura, conectividad, despliegue)
   VB: En su totalidad si está preparando se está orientado y se está preparando en desarrollar soluciones con tecnologías en internet.

7. ¿Qué mejoras implican estas innovaciones para todos?
   VB: Entregar un mejor servicio a la ciudadanía, reducir costos dentro de la empresa y ser más eficaz y eficiente. Por ejemplo si un trabajo lo hacían 10 personas y con tecnología solo utilizo uno se está abaratando costos.
8. ¿Cómo se pueden aprovechar las empresas Ecuatorianas del Internet de las Cosas?
   VB: Desarrollando tecnología que sea útil para las personas y empresas que lo utilicen.
9. ¿Cómo ves la participación de las empresas públicas y privadas en la adopción del Internet de las cosas?
   VB: En Ecuador se han visto algunos proyectos innovadores de domótica con dispositivos móviles y aplicaciones para Smartphone.
10. ¿Cuáles son los mayores retos a los que nos enfrentamos en el Internet de las cosas?
    VB: Costos por los despliegues de las redes de comunicación que aún son altos y de las plataformas de administración, hay empresas o personas que no cuentan con los recursos para acceder a estas tecnologías innovadoras.
11. En el campo que laboras conoces de alguna implementación con objetos inteligentes que se haya llevado a cabo. ¿Cuál? ¿Qué impacto tubo? ¿Qué proyectos se están planteando en el GAD?
    VB: La implementación de la Smart City en la ciudad de Portoviejo que se desea llevar a cabo con la implementación de cámaras inteligentes, sistemas de parqueo inteligente y otras más que permitirán un mejor vivir a los ciudadanos de esta ciudad.

Firma del Entrevistador

Firma del Entrevistado

ENTREVISTA AL ING. VINICIO BUCHELI, DIRECTOR DE SISTEMAS DEL GAD-PORTOVIEJO

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

ENTREVISTA

Entrevistador: Fabián Geovanny Cuzme Rodríguez

Entrevistado: Ing. Rodney Fabian Castellanos Cauja

Especialistas de Proceso y Control de Calidad

Empresa: BUPARTECH

Fecha: 08-09-2014

1. ¿Qué es el internet de las cosas?
   RC: Es lograr tener una conexión entre todas las cosas que nos rodea y lograr tener una comunicación basado en eso para nuestro beneficio, basado en las tecnologías y comunicaciones que actualmente tenemos.

2. ¿Qué beneficios consideras que traería la adopción del internet de las cosas?
   RC: El mayor beneficio que todos tendría es la optimización de tiempo en todas nuestras actividades, ósea minimizar los tiempos de respuesta en base a nuestras necesidades. Con estas conexiones vamos a tener más productividad en nuestras actividades diarias. Pero esto conlleva a tener una disponibilidad de los servicios, requiere que se tengan equipos de alto rendimiento de almacenamiento y procesamiento, y software que permita la administración de la información generada.

3. ¿Qué seguridades se deberían considerar en los objetos? (Hardware y software)
   RC: Considera una conjugación de seguridad de hardware y software, hay que ver la criticidad del sensor que se está manejando, se ve a los dos niveles como muy importantes y de alta prioridad para aplicar niveles de seguridad aceptables.

4. ¿Qué seguridades deberían tener las plataformas de almacenamiento, control, administración de los objetos inteligentes?
   RC: Se deben tener plataformas en las cuales se considere una seguridad de un 99,999% en diferentes niveles, que permitan tener confianza en la adopción del internet de las cosas, estas plataformas juegan un papel muy importante en esta adopción.

5. ¿Qué seguridades se deben tener en las redes de comunicación que interconectan los objetos?
   RC: Más que las seguridades en las redes lo que considera en tener la disponibilidad de la red, las seguridades se deberían aplicar a nivel de hardware o software que permitan colocar equipos o sistemas de criptografía, de control de permisos, accesos físicos y lógicos, generación de claves, accesos perimetrales. Esto permite asegurar los datos por la red y aunque los datos sean interceptados estos no sean descifrados.

6. ¿Qué medidas se deberían tomar para que las empresas generen confianza en sus clientes para la adopción del Internet de las cosas?
   RC: Las empresas deberán generar confianza a los clientes en base a los casos de éxito que la mayoría de empresas o personas van a pedir, esto es que a nuestro primer cliente mostrarle los beneficios y hacer que nuestro primer trabajo sea un trabajo exitoso.

7. ¿Las tecnologías existente en el Ecuador están preparadas para adopción del Internet de las cosas? (Infraestructura, conectividad, despliegue)
   RC: En este punto en el Ecuador quizás no se tenga una adopción rápida del IoT pero será algo que se ira introduciendo poco a poco, la infraestructura y conectividad que existe en el Ecuador deben mejorar mucho más para tener una adopción segura del IoT.

8. ¿Qué mejoras implican estas innovaciones para todos?
   RC: Las mejoras son muchas tanto en salud sensores que dan datos sobre nuestro estado de salud, administración pública para la gestión de semáforos y parqueos de las ciudades, entornos de hogares inteligentes automatizados, edificios que de alguna manera van a cambiar la forma de vida de todas las personas.

9. ¿Cómo se pueden aprovechar las empresas Ecuatorianas del Internet de las Cosas?
   RC: Es una nueva tecnología y deben aprovecharla de cierta manera para mejorar la calidad de vida y ser un poco más nobles con el medio ambiente, debido a que esta tecnología nos permite estar en contacto con todo lo que queramos y poder administrar de mejor manera los recursos.

10. ¿Cómo ves la participación de las empresas públicas y privadas en la adopción del Internet de las cosas?
    RC: Tanto para empresas vendedoras como las consumidoras de tecnología deben apuntar al cambio constante y adaptarse a ellos, siempre tomando las medidas de seguridad correspondiente para tener éxito.

11. ¿Cuáles son los mayores retos a los que nos enfrentamos en el Internet de las cosas?
    RC: Los mayores restos a los que nos enfrentamos con el Internet de las Cosas son la privacidad y la seguridad, ya que son partes fundamentales de la integridad de la información que se maneja.

12. En el campo que laboras conoces de alguna implementación con objetos inteligentes que se haya llevado a cabo. ¿Cuál? ¿Qué impacto tubo? ¿Existe alguna en proyecto?

RC: No se ha realizado ninguna hasta el momento.

Firma del Entrevistador

Firma de Entrevistado