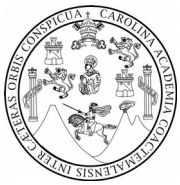


Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

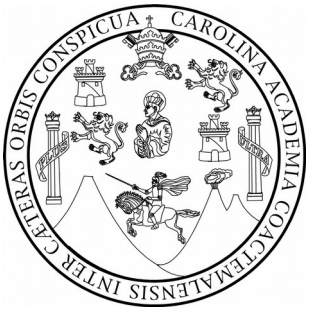
LA PRIVACIDAD DE LA INFORMACIÓN GENERADA POR DISPOSITIVOS DE DOMÓTICA EN EL INTERNET DE LAS COSAS

Diego Fernando Solis Franco

Asesorado por el Ing. Marlon Francisco Orellana López

Guatemala, octubre de 2016

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

LA PRIVACIDAD DE LA INFORMACIÓN GENERADA POR DISPOSITIVOS DE DOMÓTICA EN EL INTERNET DE LAS COSAS

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

DIEGO FERNANDO SOLIS FRANCO
ASESORADO POR EL ING. MARLON FRANCISCO ORELLANA LÓPEZ

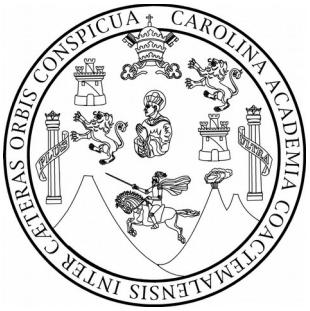
AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, OCTUBRE DE 2016

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA



NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Pedro Antonio Aguilar Polanco
VOCAL I	Ing. Angel Roberto Sic García
VOCAL II	Ing. Pablo Christian de León Rodríguez
VOCAL III	Inga. Elvia Miriam Ruballos Samayoa
VOCAL IV	Br. Raúl Eduardo Ticún Córdova
VOCAL V	Br. Henry Fernando Duarte García
SECRETARIA	Inga. Lesbia Magalí Herrera López

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Pablo Christian de León Rodríguez
EXAMINADOR	Ing. César Augusto Fernández Cáceres
EXAMINADOR	Ing. Herman Igor Véliz Linares
EXAMINADOR	Ing. José Ricardo Morales Prado
SECRETARIA	Inga. Lesbia Magalí Herrera López

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

LA PRIVACIDAD DE LA INFORMACIÓN GENERADA POR DISPOSITIVOS DE DOMÓTICA EN EL INTERNET DE LAS COSAS

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha 18 de marzo de 2015.

Diego Fernando Solis Franco

Guatemala, 3 de septiembre de 2015

Ingeniero
Carlos Alfredo Azurdia Morales
Escuela de Ingeniería en Ciencias y Sistemas
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

Ingeniero Azurdia:

Como asesor del trabajo de graduación del estudiante **Diego Fernando Solis Franco**, quien se identifica con carnet **201114424**, hago constar que finalizó satisfactoriamente el trabajo de investigación titulado: **"La privacidad de la información generada por dispositivos de domótica en el Internet de las cosas"**, el cual revisé y doy mi aprobación al mismo.

Atentamente,

Ing. Marlon Francisco Orellana López
Colegiado No. 8182

MARLON FRANCISCO ORELLANA LÓPEZ
INGENIERO EN CIENCIAS Y SISTEMAS
COL. 8182

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 30 de Septiembre de 2015

Ingeniero
Marlon Antonio Pérez Türk
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **DIEGO FERNANDO SOLIS FRANCO** con carné **2011-14424,** titulado: **"LA PRIVACIDAD DE LA INFORMACIÓN GENERADA POR DISPOSITIVOS DE DOMÓTICA EN EL INTERNET DE LAS COSAS",** y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE INGENIERÍA EN
CIENCIAS Y SISTEMAS
TEL: 24767644

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, del trabajo de graduación ***"LA PRIVACIDAD DE LA INFORMACIÓN GENERADA POR DISPOSITIVOS DE DOMÓTICA EN EL INTERNET DE LAS COSAS",*** *realizado por el estudiante DIEGO FERNANDO SOLIS FRANCO aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

Ing. Marlon Antonio Pérez Turk
Director
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 05 de octubre de 2016

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

DTG. 463.2016

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al Trabajo de Graduación titulado: **LA PRIVACIDAD DE LA INFORMACIÓN GENERADA POR DISPOSITIVOS DE DOMÓTICA EN EL INTERNET DE LAS COSAS,** presentado por el estudiante universitario: **Diego Fernando Solis Franco,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

Ing. Pedro Antonio Aguilar Polanco
Decano

Guatemala, octubre de 2016

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERÍA

/gdech

ACTO QUE DEDICO A:

Mi familia Porque “La familia que crece unida, permanece unida... para siempre.”

AGRADECIMIENTOS A:

Mis padres	Liliam Franco y Alfonso Solis, por todo su amor, apoyo incondicional y ejemplo de vida.
Mis hermanos	Diana y Rodrigo Solis, porque sin ustedes la vida no sería la misma.
Mis amigos	Ana Lucía López, Carlos Yoque, Erick Navarro, Hugo González y Jorge Flores, por todos los buenos y malos momentos que vivimos dentro y fuera de las aulas.
Mi asesor	Ing. Marlon Orellana, por su tiempo y sus consejos.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
$	Dólar estadounidense
kbps	Kilobit por segundo
MHz	Megahercio
%	Porcentaje

GLOSARIO

Automatización Consiste en el uso de máquinas o sistemas para controlar procesos.

Autonomía Capacidad de un sistema de tomar decisiones sin intervención humana.

Determinista Sistema en el que el azar no está involucrado en el funcionamiento del mismo.

Disruptivo Acción o situación que produce un cambio importante o determinante.

Domótica Sistemas que buscan usar dispositivos y tecnología para el control de una vivienda.

Estándar Que puede utilizarse como modelo o referencia.

Heterogeneidad Que está compuesto por diversos tipos o clases.

Normalizado Que cumple con las reglas o normas establecidas.

Nube Conjunto de servicios e infraestructura que se provee a través de internet.

Omnipresente	Que está presente en todas partes.
Paquete	Conjunto de datos o información que viajan a través de la red como una unidad.
Plataforma	Sistema base que se utiliza para que otros componentes funcionen.
Probabilista	Sistema en el que el azar está involucrado en el funcionamiento del mismo.
Protocolo	Reglas que permiten que dos sistemas se comuniquen para transmitir información.
Radiofrecuencia	Porción menos energética del espacio electromagnético, entre 3 hercios y 300 gigahercios.
Ruido	Señal no deseada que se mezcla con las señales útiles que se transmiten por un canal.
Ubicuo	Que está presente en cualquier momento y puede moverse para el efecto.

RESUMEN

La aparición del internet, a mediados de los años noventa permitió la comunicación eficiente entre computadoras a través de una red, hizo que el mundo como se conocía cambiara completamente. Desde entonces el crecimiento no se detuvo y recientemente apareció una nueva forma de utilizarlo, se conoce como el internet de las cosas.

Conectar cualquier cosa o dispositivo a internet es posible a través de esta tecnología y con ello aparece un nuevo mundo de posibilidades. Los electrodomésticos podrán comunicarse entre sí y comunicar a su propietario sobre la información que sea importante para él. Los dispositivos de domótica junto al internet de las cosas permitirán crear hogares más conectados.

Como esta visión es nueva existen varios problemas asociados que deberán ser resueltos en el mediano plazo, para permitir que la experiencia en el futuro sea mucho más agradable. Temas como la privacidad y la seguridad de la información darán mucho de qué hablar en los próximos años y se espera que existan entes internacionales encargados de la regulación de estos y otros temas.

A través de una encuesta se evaluó la percepción de los guatemaltecos en temas como el internet de las cosas, la privacidad y seguridad de la información, y los dispositivos de domótica. El objetivo principal de esta encuesta es medir el nivel de penetración de este tema en el entorno y conocer cuáles son las preocupaciones que los usuarios poseen en estos temas.

OBJETIVOS

General

Proponer y establecer soluciones a los problemas de privacidad de la información generada por dispositivos de domótica en el internet de las cosas a partir de las soluciones usadas en el internet convencional.

Específicos

1. Explicar la importancia presente y futura del internet de las cosas como una forma de comunicación efectiva entre dispositivos de domótica, sin necesidad de la intervención humana.

2. Identificar los elementos de tecnología que componen el internet de las cosas, sus ventajas, desventajas y aplicaciones para el hogar.

3. Exponer, proponer y analizar soluciones a los problemas conocidos en materia de privacidad y seguridad de la información que se genera, fluye y se maneja a través del internet de las cosas y los dispositivos de domótica.

INTRODUCCIÓN

En la actualidad, la mayoría de personas alrededor del planeta cuenta con una conexión a internet y un dispositivo electrónico o una computadora personal para utilizarla. Durante muchos años el concepto de internet se estableció como una amplia red de computadoras que comparten información y que es utilizada por los seres humanos. Esas computadoras conectadas a internet son generalmente teléfonos inteligentes, tabletas y computadoras personales.

Con el auge de la necesidad de estar conectados, el crecimiento de los dispositivos electrónicos y medios de acceso a internet se han incrementado, dando lugar a nuevas necesidades. El internet de las cosas empezó a sonar hace pocos años y se trata de dar conexión a internet a las cosas, pero no a teléfonos inteligentes o computadoras, sino a cosas que existen actualmente, como una almohada, mesa, camisa o una refrigeradora. Conectar todas estas cosas a internet tiene un objetivo: hacer que las tareas diarias y la vida en general sean más sencillas. Ya no es necesario utilizar dispositivos con altas capacidades de procesamiento de información, las cosas necesitan unos cuantos sensores y una conexión a internet para obtener datos del entorno, enviarlos a una plataforma en la nube y que un servicio responda a la cosa con un mensaje útil para los seres humanos.

Esta tecnología se presenta como algo que permite vivir de una manera más informada, donde se puede manejar la información de todas las cosas que están alrededor y estas pueden comunicarse entre sí para brindar una mejor experiencia. Con esta habilidad se introducen también grandes problemas,

entre de ellos, la privacidad y la seguridad de la información que las cosas transmiten. Ya que estos dispositivos conocerán mucha información de las personas es relativamente fácil que, si no se aplican controles a la privacidad y seguridad de la información sea vendida a terceros o utilizada por las empresas que prestan el servicio en la nube, para el procesamiento de los datos que envían las cosas.

Es necesario tener una solución a los principales problemas de privacidad y seguridad que se presentan como nuevos en el internet de las cosas. En esta investigación se expondrán esos problemas y se plantearán posibles soluciones a los mismos.

1. EL INTERNET DE LAS COSAS

1.1. Antecedentes

Desde los inicios de la humanidad, se ha buscado la forma de comunicarse con los demás, ideando a lo largo de la historia diferentes medios para lograr este objetivo. La comunicación entre seres humanos no cambió mucho durante siglos, sino hasta la invención del telégrafo y el teléfono, permitiendo la comunicación a través de largas distancias y sin la necesidad de esperar semanas o incluso meses.

El hito más importante en la comunicación se alcanzó con la invención del internet, ya que desde sus inicios, hace más de 50 años, hasta la actualidad ha evolucionado como el medio de comunicación más efectivo. Su proceso de madurez tardó en aparecer, a mediados de la década de los años noventa y desde entonces no ha dejado de crecer.

El internet ha cambiado y evolucionado al ritmo que la sociedad y el mundo lo requiere. Los primeros usos del internet pretendían cubrir únicamente necesidades académicas, pero en la actualidad se concibe el internet como un registro enorme de información y conocimiento de todo tipo.

Recientemente con el crecimiento y expansión global de la tecnología y los dispositivos móviles, apareció una nueva forma de ver a internet, ya no como un sitio donde las personas interaccionan sino que, además, las máquinas puedan comunicarse sin intervención humana, que puedan servir

como herramientas para mejorar la calidad de vida de las personas y ayuden a facilitar todas las actividades que no requieren especial atención por los humanos.

1.2. Internet

Sin duda alguna, la mejor herramienta de comunicación actualmente es la que se realiza a través de internet. La velocidad de las transferencias de datos e información y la evolución en la calidad de las conexiones disponibles para todos los usuarios permiten una comunicación instantánea, además, el acceso a un inmenso catálogo de información y servicios, disponibles en cualquier lugar y en cualquier momento.

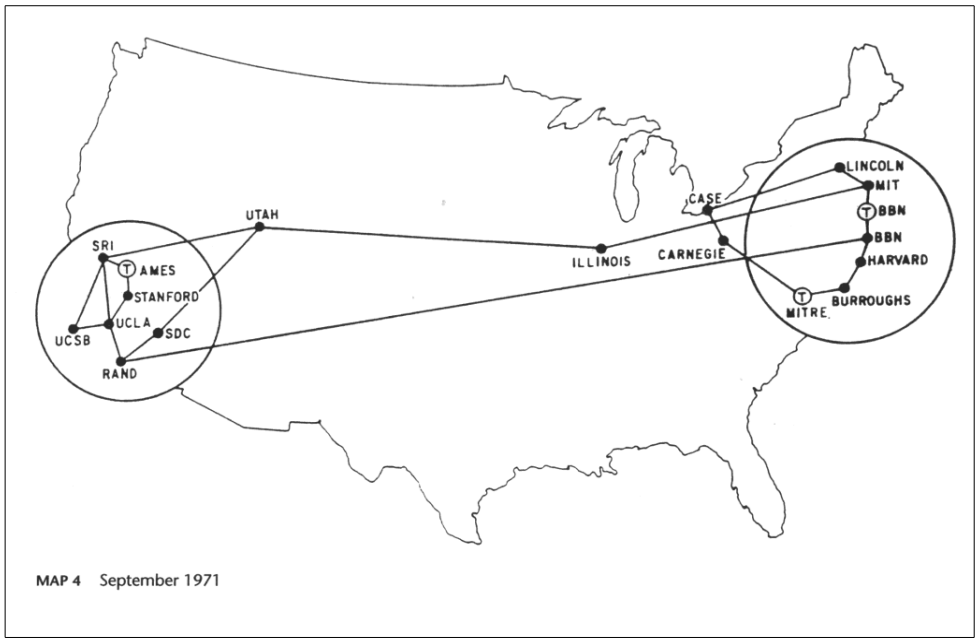
1.2.1. Historia

El inicio de internet como tal se dio en 1961, cuando varios investigadores del Instituto Tecnológico de Massachusetts (MIT, por sus siglas en inglés) en Estados Unidos propusieron la creación de un conjunto de computadoras conectadas, donde cualquier persona pudiera acceder a la información desde cualquier lugar y en cualquier momento.

En los años sesenta no existía infraestructura de comunicaciones que hiciera posible la propuesta de los investigadores del MIT. El Gobierno de Estados Unidos, se dio cuenta de la necesidad de implementar una plataforma de comunicación para mejorar los temas de defensa nacional y decide dar apoyo al proyecto de los investigadores en 1962, a través de la Agencia de Proyectos de Investigación Avanzada en Defensa (DARPA, por sus siglas en inglés).

Para 1965 aparecieron los primeros libros y publicaciones tratando acerca de las características que la red de computadoras tendría, dando paso a los primeros conceptos de manejo de redes que se conocen en la actualidad. Se estableció que la comunicación se realizaría a través de paquetes y que para transmitirlos de un lugar a otro no eran necesarios circuitos electrónicos dedicados. En ese mismo año, Lawrence Roberts y Thomas Merrill crean la primera conexión de red entre computadoras mediante una línea telefónica, conectándose con una computadora en Massachusetts y otra en California.

Figura 1. **Mapa de ARPA en 1971**



Fuente: *Historical Maps of Computer Networks.* http://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html. Consulta: abril de 2015.

Más tarde, en 1967 DARPA presenta el plan para la implementación de la red ARPANET, precursora de lo que hoy se conoce como internet y que conectaría distintas universidades y centros de investigación a lo largo de Estados Unidos. Por sus avances en investigación en envío de paquetes, la Universidad de California en Los Ángeles (UCLA, por sus siglas en inglés) fue elegida como primer nodo de la red, uniéndose más tarde el Instituto de Investigación de Stanford (SRI, por sus siglas en inglés), como segundo nodo, la Universidad de California en Santa Bárbara (UCSB, por sus siglas en inglés) y la Universidad de Utah, para 1969. En la figura 1 se puede observar la distribución de la red ARPA en 1971.

En 1972 se creó la primera aplicación capaz de enviar y recibir correos electrónicos. Esto cambió completamente la manera de comunicación, se utilizó principalmente, entre los investigadores de las universidades asociadas a la red y luego, cuando ARPANET permitió la conexión con las redes externas, se convirtió en una de las mejores formas de comunicación.

Tras la conexión de más redes a ARPANET, esta se convirtió en internet, fiel a la idea original de sus diseñadores. La clave del crecimiento de esta red entre universidades hasta lo que se conoce hoy como internet se dio gracias a la apertura de sus creadores a compartir el funcionamiento de su arquitectura, permitiendo mejoras y nuevas aplicaciones. Muchas fueron las personas que trabajaron para que la infraestructura detrás de internet superara los distintos problemas que se presentaron en su momento.

Con la expansión de internet y la arquitectura abierta que presentaron sus creadores, fue necesaria la creación de estándares para la comunicación, ya que cualquier red se podría conectar a ARPANET. Las bases de esta

comunicación se establecieron con la creación del conjunto Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP, por sus siglas en inglés), que es hasta hoy el conjunto de estándares que definen la manera en que las computadoras se comunican a través de internet. A pesar de que aparecieron otros protocolos y estándares, TCP/IP se mantuvo como líder y fue implementado por la mayoría de sistemas operativos, convirtiéndolo en el protocolo preferido para la conexión en internet.

Con la transición a TCP/IP a mediados de los años ochenta, la conexión de internet se convirtió en global, haciendo que instituciones fuera de Estados Unidos, que habían estado trabajando de manera paralela en redes parecidas a ARPANET, se pudieran conectar. Además, la proliferación en el uso de internet dio paso a la creación de de la World Wide Web a principios de los años noventa, estableciendo un modo de acceso a la información desde cualquier punto del planeta a través de navegadores web.

En octubre de 1995, el Consejo Federal de Redes de Estados Unidos (FNC, por sus siglas en inglés) estableció la definición formal del término internet:

> Internet se refiere al sistema de información global que: (i) está enlazado lógicamente a un espacio global de direcciones únicas basadas en el IP o sus subsecuentes extensiones/añadidos; (ii) puede soportar la comunicación usando el conjunto TCP/IP o sus subsecuentes extensiones/añadidos y otros protocolos compatibles con IP; y (iii) provee, usa o da accesibilidad, ya sea de manera pública o privada a servicios de alto nivel superpuestos en las comunicaciones y las infraestructuras relacionadas ya descritas.[1]

1 Breve historia de internet. http://www.internetsociety.org/es/. Consulta: abril de 2015.

El internet ha evolucionado de manera increíble a lo largo de los años, e instituciones como el World Wide Web Consortium (W3C) se encargan de mantener al día todos los estándares que permiten la comunicación en internet. En la actualidad, internet engloba una gran cantidad de servicios e infraestructura y dejó de ser una herramienta solo de comunicación, ahora es posible realizar cualquier cosa a través de internet y gracias al crecimiento en la capacidad de las computadoras modernas, el mundo se encuentra a un clic de distancia.

1.2.2. Usos comunes

El uso de internet se ha expandido de manera acelerada, de acuerdo a la Unión Internacional de Telecomunicaciones en Ginebra, Suiza se estima que la cantidad de usuarios de internet por cada 100 habitantes en el mundo creció de 2 personas en el 2000 a 39 en el 2013. En los países desarrollados las estadísticas son más sorprendentes, ya que se estima un crecimiento de 11 en el 2000 a 77 personas en el 2013. Estas cifras darían un aproximado de 1 860 millones de personas en el mundo con acceso a internet en la actualidad.

Actualmente es posible realizar cualquier cosa a través de internet, a pesar de que en los inicios, el correo electrónico fue la estrella de los servicios, ahora existen aplicaciones de mensajería instantánea que funcionan sobre internet y que permiten una comunicación aún más rápida, que con el correo electrónico.

Sin duda alguna, el uso más común de internet es la búsqueda de información y ocio, es casi imposible no encontrar en internet a una empresa o a una persona. La educación ha migrado en gran parte a internet, ahora es

posible encontrar una infinidad de cursos gratuitos que se imparten a través de la red.

Incluso el modelo tradicional en que el estudiante asiste a clases en el colegio o la universidad se está cambiado progresivamente a un entorno enfocado a internet, donde el estudiante puede acceder al contenido del curso en cualquier lugar y en cualquier momento, a través de un dispositivo como una computadora o un teléfono inteligente que cuente con conexión a la red. Aunque en este momento ambos sistemas coexisten, es posible que en algunos años se sustituya el modelo presencial por educación virtual y a distancia.

Las aplicaciones de vídeo llamadas, que hace veinte años eran inimaginables, cada día cuentan con mejores experiencias de usuario. Muchas empresas están realizando sus reuniones a través de internet, incluso varios contratos se alcanzan mediante la utilización de esta tecnología. La agilización de las conexiones y la rapidez con la que las personas pueden acceder a internet ha facilitado el uso de este tipo de herramientas, ahora es posible hablar con una persona del otro lado del mundo en tiempo real, incluso con traducción automática.

Los buscadores, como Google o Bing son probablemente la herramienta de más frecuente acceso cuando una persona se conecta a internet, presentan una manera sencilla de encontrar información en la red y, aunque en un principio eran defectuosos, ahora los resultados de las búsquedas se presentan en milisegundos y su exactitud es extraordinaria.

El crecimiento de dispositivos móviles como los teléfonos inteligentes y las tabletas electrónicas, han permitido que personas que se encuentran en lugares remotos puedan tener acceso a estos servicios. Las redes de comunicaciones celulares, principalmente en Guatemala, han crecido de manera sorprendente, llevando las conexiones a internet a casi todo el país.

Las redes sociales que hace quince años no existían, ahora dominan las preferencias entre los usuarios, y es que no solo funcionan como un medio para la distracción y diversión, sino que además permiten la comunicación con los demás usuarios de manera instantánea. Incluso existen redes sociales empresariales y que permiten sacar provecho de la interacción entre los miembros de la empresa para aumentar su productividad. Sistemas de acceso remoto permiten a una persona que se encuentra en otro país acceder a su computadora sin necesidad de cargarla consigo.

Una tendencia importante del uso de internet es el Cloud Computing o computación en la nube, en la cual todos los servicios se encuentran sobre la infraestructura de internet, almacenamiento, análisis y gestión de información son algunos ejemplos, en los cuales ya no es necesario tener un lugar físico donde se contengan y que puedan ser accedidos desde cualquier lugar, en cualquier momento.

Gracias al avance de la tecnología, internet se está convirtiendo en la base de conocimiento de la humanidad y por medio de innovaciones, como el internet de las cosas, la manera en que se vive podría cambiar de manera radical, en beneficio de las grandes mayorías.

1.2.3. Impacto social

La brecha digital comprende todas las diferencias que existen entre los países desarrollados y aquellos que se encuentran en la pobreza o en vías de desarrollo, en materia de acceso a internet y conexiones móviles. La diversificación en los medios de conexión a internet han permitido que esta brecha disminuya considerablemente, aunque aún existen países donde su acceso está limitado o restringido por los gobiernos. Esta desigualdad ha establecido limitaciones para que los usuarios menos afortunados puedan tener acceso a estos servicios.

A pesar de esto, internet ha colaborado en el desarrollo de distintas sociedades. Aprender idiomas o capacitarse en cualquier rama es mucho más sencillo con el acceso a internet. La forma de interaccionar de las personas ha cambiado, gracias a las redes sociales. La información fluye de una manera más rápida, lo que permite que personas al otro lado del mundo se enteren de lo que sucede en cuestión de segundos. Varios son los países que, gracias al internet y las redes sociales, han tenido una voz para advertir al mundo de los problemas que tienen y que sin este medio serían imposibles de compartir.

Las sociedades están cambiando, asimismo, la forma de trabajar y la forma de actuar; todo en favor de las nuevas tecnologías que soportan al internet y que han aparecido para mejorar la calidad de vida de las personas. Definitivamente la creación de internet supuso uno de los avances más notables en la historia de la humanidad.

1.3. El internet de las cosas

Al estilo de las películas de ciencia ficción, el internet de las cosas ha llegado para quedarse. Gracias a esta tecnología es posible que cualquier objeto se conecte a internet y pueda comunicarse con otros dispositivos. Junto con algunos elementos de inteligencia artificial, este campo permitirá un desarrollo aún más acelerado de las comunicaciones, ya no solo humanas, sino también de las cosas.

1.3.1. ¿Qué es el internet de las cosas?

El término apareció por primera vez en 1999, cuando varios científicos e investigadores del MIT en Estados Unidos propusieron la identificación electrónica de cualquier dispositivo. Con esto los investigadores querían establecer la manera de identificar a cada uno de los dispositivos presentes en el mundo a través de un código único que no cambiaría con la ubicación del dispositivo, sino que lo representaría desde su creación hasta que dejara de usarse.

No fue sino hasta 2010, cuando el término tomó importancia y varios libros y artículos científicos fueron publicados tratando el tema. El internet de las cosas o *Internet of Things (IoT)* comprende toda la tecnología existente y que se desarrollará, lo cual permitirá la conexión de las cosas que se utilizan diariamente a la red más grande del mundo.

Desde su concepción, como se mencionó en la sección anterior, el internet fue pensado para la comunicación persona-persona, como con el uso del correo electrónico y mensajería instantánea. Durante el desarrollo de internet surgieron

nuevas formas como persona-máquina o máquina-persona, en la que una persona brinda información a una computadora o dispositivo conectado a internet y este responde de acuerdo a una serie de configuraciones programadas previamente y viceversa.

Con el internet de las cosas se creó un nuevo paradigma de comunicación: máquina-máquina, en el que las máquinas o dispositivos conectados a internet pueden comunicarse entre sí, sin la interacción de los seres humanos. Esto cambia radicalmente el concepto inicial de internet y abre nuevas posibilidades en lo que puede hacerse a través de esta red.

La comunicación máquina-máquina, también se conoce como comunicación cosa-cosa, ya que es parte del término “internet de las cosas”. Es importante conocer que las cosas u objetos que pueden conectarse a internet en este nuevo paradigma de comunicación comprende a aquellos objetos que forman parte de la vida diaria y que pueden tomar información del entorno, trabajar con otros dispositivos, conectarse a internet y producir una salida o respuesta que sea útil para los humanos.

Dentro de las cosas que pueden conectarse al internet de las cosas no se consideran a los dispositivos que interaccionan de la manera convencional con el internet, tal es el caso de computadoras, tabletas electrónicas, teléfonos inteligentes, entre otros. El internet de las cosas establece que cualquier objeto pueda adaptarse para recibir información del entorno y trabajar en conjunto con otros dispositivos, sin la interacción humana. Desde una sombrilla hasta la televisión o el refrigerador, los dispositivos que se conecten a este poseerán un identificador que lo hará único, con el cual transmitirán la información que capturan y podrán actuar de acuerdo a la misma.

Todos los servicios basados en el internet de las cosas proporcionarán mayor automatización a las tareas que involucren objetos y personas, con el objetivo de construir un mundo más inteligente, no solo en la industria sino también en el hogar y en el trabajo. Muchas empresas de desarrollo de dispositivos electrónicos han iniciado a apostar por esta tendencia, poniendo en el mercado productos con diferentes capacidades, pero que a resumidas cuentas puedan interaccionar con su entorno.

La implementación del internet de las cosas es una tarea bastante complicada, ya que la heterogeneidad de los dispositivos hace necesaria la estandarización de las comunicaciones y conexiones a internet. El conjunto TCP/IP, que tan bien sirvió para la expansión del internet convencional, podría ser la respuesta, y los esfuerzos iniciales en la construcción del internet de las cosas están apuntando a emplear esta tecnología en conjunto con otros estándares de la industria. El Protocolo de Internet versión 6 (IPv6, por sus siglas en inglés), que a diferencia de la versión 4 puede identificar hasta 223 dispositivos en un metro cuadrado, se ha tomado como el punto de partida para conectar e identificar las cosas y objetos conectados al internet de las cosas.

La idea principal detrás del internet de las cosas es dar paso a la computación ubicua, es decir, que la computación esté presente en cualquier lugar y momento, de manera omnipresente, recopilando información de los seres humanos y su entorno, procesarla y brindar información y contenido de interés que permita mejorar la manera en que los seres humanos desempeñan sus tareas.

1.3.2. La tecnología que lo soporta

Debido a que la concepción inicial de internet era la comunicación persona-persona y no máquina-máquina, los científicos e investigadores han propuesto una serie de elementos a tomar en cuenta para la implementación del internet de las cosas:

- La tecnología de conexión de los objetos.
- La interoperabilidad entre los objetos.
- El modelo de comunicación entre objetos conectados.
- La posible interacción con modelos existentes.
- La selección de un modelo de transporte.
- El direccionamiento, identificación y nombramiento de objetos.
- La seguridad y privacidad.
- El impacto económico y la evolución de la cadena de valor de las telecomunicaciones.

Es muy probable que con el desarrollo del internet de las cosas surjan nuevas tecnologías que permitan cubrir de manera específica cada uno de los elementos listados arriba. Por el momento estas actividades se cubren con la tecnología existente y varios de los científicos esperan que el internet como tal evolucione nuevamente, para dar paso a las nuevas conexiones máquina-máquina.

Los principales componentes de un objeto o cosa que se conecta al internet de las cosas son:

- Sensores: permiten recibir la información del entorno que rodea al dispositivo.
- Actuadores: son componentes u otros dispositivos que permiten ejecutar una respuesta ante el procesamiento remoto de la información capturada por los sensores.
- Identificador único: permite asignar una forma de identificación al dispositivo dentro del internet, para que la información que envía y recibe sea procesada como es debido.
- Conexión: establece la comunicación con otros dispositivos a través del internet y permite enviar y recibir la información.

Debido a que los objetos conectados al internet de las cosas son instrumentos de uso cotidiano, las posibilidades en materia de poder de procesamiento, memoria y conexión son limitadas. Como en la actualidad está siendo implementado sobre la tecnología existente, es necesario que estos objetos y cosas sean adaptados para trabajar con la misma y es tarea de las empresas dedicadas al desarrollo de estos dispositivos, la creación de tecnologías más eficientes.

Desde la aparición del término en 1999, la Identificación por radiofrecuencias (RFID, por sus siglas en inglés) ha sido la manera más eficiente para identificar cosas y objetos. Este estándar junto con el conjunto TCP/IP permiten la identificación y conexión de los dispositivos.

Con respecto a los sensores y actuadores, estos sí existen en gran variedad y permiten realizar un sinnúmero de mediciones y acciones con los dispositivos que los contienen. Una división importante dentro del internet de las cosas abarca además, los dispositivos nanotecnológicos, que podrían valerse

de los grandes avances en física, química y biología para controlar de mejor manera el entorno no solo de objetos inanimados como un vehículo o un tostador, sino también de objetos animados como las personas mismas o los animales.

Como en el internet de las cosas se habla de miles de millones de dispositivos conectados, recibiendo información y actuando. Es necesario también una plataforma de procesamiento de esa información. Ya que las capacidades dentro de los objetos es limitada, el procesamiento se relega a una plataforma amplia conectada a internet y que proporciona un servicio a los objetos también conectados a la red. El internet de las cosas potencia la estructura de computación en la nube, ya que todos los servicios de procesamiento de la información se encuentran usando esa infraestructura.

Procesar tanta información requiere que los sistemas sean bastante potentes y el uso de herramientas como *Big Data* proveen una solución a este problema. *Big Data* establece que el procesamiento de cantidades inmensas de información compleja es inadecuado a través de las técnicas tradicionales de procesamiento de datos. El concepto de *Big Data* se basa en cuatro principios sobre el tratamiento de los datos: volumen, variedad, velocidad y veracidad, conocidas comúnmente como las 4 *v's* de *Big Data*.

El volumen se refiere a las cantidades gigantes de información, como las generadas por lo miles de millones de objetos que se conectarán al internet de las cosas; la variedad se refiere a la heterogeneidad de los dispositivos y la información que fluirá a través del internet de las cosas; la velocidad se refiere a que el procesamiento y análisis de la información deberá ser inmediata y en tiempo real; la veracidad se refiere a que es necesario constatar que la

información es real y que puede aportar un valor agregado a los seres humanos.

Big Data no se refiere solo a temas del internet de las cosas, pero sin duda es una de las mejores herramientas que se adaptan a las necesidades que presenta el internet de las cosas.

1.3.3. ¿Quién lo construye?

A pesar de que la tecnología que yace debajo del internet es compleja y es mantenida por grandes organizaciones de investigación y desarrollo a nivel mundial, casi cualquier persona puede involucrarse en la construcción del internet de las cosas. Así como las personas de manera independiente crearon páginas web y blogs a mediados de los noventa y que supusieron la explosión de internet, los actores del internet de las cosas serán aquellos que desde ya se interesen por esta disciplina.

En el proceso de construcción del internet de las cosas serán necesarios algunos puestos claves, personas que funjan como un eslabón entre todas las disciplinas necesarias para la creación de las “cosas” que se conectarán a este. La idea que propone esta tecnología es, como se mencionó con anterioridad, la conexión de cualquier objeto al internet y son las mismas personas que construyen esos objetos, que hasta ahora no poseen conexión, quienes deberán involucrarse en la expansión de esta tecnología.

Un proyecto de cosas que se conectan al internet seguramente contará con artistas, diseñadores, ingenieros y obreros. Es como tomar todo lo que se tiene en la actualidad y agregarle un conjunto de elementos que permitan la

captura de información, conexión a internet e interacción con otros elementos del entorno. El enfoque se dirige a crear el “internet de las cosas hermosas”[2] y no solo conectar cualquier elemento a internet.

La principal característica que los constructores del internet de las cosas deben tener es la imaginación. Muchas empresas grandes de electrodomésticos están agregando estaciones a las líneas de producción, estaciones en las que se añaden los componentes necesarios para que sus máquinas se conecten a internet y permitan una mejor experiencia para el usuario. La cuestión es que no solo agregan los componentes porque sí, los agregan de manera tal que resuelvan problemas que los usuarios tienen y creen una cultura del uso de los mismos. Inevitablemente, en los próximos años el internet de las cosas pasará a ser tan común como el convencional y ver todos los objetos de la casa u oficina comunicándose entre sí para brindar la mejor asistencia, será una realidad.

1.3.4. Beneficios

El diseño del internet de la cosas supone una idea en la que se pueda ahorrar tiempo y dinero, probablemente los recursos más preciados por los seres humanos. El crecimiento del internet de las cosas y la automatización en la comunicación de todos estos objetos permitiría ahorrar recursos, tanto de manera individual, empresarial o social.

Uno de los beneficios principales que presenta es la cantidad de información que se genera hoy y en los próximos años. La información puede transformarse en conocimiento y saber manejar el conocimiento se transforma

2 MCEWEN, Adrian. *Designing the Internet of Things*. p. 18.

en poder. Las capacidades ilimitadas que proporciona proveerá a los seres humanos con toneladas de información, que al ser analizadas e interpretadas permitirán mejorar increíblemente el mundo y la manera en que se vive.

Conectar todos los objetos a la red permitiría, por ejemplo, para una empresa que posee una línea de producción, monitorear todos sus procesos, ahorrar recursos y evitar el desperdicio. Una persona podrá recibir información acerca de los productos que tiene en la despensa de su casa, cuáles faltan o cuáles están por terminarse, para crear una lista de supermercado que ahorraría hacer viajes repetidos a la tienda o al supermercado para abastecerse.

Otro de los grandes beneficios se puede ver en el área de salud. Los hospitales podrán implantar *chips* debajo de la piel de las personas y a través de los distintos sensores biológicos que estos contengan llevar control del historial clínico de las personas, sus signos vitales, hábitos, etcétera, que pueden mejorar notablemente la salud de las personas. Probablemente estos dispositivos informarán a las personas sobre los medicamentos que deben tomar, las dosis e incluso monitorear la reacción a los mismos.

El camino que está marcando apunta a un mundo donde todas las personas tengan acceso a dispositivos que mejoren su vida y ayuden en tareas sencillas. A largo plazo el internet de las cosas puede ayudar a reducir la brecha existente entre las clases sociales y a ser más humanos.

1.3.5. Problemas

Como cualquier cosa, y especialmente en el mundo de la tecnología, el internet de las cosas presenta ciertos problemas a los cuales es necesario prestar bastante atención. Si bien esta tecnología permite facilitar todas las tareas valiéndose de la información recuperada del entorno y de las mismas personas por los objetos, al tratarse de una creación humana está sujeta a errores.

El problema más grande y que se abarca en el resto de este documento, es la privacidad de la información. Ya que los objetos conectados al internet de las cosas manejarán grandes cantidades de información de las personas, algunos datos podrían parecer de interés para las personas con malas intenciones. El robo de un historial médico, información bancaria, métodos de seguridad del hogar o de los vehículos, podría permitir que las personas con conocimientos avanzados puedan penetrar en su intimidad o exponer cosas que no quieren mostrar.

A pesar que las distintas organizaciones que soportan el internet convencional se ha preocupado de este tipo de asuntos, al ser el internet de las cosas una tecnología disruptiva que cambia completa o parcialmente las maneras en que los dispositivos se conectan a internet, es necesario tomar medidas en el asunto, este es un tema que se trata a mayor detalle en los capítulos posteriores.

Dejar la puerta abierta en temas de privacidad supone también problemas de seguridad. Por ejemplo, si las empresas dedicadas al manejo de la información generada por los objetos conectados realizan actos de

comercialización de la información con otras empresas y organizaciones, sin el consentimiento de las personas, podría suponer el debilitamiento de la sociedad como tal, haciendo a los individuos más frágiles y expuestos.

Problemas más relacionados con el ámbito técnico y que serán superados en los próximos años, incluyen las tecnologías de conexión para los nuevos dispositivos. Aunque en la actualidad los medios de comunicación para estos dispositivos se encuentran en prototipos o en desarrollo, se espera que en los próximos años las grandes empresas de electrónica y centros de investigación internacional creen soluciones a las limitaciones, que la infraestructura actual supone para el crecimiento del internet de las cosas.

1.3.6. Aplicaciones de domótica

La domótica, del latín *domus* (casa) y del griego *tica* (que funciona por sí solo), comprende el conjunto de todos los sistemas que permiten automatizar las viviendas y hogares. A través de estos sistemas es posible controlar cualquier aspecto de la vivienda desde el consumo energético hasta el confort de las habitaciones. Este concepto se remonta a los orígenes de la electricidad misma cuando los primeros controles remotos aparecieron.

En su historia reciente, la domótica ha aparecido como un factor común en todas las historias de ciencia ficción. Su implementación no se ha expandido como se esperaba y por mucho tiempo se han realizado aplicaciones diferentes y que no son compatibles entre sí. Hasta hace pocos años, con el auge del internet de las cosas, la domótica ha tomado la relevancia esperada. Es el conjunto de estas tecnologías lo que muchas personas han esperado durante mucho tiempo.

Los beneficios del internet de las cosas en conjunto con los dispositivos de domótica permitirán la creación no solo de hogares automatizados, sino inteligentes. Además, con el creciente mercado de dispositivos móviles, el control del hogar y la interacción con el será mucho más sencillo. Tener un panel de control de todas las funciones del hogar y realizar mediciones en tiempo real del consumo energético, la calidad del aire, el estado de la estructura, alimentos necesarios e incluso la limpieza del suelo, podrán accederse de manera inmediata.

La domótica es probablemente, una de las ramas en las que el internet de las cosas puede aplicarse en mayor medida. Este trabajo de investigación se centra en la información generada por los dispositivos de domótica que se conectan o se conectarán en un futuro cercano al internet de las cosas. Algunos de estos dispositivos incluyen:

- Controles de energía.
- Climatización.
- Control de puertas y ventanas.
- Iluminación.
- Sistemas de entretenimiento (televisiones, equipos de sonido, reproductores multimedia y centros de entretenimiento).
- Electrodomésticos (refrigeradores, estufas, hornos, tostadores, cafeteras, procesadores de alimentos, lavadoras y secadoras).
- Controles de seguridad y acceso.
- Controles de limpieza.

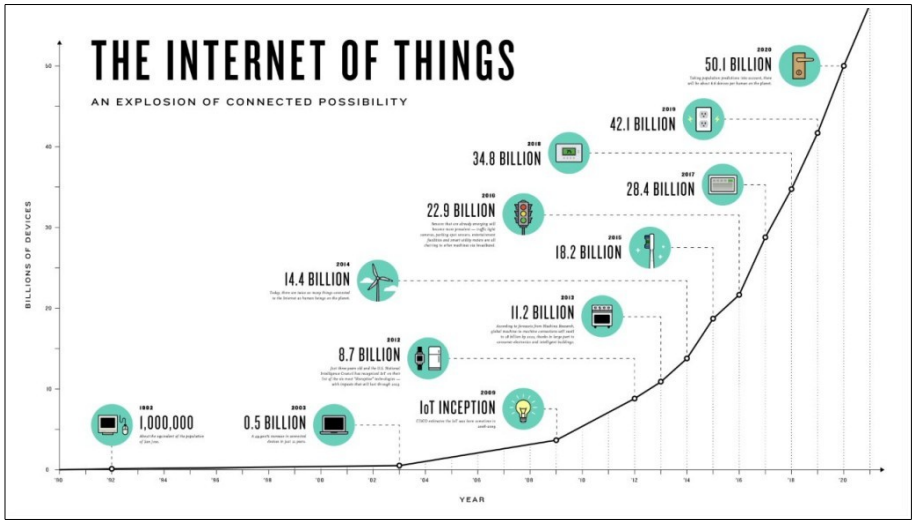
Toda la información que estos dispositivos pueden recolectar, compartir y analizar harán que la experiencia y administración del hogar sean más

sencillas. Recientemente con el auge en la conexión de dispositivos del hogar a internet, surgió la comunicación mediante cableado eléctrico (PLC, por sus siglas en inglés) que es capaz de transmitir señales de radio a través de la infraestructura actual de líneas de energía eléctrica. Con este tipo de comunicación, la conexión de los dispositivos de domótica, como televisores y refrigeradoras no necesitarán un módulo especial de conexión a internet.

1.3.7. El futuro del internet de las cosas

Tiene un futuro prometedor. El crecimiento de la tecnología y la adaptación de la existente permitirá que todos los objetos que están al rededor puedan comunicarse de manera eficiente, haciendo que todo sea más fácil.

Figura 2. **Crecimiento posible del internet de las cosas**



Fuente: SINGH, Tarry. http://tarrysingh.com/2014/07/fog-computing-happens-when-big-data-analytics-marries-internet-of-things/. Consulta: abril de 2015.

En la figura 2 se puede observar el crecimiento esperado en la conexión de dispositivos al internet de las cosas para el año 2020, mostrando un comportamiento exponencial, pasando de 18,2 miles de millones de dispositivos conectados en el 2015 a 50,1 miles de millones en el 2020.

Muchas empresas nuevas surgirán para aprovechar las capacidades ilimitadas del internet de las cosas, pero también las ya bien conocidas como Apple, Google, IBM, Intel y Microsoft apuestan por esta tecnología y están demostrando por qué son las compañías con más influencia en este tema. Grandes cantidades de dinero se están invirtiendo en el crecimiento del internet de las cosas y es probable que el crecimiento en la cantidad de dispositivos ya descrito no solo se cumpla, sino que se sobrepase.

2. PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN EN INTERNET

2.1. Datos, información y conocimiento

A lo largo de la historia de la humanidad ha resaltado la importancia del conocimiento, gracias a este se tomaron las decisiones más importantes en el pasado. Conseguir el conocimiento requiere un proceso, que inicia con los datos como unidades básicas, transformados en información y esta a su vez evolucionada en conocimiento. El conocimiento puede también evolucionar en sabiduría, que puede utilizarse de la mano del entendimiento para tomar decisiones en el presente, con base en eventos del pasado, para mejorar el futuro.

2.1.1. ¿Qué son los datos?

Se consideran como la materia prima del conocimiento que, de manera independiente, carece de significado. Los datos representan hechos del mundo y que no pueden ser modificados de manera arbitraria, describen cualquier elemento que puede ser percibido tanto por los seres humanos como por las máquinas. Los datos generalmente son medibles y permiten identificar algún elemento real del entorno.

La temperatura del ambiente y la cantidad de luz en una habitación son ejemplos de datos, ya que son medibles y de manera individual y sin un contexto que los contenga no poseen un significado concreto. Los seres

humanos por medio de los sentidos perciben los datos del entorno. Para que las máquinas sean capaces de obtener estos datos, las personas crean sensores, dispositivos que emulan la funcionalidad de los sentidos para percibir el entorno.

2.1.2. ¿Qué es la información?

Consiste en la primera evolución de los datos. Cuando estos son considerados en conjunto y se agrega además un contexto, una categoría, un propósito y relevancia se convierten en información. Entonces, la información es el conjunto de datos que tienen un significado, que de manera individual no podrían contener.

La utilidad y valor que se agrega a los datos permite que estos se conviertan en información. Una característica importante de la información es que esta elimina o reduce la incertidumbre presentada por los datos. Actualmente, el medio más común para almacenar información son las bases de datos, aunque su nombre correcto quizás sea bases de información, ya que la definición anterior sugiere que los datos con significado se convierten en información.

Continuando con el ejemplo de la sección anterior, si los datos recopilados sobre la cantidad de luz en la habitación y la temperatura del entorno son contextualizados en un día de verano, estos datos se transforman en información sobre las condiciones de luz y temperatura en un día de verano.

2.1.3. ¿Qué es el conocimiento?

Es la evolución de la información, es decir, la segunda evolución de los datos. Así como la información es un conjunto de datos con sentido, el conocimiento corresponde a un conjunto de información que posee un sentido de utilidad. El conocimiento está asociado, generalmente, a la acumulación de información relacionada y que mediante un proceso determinista es útil para el conocedor.

Además de la información, otro componente importante del conocimiento es la experiencia. La información de distintos eventos pasados construye el conocimiento para ser utilizable en el presente. Entonces, para utilizar el conocimiento es necesario comparar los distintos tipos de información y buscar conexiones dentro y fuera de la información. Como resultado, el uso del conocimiento permite incorporar nuevas experiencias, nueva información y tomar acciones en distintas circunstancias.

El conocimiento está asociado con la inteligencia, actualmente se habla de internet como la base de conocimiento de los seres humanos, ya que en él se encuentra mucha información pasada y presente que puede convertirse en conocimiento para la toma de decisiones, no solo personales sino también empresariales.

Continuando con el ejemplo de las dos secciones anteriores, si se realiza una comparación de la información de los últimos cinco años, tomando un día de verano de cada uno, en los que se obtuvieron los datos sobre la cantidad de luz en la habitación y la temperatura del entorno, se descubrirán conexiones o relaciones en los distintos conjuntos de información, probablemente la relación

indicará una cantidad de luz abundante y una temperatura elevada, si se contextualiza en un país como Guatemala, donde los días de verano son llenos de luz y muy calurosos, esto es algo conocido, por lo tanto, producto del conocimiento.

2.1.4. Más allá del conocimiento

La siguiente evolución de los datos es la sabiduría. Cuando el conocimiento puede emplearse para tomar acciones en situaciones donde se desconoce parcial o totalmente de las condiciones del entorno, se conoce como sabiduría. Esta característica es propia de los seres humanos y hasta el momento, las máquinas (aún las que cuentan con inteligencia artificial) no pueden representarla de ninguna manera. La sabiduría necesita discernir y juzgar las situaciones para poder aplicar el conocimiento, está fuertemente ligada al concepto de entendimiento.

La sabiduría no es determinista ni probabilista, por esas razones se considera como una característica meramente humana, y para alcanzarla es necesario comprender completamente los datos, la información y el conocimiento, tal como se muestra en la figura 3.

Figura 3. **Jerarquía del conocimiento**

Fuente: elaboración propia, basada en *DIKW Pyramid.* http://en.wikipedia.org/wiki/DIKW_Pyramid. Consulta: abril de 2015.

2.2. Privacidad

Consiste en la capacidad de los seres humanos de aislar ciertos aspectos de su vida personal a las demás personas, de manera tal que estos permanezcan ocultos o visibles solo a personas de confianza. Está ligada a la confidencialidad e intimidad de cualquier elemento perteneciente a la vida de los individuos.

Aunque en la Constitución Política de la República de Guatemala no existe un artículo dedicado al tema de la privacidad, sí habla sobre el respeto a la intimidad de cada uno de los guatemaltecos. En la Declaración Universal de los Derechos Humanos presentada por la Asamblea General de las Naciones

Unidas en 1948 se expresa el derecho a la vida privada de la siguiente manera: “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”[3].

La pregunta más discutida en materia de privacidad es ¿qué es privado? y la respuesta a esta está relacionada directamente con la cultura de las personas, pero, generalmente se refiere a aquellas cosas que son importantes y sensibles para una persona. Algunos de los elementos universalmente aceptados como privados son: el cuerpo, el hogar, la propiedad, los pensamientos, los sentimientos, los secretos y la identidad de cada persona.

La mayoría de constituciones y leyes de los países protegen la privacidad de los seres humanos, pero existen ciertas actividades que asaltan a la privacidad de las personas, William Prosser estableció en 1960 las siguientes:

- Intrusión al espacio privado de las personas, sus negocios o su deseo de estar solo.
- Divulgación de información personal que, al momento de revelarse, podría ser vergonzosa.
- Promover el acceso a la información sobre una persona que podría ocasionar que otras personas tengan pensamientos erróneos sobre ella.
- Usurpación de los derechos de personalidad de un individuo y el uso de su imagen para promover intereses ajenos a los suyos.

3 UNESCO. Oficina Regional de Educación de la UNESCO para América Latina y el Caribe. *Declaración Universal de Derechos Humanos.* p. 14.

2.3. Privacidad de la información

Debido a que la información puede representar un valor para las personas y organizaciones, la privacidad de la misma es muy importante. La privacidad de la información consiste en la capacidad de las personas y organizaciones para determinar qué información sobre ellos será comunicada con las demás personas u organizaciones. Al igual que con el concepto general de privacidad, la información depende de la estructura social, los elementos culturales y las leyes vigentes que protegen a los individuos y organizaciones.

La privacidad de la información está relacionada con el control del procesamiento, adquisición, divulgación y uso de la información de una persona. A diferencia de la privacidad de espacio o de pensamiento, donde las violaciones son fácilmente identificables, una violación en la privacidad de información es difícil de demostrar. Muchos países como Estados Unidos y los miembros de la Unión Europea cuentan con legislaciones fuertes que condenan los abusos contra la privacidad de la información.

De acuerdo a la Escala Global sobre la Preocupación de la Privacidad de la Información (GIPC, por sus siglas en inglés) existen cuatro dimensiones que son percibidas en general sobre la privacidad de la información: la recopilación, el uso no autorizado por terceros, el acceso inapropiado y los errores. Aunque esta escala no es definitiva y puede cambiar con el tiempo, es bastante efectiva cuando se tratan casos sobre privacidad de la información.

Una ejecución correcta de la privacidad de la información evita la vergüenza de los individuos, permite construir la intimidad y evita el uso indebido de la información. Por otro lado, algunos de los aspectos negativos de

la privacidad de la información son: el comercio no es preciso porque los compradores pueden ocultar parte de su información y la confianza entre las personas se debilita por la posibilidad de no revelar pensamientos o ideas.

2.3.1. Privacidad en internet

Debido a que en internet la información fluye sin restricciones, existen altas probabilidades de que la privacidad de las personas sea violada. Generalmente cuando se realiza el registro de una cuenta nueva en cualquier sitio de internet, se proporcionan datos personales y se aceptan los términos y condiciones del servicio. En la mayoría de ocasiones, estos términos y condiciones son demasiado largos para que las personas se tomen el tiempo de leerlas y aceptan a ciegas la comercialización de su información privada.

Steve Rambam, investigador especializado en privacidad de la información en internet, indica que la privacidad en la red más grande del mundo no existe y que es necesario vivir con ello. Los sitios de internet requieren el uso de la información de sus usuarios para mejorar la experiencia de navegación, aunque en la mayoría de ocasiones tomen información sensible, que puede dar lugar a cierto tipo de vigilancia de las actividades que los usuarios hacen en internet.

La experiencia en internet depende, principalmente del nivel de acceso que el usuario brinde a los sitos que visita, existen herramientas de software que permiten alcanzar un anonimato casi completo al navegar en internet, pero hace que la experiencia sea poco personalizada y carezca de funciones agregadas. Es común en la actualidad que las personas compartan cualquier tipo de información privada en las redes sociales que, a pesar de ser buenas

herramientas para el trabajo colectivo, pueden llevar esa información a personas con las que no se desea compartirla.

Al compartir la información privada en internet se corren varios riesgos, por ejemplo, si se comparte información sobre el historial médico y clínico con un sitio que a primera vista parece muy seguro y que respeta la privacidad, puede incluir en sus términos y condiciones el compartir la información con terceros o en la mayoría de casos, no especificar el manejo que se dará de la información que el usuario comparte. Obviamente esta última dejará la puerta abierta para que, incluso pueda comercializarse esta información y que el usuario pueda ser hostigado por terceros que poseen su información médica. La sensibilidad de esta información también puede desencadenar problemas más graves, como atentados personales o actos violentos.

En gran medida el riesgo que se corre en internet depende de qué información se comparta con terceros y cuáles son las intenciones de estos. Facebook, la red social con más usuarios en el mundo, que además es propietaria de Instagram, la red social de fotografías con más usuarios, y WhatsApp, el servicio de mensajería instantánea más grande, recopila información de sus usuarios a través de los tres servicios. Cuando se utilizan sus servicios en un navegador web, la compañía emplea *cookies* o archivos que permiten realizar un seguimiento de las acciones del usuario, no solo en su sitio, sino cualquier en actividad que realice dentro del navegador web.

Lo mismo ocurre con las aplicaciones para teléfonos inteligentes, estas valiéndose de los servicios de localización como el Sistema de Posicionamiento Global (GPS, por sus siglas en inglés), recopilan información de la ubicación del usuario y realizan un seguimiento de los movimientos que realiza, las personas

que se encuentran en sus alrededores y las búsquedas que se realizan en internet.

En un intento de resguardar la privacidad, varias compañías han creado herramientas de software para invalidar las *cookies* dentro de los navegadores, pero las grandes compañías han creado nuevas soluciones que no pueden ser bloqueadas con tanta facilidad, como las *flash cookies* que emplean la tecnología *flash* para animaciones digitales y que no pueden ser detectadas por las herramientas mencionadas; también se encuentra el *device fingerprinting,* que originalmente se creó para evitar los fraudes en internet, pero se ha convertido en un medio para que los sitios de internet puedan conocer exactamente quién los visita, pareciendo transparentes a los usuarios y sin informarles que se realiza un seguimiento de sus actividades.

Los motores de búsqueda, como Google o Bing, almacenan información privada de los usuarios para mejorar la calidad de los resultados de búsqueda. En la mayoría de situaciones, estos sitios almacenan la dirección del Protocolo de Internet (IP, por sus siglas en inglés), la ubicación geográfica y la información del dispositivo desde el cual se accede al buscador. Aunque las empresas que administran estos sitios indican que la información no es comercializada, varios casos sobre violación de privacidad se han registrado en Estados Unidos y la Unión Europea, que como resultado han permitido a las personas retirar completamente su rastro de internet o hacer que las compañías modifiquen sus términos y condiciones de uso.

Otro aspecto importante de la privacidad en internet es el medio de conexión. Todos los usuarios se conectan a internet a través de un proveedor de servicios de internet (ISP, por sus siglas en inglés), el cual recibe y envía

todos los datos e información que los usuarios intercambian en la red. Aunque la mayoría de ISP solo funcionan como puente entre el usuario y los sitios de internet, es necesario conocer las condiciones en el contrato del servicio, ya que, generalmente este es el único sustento legal con el que los usuarios pueden tomar acciones judiciales en caso de la violación de su privacidad.

Existen muchos más riesgos de la privacidad en internet, que no es necesario conocer a profundidad, pero es necesario destacar la importancia de conocer lo que se comparte en internet. En la mayoría de situaciones es el usuario el que permite el acceso, uso y comercialización de su información privada. Actualmente casi todas las compañías que emplean la información de los usuarios lo expresan claramente en los términos y condiciones de uso y servicio.

2.4. Seguridad

Consiste en todos los métodos y mecanismos que permiten agregar resistencia o protección contra los peligros. Generalmente se aplica sobre cualquier bien vulnerable y que representa valor para una persona, sociedad u organización. La seguridad intenta crear una barrera entre los bienes y las amenazas y su efectividad depende de la utilización correcta de los métodos y mecanismos, determinados por la circunstancia.

Cuando se habla sobre seguridad existen dos conceptos clave: la percibida y la real. La seguridad está asociada en la mayoría de circunstancias al miedo, ya que las personas tienen la necesidad de seguridad. En algunas ocasiones, la seguridad real es menor que la percibida, ya que los mecanismos de seguridad implementados no son tan elaborados y existen únicamente con el

fin de proveer la sensación de seguridad al usuario final. Para medirla, sin lugar a dudas, la herramienta de evaluación más efectiva es la percepción de los usuarios.

Fuertemente asociadas al tema de seguridad se encuentran las garantías, estas permiten crear un punto de acuerdo entre los proveedores de la seguridad y los usuarios finales, los últimos tienen la certeza que a través de estas, sus propiedades, ideas y demás se encuentran protegidos o al menos pueden recuperarse parcialmente.

Muchos expertos recomiendan no fiarse únicamente de un método o proveedor de seguridad, siempre es bueno contar con un respaldo para situaciones de emergencia, ya que si por alguna circunstancia alguno de los métodos o proveedores falla, puede tenerse la certeza que la seguridad no se verá comprometida.

Cuando se habla de seguridad aparecen los conceptos de riesgo, amenaza y vulnerabilidad. Un riesgo es cualquier situación o acontecimiento que puede originar una pérdida de valor para una persona u organización. Una amenaza es cualquier método o actividad que permite desencadenar un riesgo, puede ser controlable o no, de acuerdo a las circunstancias. Por ejemplo, una amenaza controlable es el acceso que se da a personal ajeno a una organización, mientras que una amenaza no controlable podría ser un fenómeno natural o catástrofe. Por último se encuentran las vulnerabilidades, estas son debilidades que se pueden identificar y que posiblemente serán atacadas por personas o sistemas ajenos para crear una amenaza.

2.5. Seguridad de la información

Consiste en todos los métodos, prácticas y mecanismos que permiten defender la información de accesos no autorizados. En estas circunstancias la privacidad y seguridad de la información se relacionan. La implementación de seguridad en la información es una manera de garantizar la privacidad de la misma, ya que esta se encarga de proteger la información de acceso, uso, revelación, modificación e inspección no autorizada y que puede perjudicar tanto a la información misma como a las personas u organizaciones dueños de esta.

Debido a que en la actualidad, la mayoría de la información se encuentra en estado digital y transita en los sistemas de información, la seguridad que se aplica a la misma está relacionada con la seguridad que se aplique sobre los sistemas y tecnologías de la información. Existen carreras profesionales que tienen como objetivo entrenar personas expertas en esta materia y no se limitan a computadoras personales, sino a cualquier conjunto de sistemas que manipulen cantidades considerables de información.

Para cualquier persona u organización, la información es un valor importante, por lo tanto es necesario asegurarla. Proteger los datos es proteger la información. El aseguramiento de la información requiere no solo un plan contra los desastres o atentados, sino un plan para la recuperación y reestructuración de la misma. Probablemente la amenaza más latente son los desastres naturales, pero pueden existir también funcionamientos incorrectos del equipo que contiene la información, robo de estos equipos o accesos no autorizados, tanto de manera física como lógica. La solución más frecuente en temas de seguridad de la información es la redundancia de los sistemas.

La redundancia en sistemas de información consiste en todos los métodos y mecanismos que permiten mantener una o varias copias totales o parciales de los datos e información, ya sea en la misma ubicación o en lugares remotos, con el objetivo de no depender de una única copia y eliminar tanto los riesgos físicos (hardware) como los lógicos (software). Cualquier intromisión en la información de una empresa o persona puede significar la exposición de elemento sensibles y que generen problemas o pérdidas monetarias para los propietarios de la información.

2.5.1. Seguridad en internet

El auge de internet en los últimos años ha presentado nuevos problemas a los expertos en tecnología. Uno de ellos, y quizás el más importante, es la seguridad. El internet es uno de los lugares más peligrosos y con mayor riesgo, en materia de datos e información digital; es común escuchar que grandes empresas han perdido enormes volúmenes de información confidencial por agujeros de seguridad en sus sistemas de información.

Ya que la mayoría de accesos a internet se realizan a través del navegador web, esta aplicación representa una de las mejores opciones para conseguir información. La seguridad de los usuarios se ve comprometida si existen fallas en el funcionamiento y control de la seguridad de estas aplicaciones y personas mal intencionadas pueden aprovechar estos problemas para hacerse con la información y los datos de los usuarios.

Además, la seguridad en la red física por la que se transmite la información también es importante. Si una red no cuenta con los mecanismos adecuados de seguridad, cualquier individuo puede infiltrarse y causar daños

tanto a la infraestructura como a la información que transita por ella, darle mal uso e incluso realizar atentados a los dueños de la información. Como se mencionó en apartados anteriores, la privacidad y la seguridad van de la mano.

Para garantizar la privacidad de la información y los datos de las personas, la seguridad es uno de los factores más importantes. Es imposible proporcionar privacidad sin dar seguridad, de hecho uno de los objetivos de proveer seguridad es brindar privacidad a los usuarios, especialmente en un ambiente tan peligroso como internet.

Todos los sistemas operativos poseen vulnerabilidades de seguridad que son explotadas por medio de programas instalados en la computadora del usuario, haciendo que esta forme parte de una red enorme de ordenadores controlados de manera remota para fines oscuros, como el envío de correo electrónico no deseado o ataques de denegación de servicio contra grandes infraestructuras de red. Sin embargo, algunos de estos programas solamente se instalan en la computadora del usuario final para molestarlo y generalmente no dañan su información o comprometen su seguridad. Estos programas, aunque no todos son dañinos, se conocen como software malicioso o *malware*.

Algunas formas de *malware* son: los virus, que generalmente se apoderan de los datos e información de los usuarios contenida en sus dispositivos electrónicos y se replican de manera que puedan infectar a todos los sistemas de archivos del dispositivo; los gusanos, que se copian a sí mismos a través de la red y en los sistemas de archivos para realizar tareas programadas, generalmente con fines maliciosos; caballos de troya o troyanos, que no se replican a sí mismos, pero aparecen disfrazados dentro de otro software para ejecutar tareas maliciosas, sin que el usuario se de cuenta y aparentando ser

otro programa; *spyware* o software espía, que realiza monitoreo de las acciones que los usuarios realizan en la computadora y son reportadas a través de internet para conocer las preferencias de un usuario basado en sus acciones.

En un mundo tan conectado es imposible alejarse de internet y, por lo tanto es imposible dejar de lado las amenazas de seguridad. En el mercado existen herramientas que ofrecen seguridad en internet, son soluciones de software que permiten controlar el acceso a internet y brindar protección ante posibles amenazas, como *malware*. En la tabla I se muestran las tres mejores opciones del mercado para el 2015, con una comparativa de las características incluidas.

Tabla I. Soluciones de seguridad en 2015

Aspecto	**BitDefender Internet Security**	**Symantec Norton Security**	**Kaspersky Internet Security**
Costo de licencia anual para múltiples usuarios	$ 79,95	$ 79,99	$ 79,95
Cortafuegos	Sí	Sí	Sí
Antispam	Sí	Sí	Sí
Control parental	Sí	Sí	Sí
Copia de respaldo	No	Sí	No
Optimización	Sí	Sí	Sí

Fuente: elaboración propia, basada en RUBENKING, Neil. *The Best Security Suites for 2015.* http://www.pcmag.com/article2/0,2817,2369749,00.asp. Consulta: mayo de 2015.

Aunque las herramientas de seguridad en internet son bastante funcionales, la mayoría solo está disponible para computadoras o servidores. Existen soluciones para teléfonos inteligentes o tabletas, pero su efectividad es menor en comparación con sus pares para computadoras. Además, estas herramientas consumen bastantes recursos de memoria y procesamiento, por lo que es imposible incluirlos en dispositivos de bajos recursos, como los utilizados en los objetos que se conectan al internet de las cosas.

Muchos esfuerzos se han realizado para mejorar los métodos de seguridad y comunicación desde la creación de internet. Por ejemplo, la seguridad de la capa de transporte (TLS, por sus siglas en inglés) incluye protocolos criptográficos que permiten una comunicación segura de los dispositivos a través de la red. Esta capa se agrega a los paquetes que transitan a través de la red, por medio de certificados de seguridad que proporcionan autenticación y privacidad. Quizás esta sea la única manera de garantizar seguridad real para los usuarios, pero no es impenetrable.

3. LA PRIVACIDAD DE LA INFORMACIÓN EN EL INTERNET DE LAS COSAS

3.1. Protocolos de comunicación

Los dispositivos que se conectan al internet de las cosas, debido a su diversidad, poseen en algunos casos limitaciones de espacio, por este motivo se ha apostado por la conexión inalámbrica por medio de ondas de radio para realizar la comunicación, ya que agregar un elemento de comunicación cableada a estos dispositivos limitaría al extremo su operación y no se cumpliría con el objetivo de la computación ubicua, computación presente en cualquier lugar y en cualquier momento.

Para los dispositivos de domótica, que generalmente no presentan mucho movimiento y poseen, en la mayoría de situaciones, un lugar fijo dentro de los hogares, las limitaciones cableadas no son tan significativas como para otros dispositivos. A pesar de esto, el crecimiento en la infraestructura inalámbrica y el mejoramiento de los protocolos de comunicación ha permitido que todos incluso los electrodomésticos cuenten con una conexión de este tipo.

Televisiones inteligentes, refrigeradoras, estufas, ventanas, controles de climatización e iluminación se pueden comunicar entre sí para componer una red robusta dentro del hogar, haciendo la vida de sus ocupantes mucho más sencilla. El internet de las cosas tiene como objetivo no solo conectar los dispositivos a internet, sino crear una operación armónica de los mismos, sin la interacción de los seres humanos.

3.1.1. Estándar IEEE 802.15.4

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, por sus siglas en inglés) se encarga de definir distintos protocolos y estándares de comunicación. La familia de protocolos 802 define las tecnologías físicas y de enlace de datos, incluyendo los métodos de acceso a la red y la lógica de los paquetes enviados a través de esta, para permitir la comunicación entre distintos dispositivos.

El estándar 802.15.4 fue publicado en 2003 y revisado en 2006, este especifica los elementos de la capa física y de enlace de datos para redes de área personal inalámbricas con baja tasa de transferencia de datos (LR-WPAN, por sus siglas en inglés). El objetivo de este estándar es definir la manera de comunicación para dispositivos con bajos recursos y que necesitan comunicarse de manera inalámbrica, sin emplear otras tecnologías que suponen un alto coste en procesamiento y energía.

Este estándar está diseñado para transferir información en una distancia de diez metros, a una tasa de transferencia de 250 kbps, aunque puede utilizarse con tasas de 20 y 40 kbps, representando un consumo energético bastante bajo. Para dispositivos que se comunican entre sí y que no requieren altos niveles de procesamiento, estas tasas de transferencia son suficientes. El estándar permite la comunicación a través de tres bandas de de frecuencia: 868, 915 y 2450 MHz, aunque la más utilizada en la actualidad es la de 2450 MHz.

El estándar 802.15.4 ha dado lugar a especificaciones comerciales que trabajan sobre este, algunos ejemplos son ZigBee y 6LoWPAN, que incrementan la funcionalidad y han agregado nuevas bandas frecuencia para el

envío y recepción de datos. Muchos de los dispositivos que en la actualidad se conectan al internet de las cosas hacen uso de este estándar o alguna de las especificaciones comerciales derivadas de este y su gran éxito se debe al bajo consumo energético, que en este tipos de dispositivos, es de suma importancia.

Otro elemento clave para la utilización de este estándar es el direccionamiento de los dispositivos. Cada uno de los que utilizan 802.15.4 para la comunicación necesita una dirección única de 64 bits y que permita diferenciarlo de cualquier otro dispositivo en el planeta, esta dirección se conoce como identificador único extendido (EUI-64). Para ahorrar energía, enviando paquetes más pequeños los dispositivos pueden solicitar al controlador de la red de área personal (PAN, por sus siglas en inglés) una dirección de 16 bits, que los identifica únicamente en esa red.

Un aspecto importante, y que es relevante mencionar en este documento, es que el estándar 802.15.4 permite el uso de criptografía con cifrado simétrico para garantizar la confidencialidad, la autenticidad de los datos y evitar la repetición de información que viaja de manera inalámbrica de un dispositivo a otro. Esto permite garantizar la seguridad y privacidad, en especial para los elementos conectados al internet de las cosas y que pueden manejar datos e información sensible.

3.1.2. Comunicación mediante cableado eléctrico (PLC)

La comunicación mediante cableado eléctrico (PLC, por sus siglas en inglés) tiene como objetivo la conexión de dispositivos utilizando la red de energía eléctrica que se encuentra presente en casas y oficinas. La principal ventaja de esta tecnología es que no es necesario construir una nueva red, la

red existe y solo es necesario controlar la manera en la que se envía la información a través de este canal. Esto supone una gran ventaja, en especial para los dispositivos de domótica que se conectan al internet de las cosas, porque pueden conectarse entre sí utilizando la misma conexión que utilizan para alimentarse de energía eléctrica.

Los primeros experimentos para transmitir información a través del cableado eléctrico iniciaron a mediados de 1985, pero fue hasta 1997, cuando se realizaron las primeras pruebas de transmisión bidireccional. Desde entonces solo se ha mantenido un desarrollo lento de esta tecnología. Con la aparición de más dispositivos con capacidades para conectarse al internet de las cosas, PLC tomó auge, pero su crecimiento se ha visto limitado con la aparición de tecnologías inalámbricas como el protocolo IEEE 802.15.4, aunque para dispositivos de domótica ambos son opciones viables de comunicación porque estos, por lo general, no presentan mucho movimiento.

La desventaja más notable de la tecnología PLC es el ruido que se introduce en las señales que viajan a través del cableado. Al ser un medio que no fue diseñado para el envío y recepción de datos, no cuenta con medidas de diseño que permitan aislar las interferencias producidas por otras señales o aparatos eléctricos. El envío de datos generalmente se realiza a través de un único cable, de los dos o tres con los que cuentan las instalaciones eléctricas habituales, y esto lo hace susceptible a las variaciones que existen en la transmisión de las señales eléctricas. Es posible también, que las señales inalámbricas como las emitidas por dispositivos wifi o cualquier onda de radio cause interferencia en la transmisión de los datos, haciendo que la comunicación no sea del todo precisa.

3.2. ¿A quién pertenece la información y los datos?

El elemento más importante en el internet de las cosas son los datos que los dispositivos capturan y generan a partir de su interacción con otros dispositivos y con el entorno. Para las personas u organizaciones que hacen uso de estos dispositivos es necesario conocer a quién pertenecen realmente los datos y la información que se genera en sus dispositivos y que fluye a través del internet de las cosas.

Los electrodomésticos y dispositivos de domótica cuentan con una construcción de fábrica poco personalizable y los elementos que permiten capturar datos y procesar la información, generalmente se encuentran encapsulados, de manera que los usuarios finales no puedan cambiar sus configuraciones, viéndose en la necesidad únicamente de aceptar lo que los aparatos hacen. Desde este punto de vista los datos que estos aparatos capturan y generan, pertenecen al fabricante del dispositivo, porque no permiten al usuario personalizar la manera en que este proceso se realiza.

Algunos fabricantes prefieren no responsabilizarse por el manejo de los datos y la información, delegando esta función a un tercero, encargado de procesar todos los datos e información de los usuarios que los dispositivos conectados al internet de las cosas generan. Los datos como tales no cuentan con un propietario, porque son elementos básicos, mientras que la información que se crea a partir del conjunto de esa información es lo que debe preocupar al usuario final y es sobre esta en la que aparecen muchos actores interesados sobre la propiedad de la misma. Cuando una empresa se convierte en propietaria de la información de un usuario, puede utilizarla para su propio beneficio, sin importar las decisiones del usuario.

Las empresas que manejan la información y los datos de los usuarios deberían garantizar la privacidad y seguridad de esa información, pero en algunos casos y aprovechando que la mayoría de usuarios no leen los términos y condiciones de servicio y privacidad, hacen uso de la información para crear estrategias de mercado o para guiar las preferencias de los usuarios hacia productos de la misma compañía o de sociedades comerciales afines. En casos más difíciles esa información es vendida a otros interesados, sin informar a los usuarios finales qué se hace con su información.

Mientras no se establezca de manera clara quién controla los datos y la información de los usuarios, existirán muchas disputas, tanto legales como comerciales y con el ritmo de crecimiento del internet de las cosas es necesario que las legislaciones de los países cambien a favor de los usuarios, que son los más afectados por el uso de su información. Mientras esto no exista la información pertenecerá a las empresas y organizaciones con los suficientes recursos económicos y de computación para manejar y procesar las grandes cantidades de datos que fluyen a través de la infraestructura que soporta al internet de las cosas.

3.3. Retos de privacidad y seguridad

El crecimiento del internet de las cosas, tal y como fue definido en sus orígenes, supondrá la omnipresencia de la conectividad entre dispositivos que solo estarán limitados por la imaginación. Este tipo de presencia que tendrá el internet de las cosas en los próximos años supondrá grandes riesgos en materia de privacidad y seguridad de la información que allí se maneja. La complejidad de los riesgos y su nivel de incidencia en las vidas de los usuarios estarán determinados por las circunstancias del desarrollo de los dispositivos.

Hacer que la vida de las personas sea más sencilla a través de estos dispositivos supone que en algún momento estos sean cada vez más autónomos y puedan considerarse inteligentes, llegando a los casos en que tomarán decisiones y actuarán, comunicándose con los demás dispositivos que se encuentren en su entorno, para evitar que el usuario no realice acciones, pero esta comunicación es la que presenta los retos más grandes para que el internet de las cosas sea exitoso.

Aplicar las soluciones tradicionales de privacidad y seguridad de la información al internet de las cosas es complicado, tanto por las tecnologías que lo soportan como por la visión que este tiene. Los dispositivos tienen recursos limitados y algunas de las soluciones tradicionales requieren altos niveles de procesamiento, cosa que no es factible en el internet de las cosas. A continuación se analizan los retos en materia de privacidad y seguridad que se presentan en el internet de las cosas.

El primer reto que afronta el internet de las cosas es la continuidad y disponibilidad de los servicios basados en esta tecnología. Debido a la gran cantidad de dispositivos y la alta demanda de conexión, los servicios que ofrecen los proveedores deben estar disponibles todo el tiempo y la continuidad en la operación de los mismos debe garantizarse. Interrupciones en estos dos elementos producirían que la información no viaje de manera garantizada a su destino y que pueda sufrir pérdidas en el camino.

Otro de los retos es integrar la seguridad de la información en los dispositivos de domótica y cosas inteligentes que se conectarán al internet de las cosas. Los métodos actuales de aseguramiento de la información y los datos no es aplicable para los dispositivos que actualmente existen en el

mercado y es necesario que estos cuenten con características que permitan a los usuarios y organizaciones sentirse seguros, teniendo la certeza que los dispositivos que tienen a su alrededor están haciendo un uso correcto y adecuado de su información.

También existe como reto inminente el manejo del crecimiento de las conexiones al internet de las cosas, ya que mientras más objetos y personas están involucradas en un entorno, se vuelve más complejo y difícil de manejar cada una de las situaciones individuales que puedan surgir dentro del mismo. Para garantizar la privacidad y seguridad en un entorno abierto donde pueden existir muchos actores, que de manera involuntaria pueden alterar el funcionamiento de los demás elementos, los dispositivos deben manejar de manera individual muchos conflictos de tratamiento de datos.

La confianza que los usuarios tienen en los dispositivos que utilizan es muy importante, es un reto para los fabricantes que sus clientes se sientan seguros al utilizar un producto, más si este manejará grandes cantidades de datos e información de él y que pueden quedar expuestos por algún fallo en los sistemas de seguridad. La confianza es el atributo que más cuidado las empresas deberían poner, porque si un usuario siente confianza en un dispositivo o un producto, es muy probable que lo siga utilizando o adquiera uno de características similares.

Proporcionar seguridad solo en las comunicaciones entre dispositivos no es suficiente, los sistemas que funcionan sobre el internet de las cosas son sensibles a ataques externos que pueden terminar en el robo o pérdida total de la información de un usuario y esta puede ser sensible. Es un reto también para los fabricantes de dispositivos y para las empresas que crean toda la tecnología

que soporta al internet de las cosas, porque si los equipos y sistemas son vulnerables el usuario será vulnerable y se verá un escenario contrario al que se espera con el internet de las cosas, los dispositivos perjudicarán al usuario en lugar de ayudarlo.

Por último, otro de los retos al crear dispositivos con cierto grado de inteligencia que se conectan al internet de las cosas es la sensación de control que tiene el usuario. A pesar de que estos dispositivos pueden tomar decisiones autónomas y actuar por nosotros, los seres humanos por su naturaleza necesitan tener el control sobre las cosas, si un dispositivo da la sensación de no poder ser controlado, entonces generará desconfianza y hará que el usuario sienta que está perdiendo el poder de decisión.

3.4. Soluciones propuestas

El internet de las cosas es nuevo y necesita que muchas cosas maduren y se hagan más robustas. En la sección anterior se mencionaron los retos en materia de privacidad y seguridad que esta tecnología afronta en su desarrollo y operación. A continuación se presentan soluciones que podrían a largo plazo solventar los problemas que puedan generarse de las limitaciones que el internet de las cosas presenta en su etapa inicial.

Para resolver el problema de continuidad y disponibilidad de los servicios basados en el internet de las cosas, los fabricantes y proveedores de servicios deben primero medir la demanda y hacer una proyección a futuro del tipo de consumo que los dispositivos y cosas inteligentes realizarán sobre esta tecnología, para garantizar que la infraestructura que implementen sea escalable a futuro y pueda cubrir las necesidades de acceso que los

dispositivos demandan. Con esto se garantizaría que la información viaja de manera correcta y puntual a su destino, sin retrasos o circunstancias que puedan afectar la privacidad y seguridad.

En el caso de la integración de la seguridad directamente sobre los dispositivos, es necesario que los fabricantes tomen en cuenta que los métodos actuales son deficientes, se debe construir un sistema seguro, desde la etapa de diseño del dispositivo y no como un valor adicional en la etapa de producción, los recursos son limitados y los fabricantes podrían, por ejemplo, agregar un componente de bajo consumo que se encargue únicamente del procesamiento de mecanismos de seguridad para la información y los datos.

Ante el inminente crecimiento acelerado de dispositivos que se conectan al internet de las cosas, los fabricantes deben tomar en este momento, cuando la madurez de esta tecnología no se ha alcanzado, las medidas necesarias para dotar a los dispositivos con capacidades individuales que les permitan aislar su comportamiento de la demás red de dispositivos en entornos abiertos, donde la interacción no sea exclusiva con un usuario y que pueda producir un riesgo de privacidad y seguridad de la información intercambiada por los mismos.

Para que los usuarios sientan confianza en los dispositivos que emplean en su vida diaria estos deben ser sencillos y simples en su utilización, además el proceso de captura, procesamiento y transmisión de los datos e información que recopilan debe ser transparente, de manera que el usuario no sienta que existe algo escondido en el manejo de sus cosas personales. Es tarea de los fabricantes hacer que los dispositivos cuenten con estas características, y como se mencionó en el apartado anterior, esto creará una cultura de identificación con el dispositivo y la marca.

Por otro lado, hacer que los sistemas y los dispositivos sean seguros contra ataques maliciosos es aún más complicado, porque las limitaciones en espacio y recursos son altas, la opción más acertada es agregar la seguridad en la arquitectura de comunicación y no en los dispositivos en sí. Si la red es segura, entonces los dispositivos que se conectan a ella se encontrarán seguros, garantizando que los datos y la información de los usuarios se maneja de la manera correcta y con los fines esperados.

La autonomía de los dispositivos no debe ofuscar la capacidad de los seres humanos para controlarlos, es indispensable que los fabricantes diseñen los dispositivos y las interfaces de manera que el usuario tenga control sobre estos, de esta manera se creará confianza y una sensación de poder sobre la tecnología. Quizás es interesante un mundo donde todo funcione de manera automática, pero los fabricantes y compañías deberán sacrificar esa armonía por la capacidad de controlar completa o parcialmente lo que los dispositivos hacen.

3.5. Manejo de la información

La información que los usuarios confían a sus dispositivos es muy importante y como se menciona en las secciones anteriores, es primordial que el usuario sienta que su información está segura y que además los dispositivos respeten su privacidad, manejando los datos e información de una manera adecuada y que en ningún momento perjudique sus intereses. En este sentido los proveedores de servicios en el internet de las cosas y los fabricantes de dispositivos deben poner a disposición de los usuarios las reglas y condiciones de servicio.

A través de un contrato de servicio, las partes interesadas, tanto el proveedor como el cliente, acuerdan los niveles de aceptación para que el servicio se considere funcional, así como las condiciones para que este se de. Un contrato es la única manera que los proveedores y los clientes tienen una manera de defender sus derechos y obligaciones, si es necesario ante las entidades de ley correspondientes.

El manejo de la información es un tema que debe preocupar tanto a los usuarios y proveedores del servicio como a los fabricantes de dispositivos. Con respecto a los dispositivos de domótica, la información que estos comparten permite mejorar la calidad de vida de los habitantes de la casa, pero también cuentan con información importante como los historiales clínicos o los hábitos de alimentación de los ocupantes de la vivienda. También temas como la seguridad física de los usuarios también concierne al internet de las cosas, en especial a los dispositivos de domótica que se encuentran conectados. Un mal manejo de la información podría resultar no solo en la violación de la privacidad, sino en el daño físico de alguno de las personas que viven en el hogar.

Los términos y condiciones de uso, seguridad y privacidad son presentados a los usuarios finales a través de distintos medios. La mayoría de las veces los usuarios no prestan la debida atención a las características que el proveedor del servicio plasma en este documento y confía ciegamente en que sus datos e información contarán con privacidad y seguridad, sin siquiera enterarse que se está aceptando, en algunos casos, la comercialización de los mismos sin requerir algún permiso adicional o eliminando cualquier responsabilidad del proveedor sobre el uso que se haga de la información.

Los proveedores están obligados a presentar a los usuarios finales la manera en que se manejará su información, no solo para dar una sensación de seguridad al usuario, sino para hacer el proceso mucho más transparente. Actualmente se están desarrollando leyes y convenios en la Unión Europea y Estados Unidos, sobre el manejo que debe darse a la información en el internet de las cosas, así como las regulaciones y sanciones aplicables en este tema. En Guatemala no existe ningún precedente de legislaciones de este tipo, por lo que habrá que esperar algunos años, mientras la penetración del internet de las cosas crece, para que puedan adoptarse regulaciones que probablemente serán muy parecidas a las de los territorios ya mencionados.

La única manera en la que los usuarios pueden tener certeza de que su información se encuentra segura, es conociendo el proceso que los proveedores de servicios y fabricantes de dispositivos realizan para manejar los datos y la información que se genera y captura del entorno y que es transmitida por alguna de las tecnologías de comunicación a través del internet de las cosas. Leer y acordar los términos y condiciones, así como los contratos del servicio permite que exista una relación formal, donde ambas partes se encuentran satisfechas con las condiciones bajo las cuales se brindará o consumirá un servicio.

3.6. Estandarización y confiabilidad

La estandarización de la tecnología permite que se incremente la calidad de los productos, ya que se asegura la operación correcta de todos los componentes de un dispositivo y, que a la vez, podrán interactuar con otros componentes que cumple con las mismas especificaciones. Esto es particularmente funcional cuando las interfaces de los dispositivos necesitan

comunicarse con interfaces desarrolladas por otros fabricantes o cuando estos pertenecen a usuarios distintos y que no precisamente están configurados de la misma manera. La estandarización, en general, promueve el crecimiento del mercado, brindando mayores beneficios a los usuarios y agregando valor a los productos finales.

Para el internet de las cosas es necesario definir ciertos estándares que permitan crear armonía en la comunicación y utilización de los dispositivos y cosas inteligentes que forman parte de esta red. El formato de la información que es transmitida entre dispositivos, las características de las interfaces y los protocolos de comunicación son ejemplos claros de las necesidades que el internet de las cosas presenta y es necesario que las empresas y fabricantes que crean dispositivos y mantienen la infraestructura que hace posible la conexión entre los mismos trabajen de manera conjunta con los los entes internacionales, como la Organización Internacional de Estandarización (ISO, por sus siglas en inglés) y la IEEE.

Los hogares inteligentes que hacen uso de dispositivos de domótica, generalmente electrodomésticos, son posiblemente el ejemplo más claro de la necesidad de estandarización. Algunos fabricantes garantizan la operación exitosa de estos dispositivos, pero únicamente con otros dispositivos de la marca y de manera parcial con objetos creados por socios comerciales. Un hogar inteligente requiere que todos los dispositivos puedan comunicarse de manera normalizada y unificada, donde todos entiendan las mismas instrucciones y que puedan trabajar de manera colectiva sin importar el fabricante o la configuración de estos sistemas, para hacer que la experiencia del usuario final sea transparente y útil.

La identificación de los dispositivos en el internet de las cosas aún necesita un estándar funcional, desde la concepción inicial de esta visión se han creado múltiples variaciones de la RFID y no existe en la actualidad una versión oficial. Muchos fabricantes se han dado a la tarea de agregar sus propias características, impidiendo que se tenga un estándar único para la identificación de los dispositivos a nivel mundial. Empresas con fuerte influencia y poder económico en el sector, como Google y Microsoft en conjunto con la ISO y la IEEE han realizado esfuerzos para que se aplique una estandarización real de la identificación de los dispositivos.

Un beneficio real que los usuarios finales podrán percibir en un entorno estandarizado será la libertad de escoger a cualquier proveedor de servicios. Un dispositivo creado por un fabricante y que trabaja con determinado operador de servicios podrá migrar fácilmente a otro proveedor, sin necesidad de modificar los componentes del dispositivo. Por otro lado, cuando se defina un estándar de comunicación y la forma en que la información será interpretada, un usuario podrá, por ejemplo, tener dos televisores inteligentes, totalmente distintos y de diferentes fabricantes, mostrando la misma información en ambientes distintos dentro de un hogar, haciendo que la experiencia sea unificada.

Concretamente las organizaciones internacionales encargadas de la estandarización y los grandes fabricantes de productos y servicios destinados al internet de las cosas deben normalizar la forma en que se identifican los objetos, los métodos en que se utilizarán para transferir, procesar y analizar la información generada y capturada por los dispositivos y los protocolo de conexión a la red que compondrá la siguiente generación del internet.

3.7. Gobernanza del internet de las cosas

La gobernanza se refiere a todas las acciones que se llevan a cabo para conducir de manera exitosa una actividad y comprende un conjunto de reglas, instituciones y prácticas que buscan de manera colectiva alcanzar ciertos objetivos iniciales. Puede hablarse de gobernanza también como la discusión sobre la correcta asignación de tareas y actividades para conseguir los objetivos organizacionales.

El tema de gobernanza está vinculado estrechamente con las regulaciones que se aplican y sin lugar a duda el internet de las cosas necesita ser regulado y controlado para que su funcionamiento sea el adecuado en las diferentes circunstancias y escenarios que aparezcan. El gobierno es el ente encargado de aplicar la gobernanza y es por este motivo que es necesaria la creación de uno, compuesto por varias organizaciones, que vele por la aplicación de las regulaciones pertinentes.

Un aspecto muy importante y que no ha sido tratado por los distintos entes internacionales interesados en el tema de la gobernanza del internet de las cosas, es si este debe gobernarse en conjunto con el internet convencional o de manera separada, ya que el núcleo de su funcionamiento es el internet convencional. Debido a las diferencias que existen en los intereses sobre el internet y el internet de las cosas, lo más acertado es separar los gobiernos de ambos, de manera que uno no interfiera con el otro y estableciendo los límites y alcances en las regulaciones.

El tema más importante al crear un gobierno para el internet de las cosas es la inclusión de todos los interesados, además de la creación de un sistema completamente transparente, donde las decisiones acerca del futuro del internet de las cosas sean de dominio público y que los mismos usuarios puedan tomar partido en estas decisiones. El gobierno deberá encargarse de crear todas las regulaciones y apoyarse en los entes de justicia para hacerlas cumplir. Es importante que los temas de privacidad y seguridad de los datos sean los de mayor relevancia en las discusiones que el gobierno tome, porque al final son los elementos principales del internet de las cosas.

La gobernanza del internet de las cosas creará grandes beneficios a nivel internacional, no solo para los fabricantes y proveedores de servicio, sino también para los usuarios finales, quienes utilizarán los dispositivos y cosas inteligentes como un agregado a su vida y de acuerdo a la idea original del internet de las cosas, se espera que la experiencia del usuario sea sencilla y que facilite todas las tareas, manejando de manera adecuada toda la información. Solo un gobierno bien establecido y responsable podrá garantizar que estos principios se cumplan.

4. ANÁLISIS DE PERCEPCIÓN

4.1. Descripción de la encuesta

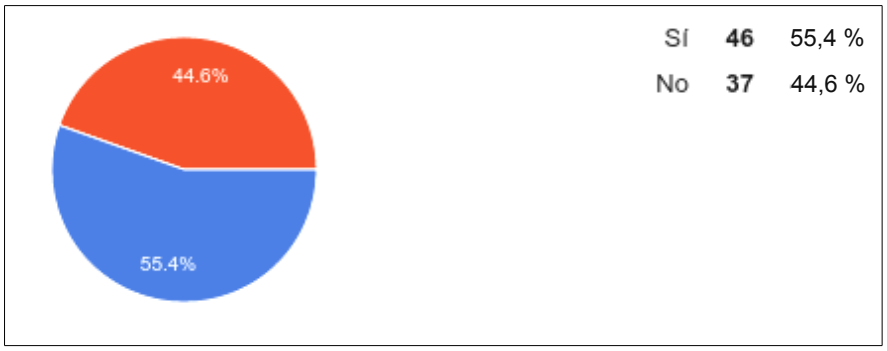
Para realizar un análisis de la percepción que los usuarios tienen sobre el internet de las cosas, domótica, privacidad y seguridad, se realizó una encuesta con diez preguntas. Se tomó una muestra de 83 personas, comprendidas entre los 18 y 30 años de edad, en su mayoría estudiantes de ingeniería y se les solicitó responder la encuesta con base en sus experiencias personales.

El cuestionario se compone de diez preguntas cerradas de opción múltiple, de las cuales ocho son preguntas de hecho y dos son preguntas de intención. Para el proceso de obtención de las respuestas se utilizó un formulario electrónico, disponible en un enlace público a través de la plataforma Google Drive. No se recopiló de ninguna manera los datos personales de los usuarios que proporcionaron sus respuestas.

4.2. Análisis de los resultados

La primera pregunta que se presentó en el cuestionario es: ¿Ha escuchado acerca del internet de las cosas? Para esta pregunta se presentaron dos opciones de respuesta: sí y no. En la figura 4 se puede observar los resultados de la tabulación de respuestas para esta pregunta y la gráfica de los porcentajes de respuesta de cada una de las opciones.

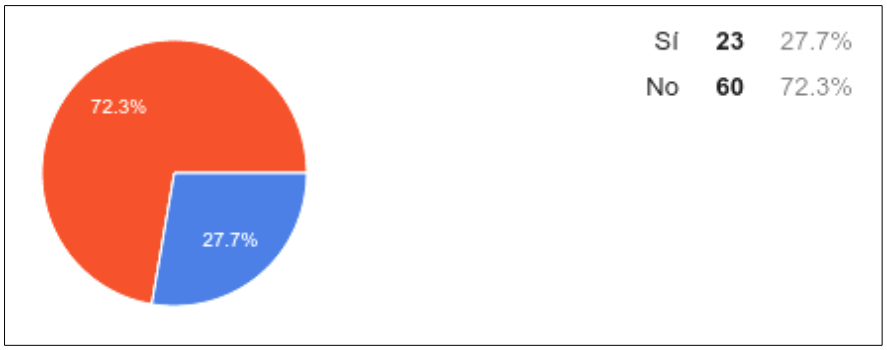
Figura 4. **Resultados de la pregunta 1**



Fuente: elaboración propia.

La distribución de las respuestas para esta pregunta es bastante equitativa, con una diferencia del 10,8 % entre cada una de las opciones. Se ve una ligera tendencia al conocimiento del internet de las cosas, esto se debe a que recientemente en las redes sociales el tema ha cobrado importancia.

Figura 5. **Resultados de la pregunta 2**



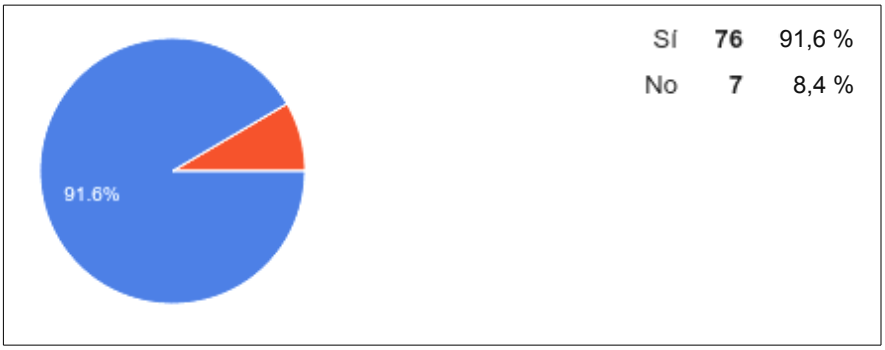
Fuente: elaboración propia.

La segunda pregunta que se presentó en el cuestionario es: ¿Considera que internet es un lugar seguro para su información? Al igual que en la pregunta anterior se proporcionaron dos opciones de respuesta: sí y no. En la figura 5 se presentan los resultados de la tabulación de respuestas y porcentajes.

Para esta pregunta se puede observar la desconfianza que los usuarios tienen sobre la seguridad de la información que internet proporciona. Es bastante lógico que las respuestas se inclinen por la respuesta negativa, ya que se han confirmado muchos casos en los que se ha violado la privacidad y seguridad de los usuarios.

La tercera pregunta que se planteó a los encuestados es: ¿Se preocupa por la privacidad de sus datos e información personal? Proporcionando dos opciones de respuesta: sí y no. En la figura 6 se presentan los resultados para la tabulación correspondiente a esta pregunta y los respectivos porcentajes.

Figura 6. **Resultados de la pregunta 3**



Fuente: elaboración propia.

Los resultados reflejan una clara preocupación de los encuestados sobre la privacidad de su información personal. Es importante mencionar que estos resultados representan una idea que se sabe de hace mucho tiempo, la mayoría de personas se preocupan por su privacidad, en especial cuando está relacionada con información sensible.

La cuarta pregunta que forma parte del cuestionario es: ¿Qué tanta información personal comparte en internet? Para este caso se presentaron cinco opciones de respuesta: ninguna, poca, moderada, mucha y toda. Esta pregunta busca medir en una escala de cinco posiciones la disposición que tienen los usuarios a compartir su información personal con las demás personas, a través de plataformas de interacción social. En la figura 7 se puede observar el resultado de la tabulación de respuestas y porcentajes representativos para cada opción.

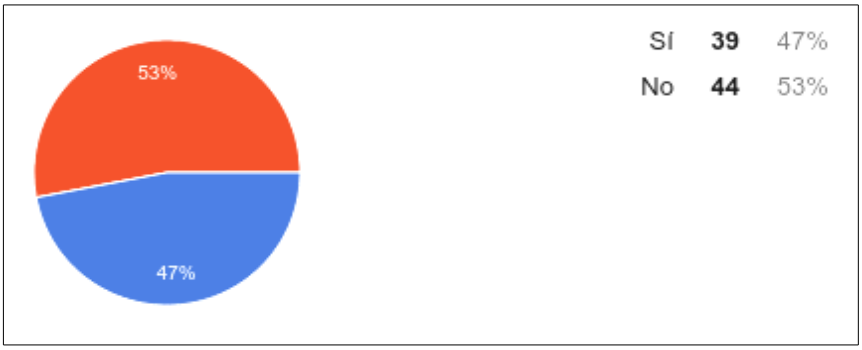
Figura 7. **Resultados de la pregunta 4**

Fuente: elaboración propia.

Debido a la naturaleza de la encuesta, se puede observar que todos los usuarios comparten su información de alguna forma en internet. De acuerdo a los resultados expresados en la gráfica anterior, se observa una respuesta entre poca y moderada al compartir la información, a pesar de que las redes sociales son un medio ideal para compartir toda la información, los usuarios están conscientes de los riesgos.

La quinta pregunta que se utilizó para este análisis es: ¿Considera que las casas inteligentes son seguras? Con esta pregunta se trata de conocer la opinión de los usuarios con respecto a las casas que cuentan con dispositivos de domótica y que de alguna u otra manera brindan opciones de control de la seguridad. Las opciones que se presentaron son: sí y no. En la figura 8 se puede observar los resultados de la tabulación y los porcentajes correspondientes a la opinión de los encuestados.

Figura 8. **Resultados de la pregunta 5**

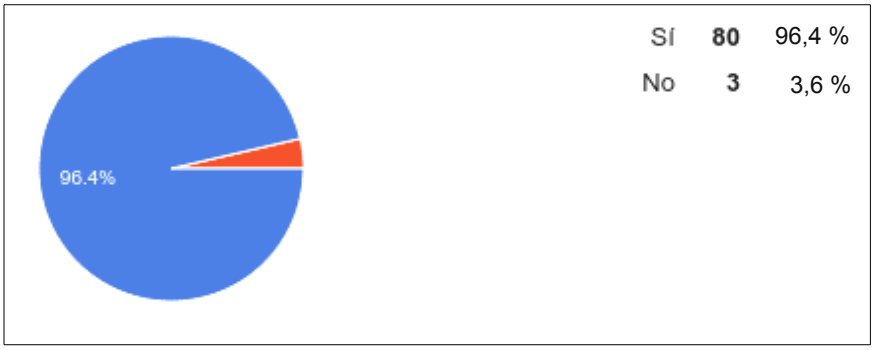


Fuente: elaboración propia.

De nuevo se presenta una respuesta dividida por parte de los encuestados, pero se puede observar que existe una mayoría que expresa su desconfianza ante las casas inteligentes. Esta respuesta indica que los usuarios no confían en la seguridad que la tecnología puede brindar a un hogar, es de esperar que los usuarios no confíen en dispositivos que pueden ser vulnerados con facilidad.

La sexta pregunta que se empleó en el cuestionario es: ¿Posee algún dispositivo inteligente? (teléfono, tableta, reloj, entre otros). Y las opciones de respuesta que se se presentaron son: sí y no. En la figura 9 se puede observar los resultados de la tabulación y los porcentajes correspondientes. El objetivo de esta pregunta era medir la penetración de los dispositivos con conexión a internet dentro de la muestra seleccionada.

Figura 9. **Resultados de la pregunta 6**



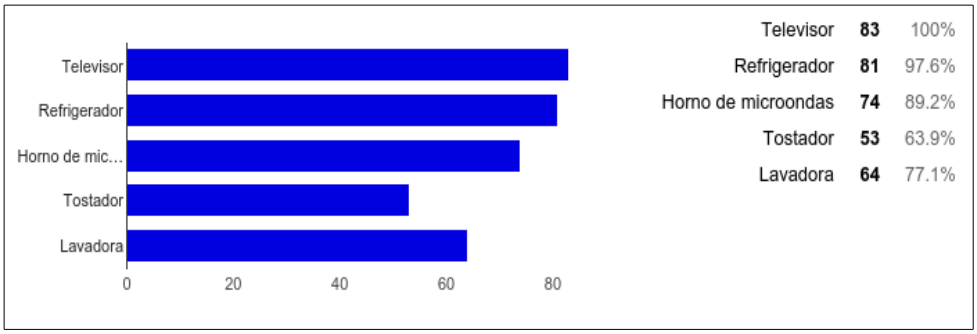
Fuente: elaboración propia.

De los resultados anteriores se puede observar que los usuarios que realizaron la encuesta en casi su totalidad poseen un dispositivo inteligente,

esto refleja el crecimiento y penetración de la este tipo de tecnología en la actualidad y con el grupo objetivo, este dato puede sugerir que el internet de las cosas será una opción para estos usuarios.

La séptima pregunta que se presentó a los encuestados es: ¿Cuáles de los siguientes electrodomésticos posee en su hogar? Proporcionando como opciones de respuesta las siguientes: televisor, refrigerador, horno de microondas, tostador y lavadora. A diferencia de las demás preguntas en el cuestionario en esta los usuarios podían seleccionar ninguna, una o más opciones.

Figura 10. **Resultados de la pregunta 7**



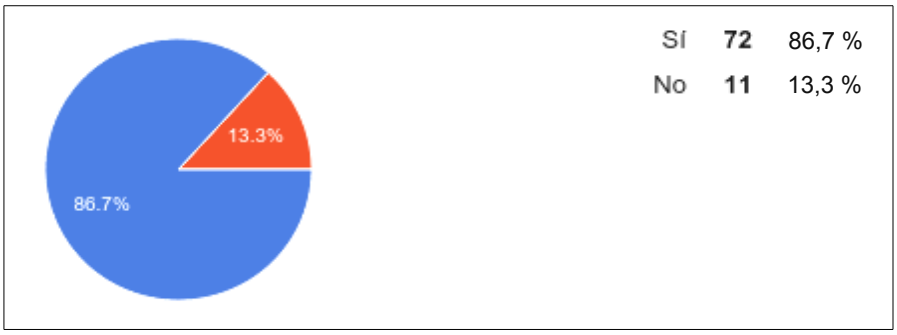
Fuente: elaboración propia.

En la figura 10 se puede observar los resultados de la tabulación y porcentajes correspondientes a la séptima pregunta. De acuerdo a estos resultados se puede observar que todos los encuestados poseen un televisor, seguido por un refrigerador y en porcentajes menores los demás electrodomésticos. Esta respuesta puede servir para seleccionar un producto

insignia en dispositivos de domótica: el televisor.

La octava pregunta que aparece en el cuestionario es: ¿Le gustaría que sus electrodomésticos se comuniquen entre sí, le brinden ayuda y faciliten sus tareas diarias? Esta es la primera de las preguntas de intención y busca medir qué tan abiertos están los encuestados a la domótica y el internet de las cosas. Las opciones que se presentaron como respuesta son: sí y no. En la figura 11 se puede observar los resultados de la tabulación y porcentajes de respuesta.

Figura 11. **Resultados de la pregunta 8**



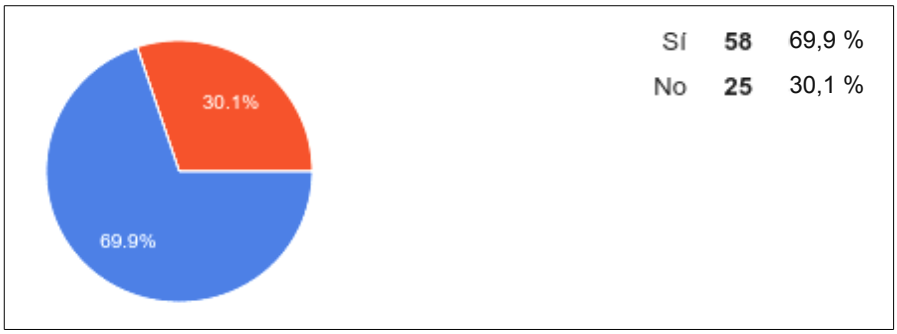
Fuente: elaboración propia.

De acuerdo a los resultados, la mayoría de los encuestados estaría en disposición de utilizar dispositivos de domótica que se comuniquen a través del internet de las cosas, para facilitar las actividades dentro del hogar.

La novena pregunta que se presentó a los encuestados es: ¿Estaría dispuesto a realizar una inversión económica en dispositivos para el hogar que se conecten a internet? Siendo la segunda pregunta de intención, en la que se

proporcionaron las opciones de respuesta: sí y no. En la figura 12 se puede observar el resultado de la tabulación de respuestas y los porcentajes correspondientes a cada una de las opciones.

Figura 12. **Resultados de la pregunta 9**

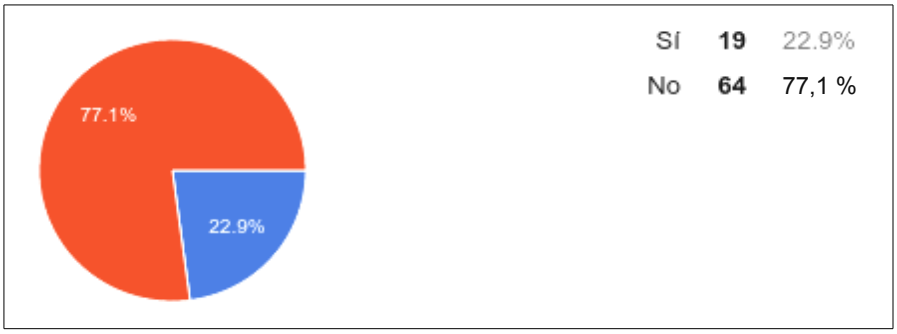


Fuente: elaboración propia.

En estos resultados no se ve una diferencia muy marcada, pero sí se puede observar una inclinación de los encuestados a adquirir un dispositivo de domótica para facilitar las tareas en el hogar. Sin lugar a duda, el internet de las cosas hará que todos los dispositivos comunes en el hogar se conviertan en dispositivos que hagan la experiencia de vivir más placentera.

La décima y última pregunta que se presentó en el cuestionario es: ¿Está acostumbrado a leer los términos y condiciones de uso, servicio y privacidad de los productos y servicios informáticos que adquiere? Las opciones de respuesta que se presentarón son: sí y no. Por medio de esta pregunta se midió el porcentaje de encuestados que se preocupa por los términos de un servicio que adquiere. En la figura 13 se pueden observar estos porcentajes y resultados.

Figura 13. **Resultados de la pregunta 10**



Fuente: elaboración propia.

De los resultados anteriores se puede observar que la mayoría de usuarios no se preocupa por los términos y condiciones al momento de adquirir un producto o servicio. Como se mencionó en apartados anteriores, el interés que el usuario presta a estas situaciones es un factor determinante en qué datos e información se comparte y se establece en gran medida la privacidad y seguridad que se aplicará a estos.

4.3. Percepción de los usuarios

Del análisis de resultados de la sección anterior se puede concluir que los usuarios demuestran aceptación a los dispositivos inteligentes y a los dispositivos de domótica para facilitar sus tareas diarias. Se puede observar también, que los problemas que presenta el internet de las cosas, expuestos en las secciones anteriores, también son importantes para los usuarios, aún cuando no han interactuado con dispositivos de ese tipo. La privacidad y seguridad son temas muy sensibles y es necesario que los fabricantes los

tomen en cuenta en la construcción de nuevos dispositivos. Es necesario que los usuarios tomen en cuenta los términos y condiciones de servicio, es posiblemente el principal punto de debilidad al usar los servicios.

Los usuarios no confían en los dispositivos de domótica para garantizar la seguridad dentro del hogar y el televisor es el producto que las grandes empresas pueden utilizar como ancla para migrar a todos los usuarios a un hogar inteligente, pero es necesario que primero se establezcan las bases de comunicación y estándares para que la interacción con los dispositivos sea segura y útil para los usuarios.

CONCLUSIONES

1. Desde la aparición de internet a mediados de los años noventa, no se había presentado una tecnología tan disruptiva como el internet de las cosas. Este tema empieza a tomar importancia y en los próximos años representará grandes inversiones para las empresas dedicadas a la creación de dispositivos de domótica e infraestructura de conexión a internet por medio de conexiones inalámbricas.

2. El internet de las cosas está compuesto por todos los dispositivos que capturan datos del entorno, los procesan y que envían información a través de una conexión a internet, donde subyace el conjunto de tecnologías encargadas del análisis de la información que se recibe de estos dispositivos. Existen varias plataformas que permiten a las cosas comunicarse entre sí, y en los próximos años aparecerán nuevas y mejores opciones. Las aplicaciones para el hogar de los dispositivos de domótica y el internet de las cosas son muy diversas y su establecimiento en permitirá mejorar la calidad de vida de las personas.

3. Los principales problemas que presenta el internet de las cosas están relacionados con la manera de identificar a los dispositivos de manera única a nivel global, los métodos y mecanismos para transmitir la información capturada y generada por los dispositivos, y la estandarización de los protocolos de comunicación por medio de los que se enviará la información. Afortunadamente estos problemas se han identificado aún cuando el internet de las cosas está en su etapa inicial,

en los próximos años las empresas con mayores recursos económicos y de investigación apostarán por brindar la mejor experiencia a los usuarios. En materia de privacidad y seguridad aún es necesaria la creación de organismos internacionales que se encarguen de la regulación de lo que un proveedor de servicios puede o no hacer con la información de los usuarios.

RECOMENDACIONES

1. Es importante que, como país se tome parte en el movimiento tecnológico que representa el internet de las cosas. Es el momento justo para que las entidades de gobierno e iniciativa privada creen un clima de estabilidad e inversión para las empresas, tanto nacionales como extranjeras, que quieran desarrollarse en este ámbito.

2. El cambio siempre es bueno, pero existen riesgos asociados a la implementación de nuevas tecnologías. La privacidad y seguridad de la información que se comparte y se compartirá en el internet de las cosas pertenece enteramente a los usuarios finales y es responsabilidad de cada persona evaluar las ventajas y desventajas que supone compartir esta información.

3. Si bien el tema del internet de las cosas es nuevo a nivel internacional, como país se debe establecer una ruta que permita el crecimiento de este tipo de cambios tecnológicos. Actualmente en Guatemala no existen regulaciones sobre muchos temas de informática e infraestructura de telecomunicaciones, por lo que es necesario que los distintos sectores presenten iniciativas de ley que permitan crear un entorno estable para los cambios en el futuro. La privacidad y la seguridad de la información digital son temas que en el país no son abordados, pero representan muchos intereses para los distintos sectores.

BIBLIOGRAFÍA

1. BANDYOPADHYAY, Debasis; SEN, Jaydip. Internet of Things: Applications and Challenges in Technology Standardization. *Wireless Personal Communications.* 2011, volumen 58, número 1.

2. BELLINGER, Gene; CASTRO, Durval; MILLS, Anthony. *Data, Information, Knowledge, and Wisdom.* [en línea]. <http://www.systems-thinking.org/dikw/dikw.htm>. [Consulta: abril de 2015].

3. CHAOUCHI, Hakima. *The Internet of Things: Connecting Objects to the Web.* Londres, Inglaterra: ISTE, 2010. 265 p. ISBN 978-1-84821-140-7.

4. HERSENT, Oliver; BOSWARTHICK, David; ELLOUMI, Omar. *The Internet of Things: Key Applications and Protocols.* 2a ed. Chichester, Inglaterra: Wiley, 2011. ISBN 978-1-119-96670-8. 448 p.

5. HOEPMAN, Jaap-Henk. In Things We Trust? Towards trustability in the Internet of Things. *Communications in Computer and Information Science.* 2012, volumen 277.

6. LEINER, Barry; et al. *Breve historia de internet.* [en línea]. <http://www.internetsociety.org/es/breve-historia-de-internet>. [Consulta: marzo de 2015].

7. MCEWEN, Adrian; CASSIMALLY, Hakim. *Designing the Internet of Things.* Chichester, Inglaterra: Wiley, 2014. ISBN 978-1-118-43063-7. 324 p.

8. MOORHEAD, Patrick. *The Problem With Home Automation's Internet of Things (IoT).* [en línea]. <http://www.forbes.com/sites/patrickmoorhead/2013/09/26/the-problem-with-home-automations-iot/>. [Consulta: marzo de 2015].

9. PRADA, Enio. *Los insumos invisibles de decisión: datos, información y conocimiento. Anales de documentación.* Madrid, España: 2008, número 11.

10. PFISTER, Cuno. *Getting started with the Internet of things.* California, EE.UU.: O'Reilly, 2011. ISBN 978-1-449-39357-1. 176 p.

11. RENDLE, Adam. *Who owns the data in the Internet of Things?.* [en línea]. <http://www.taylorwessing.com/download/article_data_lot.html>. [Consulta: marzo de 2015].

12. RUBENKING, Neil. *The Best Security Suites for 2015.* [en línea]. <http://www.pcmag.com/article2/0,2817,2369749,00.asp>. [Consulta: mayo de 2015].

13. TAYLOR, Louise. *Privacy by design – essential for the growth of the Internet of Things?.* [en línea]. <http://www.taylorwessing.com/download/article_privacy_design.html>. [Consulta: marzo de 2015].

14. UCKELMANN, Dieter; HARRISON, Mark; MICHAHELLES, Florian. *Architecting the Internet of Things*. Berlín, Alemania: Springer-Verlag, 2011. ISBN 978-3-642-19157-2. 353 p.

15. UNESCO. *Declaración Universal de Derechos Humanos.* Santiago, Chile: Oficina Regional de Educación para América Latina y el Caribe, 2008. ISBN 978-956-322-002-5.

16. VERMESAN, Ovidiu; FRIESS, Peter. *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems.* Aalborg, Dinamarca: River Publishers, 2013. ISBN 978-87-92982-96-4. 348 p.

17. VIRKKI, Johanna; CHEN, Liquan. Personal perspectives: individual privacy in the IOT". *Advances in The Internet of Things.* 2013, número 3.

18. WEBER, Rolf; WEBER, Romana. *Internet of Things: Legal Perspectives.* Berlín, Alemania: Springer-Verlag, 2010. ISBN 978-3-642-11710-7. 135 p.