

Universidad Tecnológica de El Salvador

FACULTAD DE INFORMÁTICA Y CIENCIAS APLICADAS
CARRERA TECNICO EN INGENIERIA DE HARDWARE



TEMA:

**IMPLEMENTAR UN SISTEMA DE ILUMINACION, APLICANDO EL
INTERNET DE LAS COSAS PARA EL AHORRO DE ENERGIA, PARA EL
LABORATORIO DE REDES DE LA UNIVERSIDAD TECNOLÓGICA DE EL
SALVADOR.**

TRABAJO DE GRADUACIÓN PRESENTADO POR:

SAMUELSON GALILEO BARILLAS SOSA

ERIKA JOHANA ESPINO GALDAMEZ

DAVID ADALBERTO RIVERA GUERRA

PARA OPTAR AL GRADO DE:

TECNICO EN INGENIERIA DE HARDWARE

SEPTIEMBRE, 2018

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

AUTORIDADES ACADEMICAS

ING. NELSON ZARATE SANCHEZ

RECTOR

LIC. JOSE MODESTO VENTURA

VICERRECTOR ACADEMICO

ING. FRANCISCO ARMANDO ZEPEDA

DECANO

JURADO EXAMINADOR

ING. EVELIN YAMILETH SARA VIA ARCE

PRESIDENTE

LIC. LUIS RODRIGO PALOMO QUIÑONES

PRIMER VOCAL

ING. HUGO ORTIZ SALDAÑA

SEGUNDO VOCAL

SEPTIEMBRE, 2018

SAN SALVADOR, EL SALVADOR, CENTROAMERICA

ACTA DE EXAMEN PROFESIONAL

HABIÉNDOSE REUNIDO EL JURADO CALIFICADOR INTEGRADO POR:
Lic. Luis Rodrigo Palomo Quiñonez, Ing. Hugo Joel Ortiz Saldaña, Ing. Evelin Yamileth Saravia Arce, a las 12:30m. del día Jueves, 21 Junio de dos mil dieciocho.
Y LUEGO DE HABER DELIBERADO SOBRE EL EXAMEN PROFESIONAL DE LOS ALUMNOS:

- | | |
|---|----------------------------|
| 1- <u>Erika Johana Espino Galdámez</u> | <u>Carnet 28-2460-2011</u> |
| 2- <u>David Adalberto Rivera Guerra</u> | <u>Carnet 28-6933-2014</u> |
| 3- <u>Samuelson Galileo Barillas Sosa</u> | <u>Carnet 28-6289-2015</u> |

QUIENES PRESENTARON DEFENSA DE SU TRABAJO DE GRADUACION TITULADO:
"Implementar un sistema de iluminación, aplicando el Internet de las cosas para el ahorro de energía, para el laboratorio de Redes de la Universidad Tecnológica de El Salvador"

PARA OPTAR AL GRADO DE:

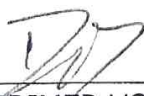
TÉCNICO EN INGENIERIA DE HARDWARE

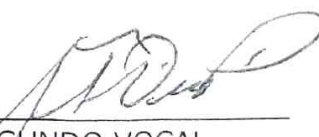
Y DEL CUAL TAMBIEN EVALUARON LOS CONOCIMIENTOS RELACIONADOS CON EL TEMA DEL MISMO. POR LO QUE ESTE JURADO RESUELVE DECLARAR EL EXAMEN COMO:

Aprobado

YA QUE CUMPLE CON LOS REQUISITOS ESTABLECIDOS EN EL REGLAMENTO DE GRADUACION DE LA UNIVERSIDAD.

San Salvador, 21 Junio de dos mil dieciocho.

F. 
PRIMER VOCAL
Lic. Luis Rodrigo Palomo Quiñonez

F. 
SEGUNDO VOCAL
Ing. Hugo Joel Ortiz Saldaña

F. 
PRESIDENTE
Ing. Evelin Yamileth Saravia Arce

INDICE

No. De Página

Introducción.....	i
Capítulo I	1
Planteamiento del Problema	1
1.Antecedentes.....	1
2.Planteamiento Problema	2
3.Objetivos	2
4.Justificación	3
5. Limitaciones	4
6.Alcances	4
Capitulo II	5
Marco Teórico	5
1.Internet.....	5
2.Historia de Internet	5
2.1 Internet de las cosas	7
2.2 Internet de las cosas	7
2.3 Construcción de un proyecto de IOT.....	8
2.4 Ventajas y contras de IOT.....	10
2.5 La seguridad en el internet de las cosas	11
2.6 Impacto del internet de las cosas.....	11
Capitulo III	13
Metodología.....	13
1.Descripción General de la Metodología	13
2.Justificación de la Elección en la Metodología.....	14
3.Método	15
3.1 Instrumentos.....	15
3.2 Procedimientos	16
3.3 Participantes.....	16

3.4 Estrategia de análisis de datos.....	17
Capítulo IV.....	19
Análisis de Resultados.....	19
1.Propuesta de Solución	20
2.Instalación del Sistema de la Luminaria.....	21
3. Manual de Instalación y Configuración del Sistema de Control	23
4.Aplicación Web para Controlar el Sistema de Luminaria.....	25
Capitulo IV.....	28
Conclusiones y Recomendaciones.....	28
1.Conclusión	28
2.Recomendaciones	30
Referencias.....	31
ANEXOS.....	33

Introducción

La investigación que se desarrollará busca el beneficio de los estudiantes y encargados de laboratorio de redes de la universidad tecnológica de el salvador, tomando en cuenta que la tecnología día con día la tenemos en constante cambio, es por ello que se tiene la facilidad de ver qué se necesita actualizar el sistema que controla la iluminación.

Es por ello que instalaremos un sistema que permitirá encender y Apagar la iluminación vía Wi Fi que también se podrá tener acceso remoto a través de la red 3g y 4 g.

Contará como acceso a través de la web o aplicación que permitirá notificar al encargado saber si la luminaria está encendida, en horas no hábiles con esto si pretendemos disminuir el consumo excesivo de energía eléctrica, a

Causa de un mal uso o un olvido o cualquier otro percance.

Se dejara material para los alumnos de la Carrera Técnico en Ingeniería de Hardware o carrera a fines de la Universidad Tecnológica De El Salvador, para que tengan un acceso a este tipo de información y tengan suficiente material para poder desarrollar proyectos relacionados con este tema.

Capítulo I

Planteamiento del Problema

1. Antecedentes

En estos últimos años, la iluminación del Laboratorio de Redes de la Universidad Tecnológica De El Salvador paso de ser de ser tradicional a incandescente.

Tipo de iluminación tradicional, esta lleva más consumo de energía eléctrica, cuando esta no se está siendo utilizada adecuadamente no se tiene un control sobre el consumo actual.

De esta manera tenemos una reducción considerable de energía eléctrica en el laboratorio de redes de la Universidad Tecnológica de El Salvador. Donde el primer cambio que se realizó fue pasar de tubos incandescentes a tubos LED donde el consumo mejoro notablemente de pasar de 4 tubos incandescentes a 2 tubos LED siempre manteniendo las mismas iluminaciones.

Actualmente se ha demostrado que el cambio que se realizó redujo notablemente el Consumo de energía, pero no cumplió con las expectativas que se habían planteado, desde el punto de vista económico.

Una problemática que hay en estos tipos de temas, es que no están incluidos en el pensum de la carrera de Técnico en Ingeniería De Hardware de la Universidad Tecnológica de El Salvador.

2.Planteamiento Problema

¿Se implementara un sistema domótica de iluminación inteligente en el laboratorio de redes de la Universidad Tecnológica De El Salvador?

3.Objetivos

Objetivo General

- Implementar un sistema de iluminación, aplicando el internet de las cosas en el laboratorio de redes de la Universidad Tecnológica de El Salvador

Objetivo Específicos

- Investigar y describir los componentes que conforman el internet de las cosas.
- Implementar un sistema de iluminación inteligente, utilizando el internet de la cosas.
- Elaborar una manual para describir los pasos de cómo implementar un sistema de iluminación inteligente

4. Justificación

La siguiente investigación consiste en la implementación de el internet de las cosas en las luminarias del laboratorio de redes de la Universidad Tecnológica de El Salvador, que podrá permitir tener el acceso dentro y fuera del campus de la Uiversidad a través de una conexión wi-fi, 3g o 4G que esta permitirá el encendido y apagado cada sección de las lamparas que se esté controlado a través de los switch inteligentes que se instalaran dándole así una solución al problema.

Se podrá tener acceso remoto dentro y fuera del campus Universitario a través de una aplicación movil que esta notificara a los encargados del Laboratorio de Redes, ya que si la luminaria aún sigue encendida de esta manera podrán ellos a pagar los switch desde cualquier dispositivo móvil, o si las luminarias estan apagadas podran encenderlas atraves de esta aplicación ,también podrán hacer un horario de encendido y apagado de laboratorio de redes de la universidad tecnologica de el salvador.

Se evitara que las luminarias del laboratorio de redes de la Universidad Tecnologica de El Salvador queden encendidas .

El proyecto puede ser un aporte tanto para estudiantes asi tambien como a los mismo docentes de la Universidad Tecnologica de El Salvador.

5. Limitaciones

Temporal

La investigación comienza del mes de febrero a mayo del 2018 y finalizara el mes de mayo de 2018

Espacial

Laboratorio de redes de la Universidad Tecnológica De El Salvador.

6. Alcances

Promesa	Entregable
Investigar y describir los componentes que conforman el internet de las cosas	Documento informativo sobre el internet de las cosas
Implementar un sistema de iluminación inteligente, utilizando el internet de la cosas.	Un sistema de iluminación controlada via internet

Capítulo II

Marco Teórico

1. Internet

Internet es la unión de todas las redes y computadoras distribuidas por todo el mundo por lo que se puede definir como una red global.

2. Historia de Internet

Internet se inició en los Estados Unidos. A finales de los años 60, la ARPA (Agencia de Proyectos de Investigación Avanzados) del Departamento de Defensa definió el protocolo TCP/IP con intención de facilitar la conexión de diversos tipos de ordenadores, principalmente para temas de investigación. Ahora el TCP/IP sirve para garantizar la transmisión de los paquetes de información entre lugares remotos, siguiendo cualquier ruta disponible

En 1975, ARPAnet comenzó a funcionar como red, sirviendo como base para unir centros de investigación militares y universidades, y se trabajó en desarrollar protocolos más avanzados para diferentes tipos de ordenadores y cuestiones específicas.

En 1983 se adoptó el TCP/IP como estándar principal para todas las comunicaciones, y en 1990 desapareció ARPAnet para dar paso junto a otras

redes TCP/IP a Internet. Por aquel entonces también comenzaron a operar organizaciones privadas en la Red.

Poco a poco, todos los fabricantes de ordenadores personales y redes incorporaron el TCP/IP en sus sistemas operativos, de modo que en la actualidad cualquier equipo está listo para conectarse a Internet.

Internet une muchas redes, incluyendo como más importantes la que proporciona acceso a los grupos de noticias (Usenet), que data de 1979 y (conceptualmente) la todavía más conocida World Wide Web, desde principios de los 90.

En España, Internet comenzó a implantarse a finales de los 80, a través del programa IRIS. En 1990 nació como tal RedIRIS, entidad que obtuvo la condición de red oficial de cara a los estándares internacionales de Internet, y que fue adoptando poco a poco cada uno de los servicios existentes.

En 1991 surgió Goya, el primer proveedor de acceso privado a Internet, y entre 1992 y 1994 se produjo su implantación de Internet en la mayor parte de las universidades y la llegada de más servicios globales y proveedores de acceso. 1995 fue el año definitivo para la popularización de Internet en España, el «boom» de los proveedores de Internet.

2.1 Internet de las cosas

Es un concepto que se refiere a la interconexión digital de objetos cotidianos con Internet. Alternativamente, Internet de las cosas es la conexión de Internet con más “cosas u objetos” que personas.

2.2 Internet de las cosas

El internet de las cosas se refiere a que en un futuro todos los objetos que se encuentran a nuestro alrededor tendrán la capacidad de conectarse a la red, siendo capaces de recoger información, procesarla y compartirla.

Este internet de las cosas ofrecerá todo un mundo lleno de posibilidades ya que habrá más cosas en internet que personas usando internet.

Diariamente crece el número de objetos y dispositivos que usan internet, lo que contribuye a la construcción de un planeta más inteligente.

Actualmente se tiene una cierta cantidad de objetos interconectados en red como los pequeños sensores que miden la temperatura, el tráfico, el caudal del agua, la electricidad o la cantidad de información transmitida entre otros pero se prevé que para el 2020 habrá 50.000 millones de objetos conectados a internet y un promedio de 6 dispositivos por cada habitante del planeta.

Ventajas y desventajas internet de las cosas al igual que dentro de cualquier proyecto, hay que tener muy en cuenta también la seguridad. Pero sin duda esto marcará el desarrollo de la tecnología de comunicación e internet para la humanidad.

Es algo que ya se viene dando desde hace pocos años, comenzando por que la gente en su mayoría actualmente posee un Smartphone o simplemente tiene acceso a internet, esto ya es un gran progreso.

No faltará mucho para que todas las personas del planeta cuenten con una conexión a internet y de esta manera todos estemos intercomunicados, luego de esto sin que pase mucho tiempo los objetos en su totalidad también lo estarán, llegando así ambos vivir en la nueva y fantástica era del internet de las cosas.

2.3 Construcción de un proyecto de IOT

Para la construcción de un proyecto de IoT se hablará de 4 cosas: dispositivos, plataforma, frontend e integración; siendo estos los parámetros más importantes para realizar esta construcción.

Dentro los dispositivos se encuentran los sensores, actuadores, la conectividad y el protocolo de comunicación.

Estos sensores adquieren dicha información que es leída por un dispositivo, los sensores pueden leer una gran cantidad de variables como por ejemplo cantidad de fluidos, temperatura, distancia, etc.

Los actuadores también forman parte de estos dispositivos ya que se encargan de permitir la interacción con el mundo físico. Esto puede ser por ejemplo: abrir ventanas, cerrar puertas, encender y apagar luces.

La conectividad hace referencia a que para este tipo de proyectos los objetos deben contar con una conexión a internet para que puedan interactuar.

El protocolo de comunicación quiere decir que los dispositivos interactúan con un protocolo estándar.

El API Rest se encarga de 2 cosas: recibir grandes cantidades de datos de los dispositivos y también se encarga de interactuar con todas las entidades para formar paneles de control personalizados e informes. Un ejemplo de esto sería un sensor de parqueo que envía el estado del mismo si es que se encuentra libre o está ocupado, luego un panel de control usa la api rest para gestionar dispositivos.

El almacenamiento big data quiere decir que grandes cantidades de datos son almacenados en una arquitectura de big data, proporcionan maleabilidad a los proyectos de IOT para gestionar datos híbridos de distintos dispositivos. Un ejemplo de esto es la posición geográfica.

La gestión de dispositivos y proyectos menciona que para cubrir algún requisito de un proyecto propone una clasificación lista para usar y flexible para la complejidad de cada caso. Contiene la configuración remota de dispositivos.

La lógica de negocio y eventos se aloja y ejecuta en la plataforma. La seguridad hace mención de que en todo proyecto está debe formar parte del diseño.

Integración para que se proporcione un potencial de la conectividad a Internet es que la plataforma se integra con ciertos sistemas de información haciendo push/pull desde o hacia CMRs o cualquier API HTTP disponible.

2.4 Ventajas y contras de IOT

Se pueden mencionar muchas ventajas en lo que sería la implementación del internet de las cosas de manera masiva, una de las ventajas es que será algo cómodo ya se podrá manejar nuestros objetos desde cualquier lugar y desde un dispositivo móvil o a través de la red. Esto supone en sí algo eficiente, pero también se tiene que pensar en las desventajas que este “beneficio” traerá consigo. Uno de los contras sería la incógnita o el no saber si

existirá un sistema tecnológico o infraestructura que soporte esta avalancha, ya que serán miles de millones de objetos interactuando con miles de millones de personas en todo el planeta.

2.5 La seguridad en el internet de las cosas

Algo importante que hay que mencionar dentro del internet de las cosas y dentro de todo proyecto es la seguridad, en este caso la seguridad de datos.

Se tendra que pensar que debido a que millones de objetos estarán conectados a la red esto podría significar un alto nivel de inseguridad de dichos la información de dichos objetos.

Hay que tener en cuenta sobretodo 5 aspectos para la seguridad: los caminos pueden no ser directos, pero sí efectivos; la amenaza de las botnets; tener cuidado con las “puertas abiertas”; la cultura de las “mejores prácticas” y la información personal, el objetivo.

2.6 Impacto del internet de las cosas

Actualmente ha generado un gran impacto sobre todo en la población más joven ya que son los que tienen más acceso a ella y son quienes verán como irá evolucionando este proyecto día a día. Las personas creen que esto

será de gran beneficio en distintos aspectos, lo primero será para formar ciudades inteligentes. (Caceres, Eliana, 2014).

Capítulo III

Metodología

1.Descripción General de la Metodología

En la metodología de la investigación de campo, se refiere al análisis y comprensión de una realidad que se plantean problemas en una zona específica, por lo cual es necesario el uso de instrumento de recopilación de datos para obtener resultado concluyente de la información en dicha zona que está siendo analizada, por lo cual se hace una selección de participantes relacionando al tema.

El principal problema de esta investigación es que muchas veces las luminarias que tiene laboratorio de redes de la Universidad Tecnológica de El Salvador quedan encendidas por largos periodos de tiempo, esto sucede al no tener un control sobre el encendido y apagado de sus luces después de horas de clase.

En otro punto es la proyección que se tendra una herramienta para los encargados de laboratorio de redes de la Universidad Tecnológica de El Salvador la cual de manera instantánea mejora el uso de las luminarias teniendo acceso a ellas remotamente .

2. Justificación de la Elección en la Metodología

Para la selección del método, se optó por la investigación de campo que se aplicará en el lugar que está ubicado en el Laboratorio de redes de la Universidad Tecnológica de El Salvador.

Se colectara datos e información directamente de las personas a través del uso de instrumentos (como entrevistas o encuestas) con el fin de analizar la situación y lograr los objetivos de la investigación resolviendo los problemas planteados (deficinico.mx, 2017)

En esta metodología tiene como propósito mejorar las opciones de ahorro energía que existen en la actualidad Mediante los sistemas inteligentes de apagados y encendidos de luminarias a través de la internet y así exponer las ventajas qué se obtiene al utilizar esta herramienta las cuales son:

- un sistema virtual automatizado de encendido y apagado.
- facil acceso atraves de aplicación móvil.
- control remoto atraves de conexión wifi e internet.
- Se procederá a evaluar la entrevista realizada para así solventar ahorro de energia.

3.Método

El problema y planteamiento de la investigación en implementar un sistema de iluminación aplicando el internet de las cosas para el ahorro de energía para el laboratorio de redes de la Universidad Tecnológica de El Salvador

Así dando una respuesta para la problemática de la investigación, Donde se utilizarán materiales para evitar hacer mal uso de las luminarias dentro de laboratorio de redes de la universidad tecnológica del Salvador.

3.1 Instrumentos

La entrevista es un instrumento de observación formada de una serie de preguntas formuladas, cuyas respuestas son anotadas por entrevistador, son de corta duración y eventualmente la puede contestar de manera directa a la persona entrevistada.

En esta investigación se utilizara la entrevista que se realizara a los catedráticos y encargados del laboratorio de redes para tener más información sobre el manejo de las luminarias, en el laboratorio de redes de la Universidad Tecnológica de El Salvador de esa manera se hizo un análisis de las necesidades que existen en la investigación.

3.2 Procedimientos

Se realiza una entrevista de manera presencial donde los catedráticos y encargados contestarán una serie de preguntas sobre el uso y el manejo de las luminarias en el laboratorio de redes de la Universidad Tecnológica del Salvador teniendo así las respuestas obtenidas en la entrevista que se realiza de forma presencial.

- Selección de tema.
- Selección de personal a entrevistar.
- Selección de preguntas.
- Pasar entrevista.
- Selección de datos arrojados por la entrevista.
- Tabulación de datos.
- Realización de gráficas y tabulación mediante los resultados obtenidos.

3.3 Participantes

Los participantes son los encargados del laboratorio redes de la Universidad Tecnológica de El Salvador y los catedráticos que imparten materias tecnológicas dentro del laboratorio, ya que ellos cumplen con las características especiales para ser seleccionados actualmente en el laboratorio de redes se encuentra en funcionamiento donde se trabajan con programas

para hacer cableados estructurados y en actualidad cuentan con ciertas dificultades ya mencionadas.

Mostrar las dificultades en el consumo excesivo de energía eléctrica por el olvido que tienen los encargados se procede al ensamblaje de un prototipo funcional creado con arduino qué será donado específicamente al laboratorio de redes para que en futuras generaciones puedo implementar este sistema en toda la Universidad Tecnológica de El Salvador.

De esta manera se le ofrece a los encargados una manera más fácil ver más fácil de tener acceso remoto a las luminarias ya que actualmente no existe ningún dispositivo o herramienta para poder tener acceso a los interruptores que se encuentran ubicados en el laboratorio de redes de la Universidad Tecnológica de El Salvador.

3.4 Estrategia de análisis de datos

En este caso se utiliza el análisis de datos cuantitativos debido a que empleamos la herramienta de encuesta y entrevista esto le da el sentido lógico al procesamiento de datos según este caso

Se muestra los resultados en Tablas o gráficas donde muestra la deficiencia de lo que las personas entrevistadas y encuestadas contestaron luego se calcula la diferencia por medio de porcentajes como este caso por medio de formularios de Google Drive

La interpretación de resultados obtenidos es un punto importante del análisis y de esta forma mostrar una Clara comprensión de las deducciones obtenidas en las entrevistas y encuestas (mayorga, 2018)

Capítulo IV

Análisis de Resultados

Para plantear el resultado que proporcione la investigación la cual está basada en método prueba y error o conocido como experimental “es la única que intenta influir en una variable y establecer relaciones de tipo causa-efecto entre las variables” (Perada, 2013).

Es decir, se implementara un prototipo el cual será el encargado de controlar las luminarias del laboratorio de redes de la Universidad Tecnológica de El Salvador reduciendo los costes de facturación de energía eléctrica.

Esta será la forma por la cual se evidenciara que con este sistema de control de luminaria el problema que se estaba generando ya no seguirá, más bien se verá un cambio ya que al tener un mejor control y acceso en el apagado y encendido de luces de dicho laboratorio el problema que se generaba ya no ocurrirá mas.

Adicional se apoyara del modelo instrucciones “es un proceso sistemático, planificado y estructurado donde se produce una variedad de materiales educativos atemperados a las necesidades de los educandos, asegurándose así la calidad del aprendizaje” (Yukavetsky, 2008).

Enfocados en el modelo ADDIE. Es un proceso de diseño Instruccional interactivo, en donde los resultados de la evaluación formativa de cada fase pueden conducir al diseñador instruccional de regreso a cualquiera de las fases previas. El producto final de una fase es el producto de inicio de la siguiente fase.

1.Propuesta de Solución

- Análisis: El paso inicial es analizar el alumnado, el contenido y el entorno cuyo resultado será la descripción de una situación y sus necesidades formativas.
- Diseño: Se desarrolla un programa del curso deteniéndose especialmente en el enfoque pedagógico y en el modo de secuenciar y organizar el contenido.
- Desarrollo. La creación real (producción) de los contenidos y materiales de aprendizaje basados en la fase de diseño.
- Implementación. Ejecución y puesta en práctica de la acción formativa con la participación de los alumnos.
- Evaluación. Esta fase consiste en llevar a cabo la evaluación formativa de cada una de las etapas del proceso ADDIE y la evaluación sumativa a través de pruebas específicas para analizar los resultados de la acción formativa. (Entornos Virtuales de Formación, 2013).

Modelo instruccional ADDIE.

2.Instalación del Sistema de la Luminaria

Consta de poder administrar de mejor manera la luminaria del laboratorio de redes de la Universidad Tecnológica de El Salvador

Siendo así un proyecto muy ambicioso qué trata la manera de dejar un mejor consumo de energía eléctrica en este momento en el laboratorio de redes de la universidad tecnológica del salvador y a futuro en todos los salones y edificios que componen la Universidad Tecnológica de El Salvador.

➤ Diseño:

Este prototipo se ejecuta de manera física y virtual el orden de las configuraciones puede ir desde la más sencilla hasta la más compleja para lograr el mejor resultado a la hora de su funcionamiento e instalación

En su manera física los componentes se han comprado debidamente certificados y se han hecho un cálculo de carga eléctrica que hay en el laboratorio de redes de la Universidad Tecnológica del Salvador para poder ensamblar y comprar los elementos que soporten la carga de Electricidad que se maneja en el laboratorio

➤ Desarrollo:

En esta fase ocuparemos los siguientes materiales

- Una placa de arduino wemos D1
- Un relay doble
- 2 switch
- 16 lámparas
- 36 tubos LED
- Fuentes de poder de 5 voltios
- Router inalámbrico
- Conexión eléctrica desde Arduino hacia luminaria

➤ Implementación:

Se llevará a cabo en el laboratorio de redes de la universidad tecnológica del Salvador. Este se conectara en el sistema de luminaria ya existente, dónde los encargados del laboratorio y alumnos que hacen uso de este, puedan hacer uso e interactuar con el prototipo donde se hará e implementara un fácil manejo dentro y fuera de las instalaciones de laboratorio de redes de la Universidad Tecnológica de El Salvador

De esta manera el proyecto ayudara a que los encargados del laboratorio puedan hacer un mejor uso del recurso eléctrico, en su primera fase que iniciará en el laboratorio de redes con este novedoso prototipo que dejaremos instalado

➤ Evaluación:

- Se verifica que el arduino encienda a la hora de hacerle la conexión haciéndole una prueba antes de entrar en funcionamiento.
- Se verifique que el arduino tenga conexión inalámbricamente vía Wifi.
- Se verifica que al el relé trabajé con los voltajes necesarios para su funcionamiento.
- Se verifica que la conexión del relé con la luminaria tenga conexión.
- Se verifica que las lámparas LED enciendan.
- Se verifica que los switch funcionen adecuadamente.

3. Manual de Instalación y Configuración del Sistema de Control

Para poder desarrollar este manual fue necesario ir capturando cada paso con imágenes, para así poder crear el manual y tener detallado cada pasó de como instalarlo.

➤ Diseño

En este manual se identifica el proceso de la utilización de los elementos, este manual estará de forma física y de forma virtual.

Contará con imágenes ilustrativas para referencias más específicas son capturadas de modelos funcionales y con una buena redacción y un lenguaje técnico comprensivo para facilitar la lectura al momento de recurrirlos.

Contará con un índice específico para facilitar al lector a encontrar cualquier información o configuración que el desee,

➤ Desarrollo

Se desarrollara en la plataforma de ofimática específicamente Microsoft Word será colocado en los anexos de la tesis

➤ Implementación:

Estará disponible para todo el público que desee informarse sobre este tema

- Biblioteca de la Universidad Tecnológica de El Salvador
- Se subirá a internet para todo publico
- Un manual especial para los encargados del laboratorio de redes de la universidad tecnológica de el salvador para que puedan guiarse para utilizar de una forma correcta estas lámparas.

➤ Evaluación

- Verificación de buena ortografía
- Imágenes con excelente resolución
- Imágenes con color adecuado
- Revisión de tipo de letra

- Revisión de tamaño de letra
- Revisión de numero de letra adecuado
- Orden de configuración y elaboración

4.Aplicación Web para Controlar el Sistema de Luminaria

Blynk es una plataforma con aplicaciones IOS y Androide para controlar Arduino, Raspberry Pi y las demás herramientas que se puedan encontrar a través de Internet.

Es un tablero digital donde puedes construir una interfaz gráfica para tu proyecto simplemente arrastrando y soltando widgets.

Es muy sencillo configurar todo y comenzarás a retocar en menos de 5 minutos.

Blynk no está atada a una tabla o escudo específico. En cambio, es compatible con el hardware de su elección. Ya sea que su Arduino o Raspberry Pi esté conectado a Internet a través de Wi-Fi, Ethernet o este nuevo chip ESP8266, Link lo pondrá en línea y listo para Internet Of Your Things.

➤ Diseño:

- Selección del mejor diseño electrónico y tradicional.
- Señalamiento de los objetivos tradicionales.
- Selección de estrategias pedagógicas.

- Bosquejo de unidades lección y módulos.

➤ Desarrollo:

Para conectar la aplicación blynk y su hardware, necesita un Auth Token.

Crea una nueva cuenta en la aplicación BLink.

- Crea un nuevo proyecto. Luego elige la placa y la conexión que usarás.
- Después de crear el proyecto, obtendremos Auth Token por correo electrónico.
- Abrimos el correo electrónico y se copia el token de autenticación.
- La biblioteca BLink se tiene que instalar manualmente.
- Descomprimir el archivo encontraremos que el archivo contiene varias carpetas y varias bibliotecas.
- Se tiene que copiar todas las bibliotecas en `your_sketchbook_folder` de Arduino IDE. Para encontrar la ubicación de `su_sketchbook_folder`
- La estructura de su carpeta `_sketchbook` ahora debe verse así:

`your_sketchbook_folder / libraries / Blynk`

`your_sketchbook_folder / libraries / BlynkESP8266_Lib`

`your_sketchbook_folder / tools / BlynkUpdater`

`your_sketchbook_folder / tools / BlynkUsbScript`

➤ Implementación:

Ejecución y puesta en práctica de la acción formativa con la participación de los alumnos y encargados del laboratorio de Hardware de la Universidad Tecnológica de El Salvador.

Capitulo IV

Conclusiones y Recomendaciones

1. Conclusión

Conforme se avanza al ritmo actual, la vida de las personas se ha transformado de una manera muy rápida en los últimos años la tecnología abarcara desde comunicaciones hasta el encendido y apagado de luces remotamente.

La utilización de controles de luminarias representa un avance en cuanto ala utilizacion de estas, se logro diseñar un control de luminaria inteligente el cual controla la iluminación del laboratorio de redes de la Universidad Tecnológica de El Salvador , a travez de la placa Arduino WEMOS DI la característica principal será que se podrá controlar las luminarias remotamente

Se creó un sistema vanguardista a partir de las necesidades que tiene el laboratorio de redes con el fin de evitar que las luminarias queden encendidas a través de este novedoso y tecnológico sistema que dejara un precedente en el sistema educativo de los estudiantes de la facultad de informática y ciencias aplicadas de la Universidad Tecnológica de El Salvador.

Todos estos factores mencionados anteriormente se pretende motivar a la Universidad Tecnológica de El Salvador para que se imparta una materia

específica a la industria 4.0, donde se ha dejado muchos temas relevantes que ya en nuestra actualidad se han vuelto necesarias, por ejemplo:

- El internet de las cosas
- Fabricación aditiva
- Big data
- Inteligencia artificial
- Robótica colaborativa
- Realidad virtual
- Realidad aumentada

El trabajo presenta un sistema de control de luminaria controlado remotamente, con un alto grado de adaptabilidad y facilidad de instalación. El sistema se aprovecha de una estrategia de control centralizada y el uso de elementos de conexión inalámbrica para lograr una mayor eficiencia en la utilización de las luminarias.

El sistema propuesto puede acomodarse a las diferentes necesidades de cada laboratorio y aulas de la Universidad Tecnológica de El Salvador asegurando la escalabilidad, la interoperabilidad y la accesibilidad (en el sentido de que el sistema es accesible desde múltiples plataformas: teléfono móvil, PC, Tablet).

2.Recomendaciones

- Capacitar a los catedráticos para estos tipos de temas vinculados a la industria 4.0 y que ellos puedan desarrollarlos sin problemas.
- Crear un laboratorio especial en la Universidad Tecnológica de El Salvador para que los alumnos del técnico en ingeniería de hardware puedan realizar sus prácticas de la industria 4.0.
- Cursos Gratuitos de la industria 4.0 para los alumnos de la Uinversidad Tecnologica De El Salvador.
- Tener las herramientas físicas adecuadas para que los alumnos puedan realizar sus practicas de la industria 4.0.
- Dotar a los estudiantes de informacion adecauda de la industria 4.0
- Que las bibliotecas de la Universidad Tecnologica DE e L Salvador cuenten con libros de la industrias 4.0.
- Que las practicas de los estudiantes sean reales y se lleven a cabo dentro o fuera de las instalciones de la Universidad Tecnologica De El Salvador
- Capacitar a los alumnos en temas tecnológicos para que puedan desenvolverse en el ámbito laboral sin problema.
- Incluir en el pensum de la carrera técnico en ingeniería en hardware los temas de la industria 4.0

Referencias

- Cáceres, E. (2014, marzo 8). *Redes biomédicas*. [Registro web]. Recuperado de <http://redesbiomedica.blogspot.com/2014/03/redes-de-datos-en-ing-biomedica-caceres.html>
- De la Huerta, J. (2001). *Circuitos combinacionales*. Recuperado de <https://Prezi.com/ur6cvq59wgnd/circuitos-combinacionales-lsi-ymsi/>
- How, K. (2016). *Sistemas operativos para servidores a través del tiempo*. Recuperado de <https://www.1and1.es/digitalguie/servidores/know-how/los-sistemas-operativos-para-servidores-a-traves-del-tiempo/>
- Julian, J. (2008). *Definicion de software*. Recuperado de <https://definicionde.software/>
- Mendez, B. (2015). *Metodos de investigacion experimental*. Recuperado de https://prezi.com/f1is_ebxysgs/metodos-de-investigacion-experimental/
- Merinp, P. (2008). *Definicion de Hardare*. Recuperado de <https://definicionde/hardware/>
- Molina, A. (2009). *Interface en Linux*. Recuperado de <https://albertomolina.files.wordpress.com/2009/10/virtualizacion.pdf>
- Ojeda, F. (2013). *Windows Server 2012*. Recuperado de <https://www.casadellibro.com/libro-windows-server-2012-manual-avanzado/9788441533202/2071914>
- Perada, G. (2013). *Investigacion experimental*. Recuperado de <https://prezi.com/>

Com/5wha4nm_rj/caracteristicas-de-la-investigacion-experimental

Peralta, J. (2013). *Historia y evolucion de sistemas operativos*. Recuperado de <https://prezi.com/f3d5ctt8ns9/todo-empezando-en-la-decada-de-los-40-historia-y-evolucion-de/>

Perez, F. (2015). *Lenguaje de programacion fortran*. Recuperado de <http://www.larevistainformatica.com/FORTRAN.htm>

Real Academia Española. (2018). *Internet*. Recuperado de <http://dle.rae.es/?id=LvskgUG>

Red, H. (2018). *Concepto de virtualizacion*. Recuperado de <https://www.RedhAt.com/es/topic/virtualizacion#>

ANEXOS

Para entender mejor los
problemas y desafíos de un
mundo más conectado

Para entender mejor los
problemas y desafíos de un
mundo más conectado



LA INTERNET DE LAS COSAS— UNA BREVE RESEÑA

Para entender mejor los problemas y desafíos de un mundo más conectado

RESUMEN EJECUTIVO



La Internet de las cosas es un tema emergente de importancia técnica, social y económica. En este momento se están combinando productos de consumo, bienes duraderos, automóviles y camiones, componentes industriales y de servicios públicos, sensores y otros objetos de uso cotidiano con conectividad a Internet y potentes capacidades de análisis de datos que prometen transformar el modo en que trabajamos, vivimos y jugamos. Las proyecciones del impacto de la IoT sobre Internet y la economía son impresionantes: hay quienes anticipan que en el año 2025 habrá hasta cien mil millones de dispositivos conectados a la IoT y que su impacto será de US\$ 11.000.000.000.000.

Sin embargo, la Internet de las Cosas también plantea importantes desafíos que podrían dificultar la realización de sus potenciales beneficios. Noticias sobre ataques a dispositivos conectados a Internet, el temor a la vigilancia y las preocupaciones relacionadas con la privacidad ya han captado la atención del público. Los desafíos técnicos siguen allí, pero además están surgiendo nuevos desafíos de políticas, jurídicos y de desarrollo.

Este documento informativo está diseñado para ayudar a la comunidad de la Internet Society a navegar los diálogos que rodean a la Internet de las Cosas a la luz de las predicciones contradictorias sobre sus promesas y los peligros que implica. La Internet de las Cosas plantea un amplio conjunto de ideas complejas y que se entrelazan desde diferentes perspectivas.

Los conceptos clave que sirven como base para explorar las oportunidades y desafíos de la IoT incluyen:

DEFINICIONES DE LA INTERNET DE LAS COSAS

Por lo general, el término Internet de las Cosas se refiere a escenarios en los que la conectividad de red y la capacidad de cómputo se extienden a objetos, sensores y artículos de uso diario que habitualmente no se consideran computadoras, permitiendo que estos dispositivos generen, intercambien y consuman datos con una mínima intervención humana. Sin embargo, no existe ninguna definición única y universal.

TECNOLOGÍAS INSTRUMENTALES

El concepto de combinar computadoras, sensores y redes para monitorear y controlar diferentes dispositivos ha existido durante décadas. Sin embargo, la reciente confluencia de diferentes tendencias del mercado tecnológico está permitiendo que la Internet de las Cosas esté cada vez más cerca de ser una realidad generalizada. Estas tendencias incluyen la conectividad omnipresente, la adopción generalizada de redes basadas en el protocolo IP, la economía en la capacidad de cómputo, la miniaturización, los avances en el análisis de datos y el surgimiento de la computación en la nube.

MODELOS DE CONECTIVIDAD

Las implementaciones de la IoT utilizan diferentes modelos de conectividad, cada uno de los cuales tiene sus propias características. Los cuatro de los modelos de conectividad descritos por la Junta de Arquitectura de Internet incluyen: *Device-to-Device* (dispositivo a dispositivo), *Device-to-Cloud* (dispositivo a la nube), *Device-to-Gateway* (dispositivo a puerta de enlace) y *Back-End Data-Sharing* (intercambio de datos a través del *back-end*). Estos modelos destacan la flexibilidad en las formas en que los dispositivos de la IoT pueden conectarse y proporcionar un valor para el usuario.

POTENCIAL DE TRANSFORMACIÓN

Si las tendencias y proyecciones sobre el desarrollo de la IoT se convierten en realidad, esto podría obligar un cambio de mentalidad con respecto a las implicancias y problemas en un mundo donde la interacción más frecuente con Internet provendrá de la interacción pasiva con objetos conectados y no de una interacción activa con el contenido. La potencial realización de este resultado —un “mundo hiperconectado”— es una prueba de la naturaleza de propósito general de la propia arquitectura de Internet, que no impone limitaciones inherentes a las aplicaciones o servicios que pueden hacer uso de la tecnología.

Se analizan cinco áreas temáticas clave de la IoT para explorar algunos de los desafíos y cuestiones relacionadas con la tecnología más urgentes. Estos incluyen la seguridad; la privacidad; la interoperabilidad y los estándares; cuestiones legales, reglamentarias y relacionadas con los derechos; y economías emergentes y cuestiones relacionadas con el desarrollo.

SEGURIDAD

Si bien en el contexto de la tecnología de la información las consideraciones de seguridad no son nuevas, los atributos de muchas implementaciones de la IoT presentan desafíos de seguridad nuevos y únicos. Hacer frente a estos desafíos y garantizar la seguridad en los productos y servicios de la IoT debe ser una prioridad fundamental. Los usuarios deben poder confiar en que los dispositivos de la IoT y los servicios de datos relacionados serán seguros y estarán libres de vulnerabilidades, especialmente a medida que esta tecnología sea más difundida y se integre a nuestra vida diaria. Los dispositivos y servicios de la IoT poco seguros pueden servir como potenciales puntos de entrada de ataques cibernéticos y exponer los datos de los usuarios al robo al dejar flujos de datos con una protección inadecuada.

La naturaleza interconectada de los dispositivos de la IoT significa que cada dispositivo mal

asegurado conectado a Internet podría afectar la seguridad y la resistencia de Internet a nivel global. Este desafío se ve amplificado por otras consideraciones, como el despliegue a gran escala de dispositivos homogéneos, la capacidad de algunos dispositivos de conectarse automáticamente a otros y la posibilidad de que estos dispositivos sean desplegados en entornos no seguros.

Por principio, los desarrolladores y usuarios de dispositivos y sistemas de la IoT tienen la obligación colectiva de asegurar que no estén exponiendo a los usuarios y la propia Internet a daños potenciales. Por lo tanto, se necesitará un enfoque colaborativo para desarrollar soluciones eficaces y adecuadas ante los desafíos de seguridad de la IoT, soluciones que se adapten bien a la escala y complejidad de los problemas.

PRIVACIDAD

El potencial de la Internet de las Cosas depende de estrategias que respeten las opciones de privacidad individuales correspondientes a un amplio espectro de expectativas. Los flujos de datos y la especificidad que permiten los dispositivos de la IoT puede liberar un valor único e increíble para los usuarios, pero las preocupaciones con respecto a la privacidad y los potenciales daños podrían dificultar la adopción plena de la Internet de las Cosas. Esto significa que los derechos de privacidad y las expectativas con respecto a la privacidad de los usuarios son esenciales para asegurar la confianza de los usuarios en Internet, en los dispositivos conectados y en los servicios relacionados.

De hecho, la Internet de las Cosas está redefiniendo el debate sobre las cuestiones de

privacidad, ya que muchas implementaciones pueden cambiar drásticamente las formas en que se recogen, analizan, emplean y protegen los datos personales. Por ejemplo, la IoT amplifica las preocupaciones sobre el potencial de una mayor vigilancia y seguimiento, la dificultad de poder optar por no ser incluidos en ciertas recolecciones de datos y la potencia que tiene la agregación de los flujos de datos de la IoT para obtener retratos digitales detallados de los usuarios. Si bien estos desafíos son importantes, no son imposibles de superar. Para aprovechar las oportunidades, se deberán desarrollar estrategias para respetar las opciones de privacidad individuales considerando un amplio espectro de expectativas, sin dejar de fomentar la innovación en nuevas tecnologías y servicios.

INTEROPERABILIDAD / ESTÁNDARES

Un entorno fragmentado de implementaciones técnicas propietarias de IoT podría inhibir su valor para los usuarios y la industria. Si bien la interoperabilidad plena entre productos y servicios no siempre es posible o necesaria, los compradores podrían ser reacios a adquirir productos y servicios de la IoT si hay falta de flexibilidad en su integración, gran complejidad en cuanto a su propiedad y preocupación con respecto a posibles dificultades para cambiar de proveedores de tecnología (*lock-in*).

Además, los dispositivos de la IoT mal diseñados y configurados pueden tener consecuencias

negativas para los recursos de red a los cuales se conectan y para Internet en un sentido más amplio. Contar con estándares apropiados, modelos de referencia y mejores prácticas también ayudará a frenar la proliferación de dispositivos que podrían alterar a Internet. El uso de estándares genéricos, abiertos y ampliamente disponibles (como el Protocolo de Internet) como componentes de los dispositivos y servicios de la IoT permitirá mayores ventajas para los usuarios, más innovación y más oportunidades económicas.

CUESTIONES LEGALES, REGLAMENTARIAS Y DE DERECHOS

El uso de dispositivos de la IoT plantea nuevas cuestiones reglamentarias y legales y también amplifica los problemas legales que ya existen en torno a Internet. Estas cuestiones son de amplio alcance y muchas veces el rápido ritmo con que cambia la tecnología de la IoT supera la capacidad de adaptación de las estructuras políticas, legales y reglamentarias asociadas.

Un conjunto de cuestiones tiene que ver con los flujos de datos transfronterizos, que se producen cuando los dispositivos de la IoT recogen datos personales en una jurisdicción y, para su procesamiento, los transmiten a otra jurisdicción donde las leyes de protección de datos son diferentes. Además, los datos recogidos por los dispositivos de la IoT podrían ser mal utilizados y potencialmente provocar

resultados discriminatorios para ciertos usuarios. Otros problemas legales relacionados con los dispositivos de la IoT incluyen el conflicto entre la vigilancia por parte de las agencias de seguridad y los derechos civiles, las políticas de retención y destrucción de datos, y la responsabilidad legal por los usos accidentales, las violaciones de la seguridad y los fallos en la privacidad.

Aunque los desafíos legales y reglamentarios son de alcance amplio y complejo, la adopción de los principios rectores de la Internet Society para promover la capacidad del usuario para *conectarse, hablar, innovar, compartir, elegir, y confiar* es una consideración fundamental para la evolución de leyes y reglamentos sobre la IoT que propicien los derechos de los usuarios.

CUESTIONES RELACIONADAS CON LAS ECONOMÍAS EMERGENTES Y EL DESARROLLO:

La Internet de las Cosas encierra la promesa de aportar beneficios sociales y económicos a las economías emergentes y en desarrollo. Esto incluye, entre otras, áreas tales como la agricultura sostenible, la calidad y el uso del agua, el cuidado de la salud, la industrialización y la gestión del medio ambiente. Como tal, la IoT promete ser una herramienta para lograr los Objetivos de Desarrollo Sostenible de las Naciones Unidas.

El alcance de los desafíos de la IoT no se limitará a los países industrializados. Las regiones en

desarrollo también deberán responder para hacer realidad los potenciales beneficios de la IoT. Además, se deberán abordar las singulares necesidades y desafíos de la implementación en las regiones menos desarrolladas, entre ellos el grado de preparación de la infraestructura, los incentivos para el mercado y la inversión, los requerimientos en cuanto a las habilidades técnicas y los recursos de políticas.

La Internet de las Cosas está ocurriendo ahora. Promete ofrecer un mundo revolucionario, “inteligente” y totalmente conectado a medida que las relaciones entre los objetos, su entorno y las personas estén cada vez más entrelazadas. Sin embargo, para que la IoT realice sus potenciales beneficios para las personas, la sociedad y la economía, es necesario considerar y abordar los problemas y desafíos asociados con la IoT.

En definitiva, un debate polarizado que enfrente a las promesas de la IoT contra sus posibles peligros no permitirá encontrar soluciones que

maximicen los beneficios de la Internet de las Cosas y minimicen sus riesgos. Por el contrario, para definir las formas más eficaces de avanzar, se necesitará la participación informada, el diálogo y la colaboración de una variedad de partes interesadas.

INTRODUCCIÓN



La Internet de las Cosas (IoT) es un tema importante en la industria de la tecnología, las políticas y los círculos de ingeniería y se ha convertido en noticia de primera plana, tanto en la prensa especializada como en los medios populares. Esta tecnología se encarna en una amplia gama de productos, sistemas y sensores en red, que aprovechan los avances en la potencia de cálculo, la miniaturización de los componentes electrónicos y las interconexiones de red para ofrecer nuevas capacidades que antes no eran posibles. Una gran cantidad de conferencias, informes y artículos de noticias están discutiendo y debatiendo el potencial impacto de la “revolución de la IoT”, desde nuevas oportunidades de mercado y modelos de negocio hasta las preocupaciones con respecto a la seguridad, la privacidad y la interoperabilidad técnica.

La implementación a gran escala de dispositivos de la IoT promete transformar muchos aspectos de la forma en que vivimos. Para los consumidores, los nuevos productos de la IoT —electrodomésticos, componentes de automatización del hogar y dispositivos de gestión de energía con conexión a Internet— nos están llevando hacia una visión de la “casa inteligente” que ofrece mayor seguridad y eficiencia energética. Otros dispositivos personales de la IoT —entre ellos los dispositivos portátiles para monitorear y gestionar la actividad física y los dispositivos médicos con conexión a Internet— están transformando la forma en que se ofrecen los servicios de salud. Esta tecnología promete ser beneficiosa para las personas mayores o con discapacidad, mejorando sus niveles de independencia y calidad de vida a un costo razonable.¹ Los sistemas de la IoT como los vehículos conectados en red, los sistemas de tráfico inteligentes y los sensores integrados

en carreteras y puentes nos acercan más a la idea de “ciudades inteligentes”, que ayudan a minimizar la congestión y el consumo de energía. La tecnología de la IoT ofrece la posibilidad de transformar la agricultura, la industria y la producción y distribución de energía mediante el aumento de la disponibilidad de información a lo largo de la cadena de valor de la producción por medio de sensores conectados en red. Sin embargo, la IoT plantea muchas preguntas y desafíos que se deben tener en cuenta y abordar para que se puedan realizar sus potenciales beneficios.

Diferentes empresas y organizaciones dedicadas a la investigación han publicado una amplia gama de proyecciones sobre el potencial impacto que tendrá la IoT sobre Internet y sobre la economía en los próximos cinco a diez años. Por ejemplo, Cisco ha proyectado que para el año 2019 habrá más de 24 mil millones de objetos conectados

a Internet,² aunque Morgan Stanley anticipa que para el año 2020 habrá 75 mil millones de dispositivos conectados en red.³ Considerando un período de tiempo más largo, Huawei sube la apuesta y anticipa que en 2025 habrá 100 mil millones de conexiones a la IoT.⁴ El McKinsey Global Institute sugiere que el impacto financiero de la IoT sobre la economía global puede llegar a ser de \$3.9 a \$11.1 mil millones en 2025.⁵ Aunque la variabilidad de las predicciones las vuelve cuestionables, en conjunto permiten entrever una influencia y un crecimiento significativos.

Algunos observadores ven a la IoT como un mundo “inteligente”, revolucionario y totalmente interconectado; un mundo de progreso, eficiencia y oportunidades, con el potencial de añadir un valor equivalente a miles de millones para la industria y la economía global.⁶ Otros advierten que la IoT representa un mundo más oscuro, un mundo de vigilancia y violaciones a la privacidad en el cual los consumidores estarán atrapados. Los titulares sobre ataques cibernéticos a automóviles conectados a Internet,⁷ las preocupaciones con respecto a la vigilancia que surgen de las funciones de reconocimiento de voz de los televisores “inteligentes”⁸ y los temores con respecto a la privacidad que se derivan del posible uso indebido de los datos de la IoT⁹ han captado la atención del público. Sumado a la gran cantidad de información que publican los medios populares y el marketing, este debate sobre “promesas contra peligros” puede hacer que la IoT sea un tema complejo y difícil de entender.

En síntesis, la Internet Society se preocupa por la IoT porque representa un componente cada vez mayor de la forma en que las personas y las instituciones probablemente interactuarán

con Internet en sus vidas personales, sociales y económicas. Incluso si resultan ser correctas las proyecciones más modestas, una explosión de aplicaciones de la IoT podría provocar un cambio fundamental en la forma en que los usuarios interactúan con —y se ven afectados por— Internet, plantseando nuevas cuestiones y diferentes dimensiones de los desafíos existentes que atravesarán a todos los usuarios/ consumidores, la tecnología, las políticas y el derecho. Probablemente la IoT también tendrá diferentes consecuencias en diferentes economías y regiones, por lo que llevará un variado conjunto de oportunidades y desafíos a todo el mundo.

Este documento informativo está diseñado para ayudar a la comunidad de la Internet Society a comprender los diálogos que rodean a la Internet de las Cosas a la luz de las predicciones contradictorias sobre sus promesas y los peligros que implica. Presenta una descripción de alto nivel de los conceptos básicos de la IoT y algunas de las principales cuestiones y preguntas que esta tecnología plantea desde la perspectiva de la Internet Society y los valores fundamentales que nuestra organización promueve.^{10, 11} También reconoce algunos de los aspectos únicos de la Internet de las Cosas que la convierten en una tecnología transformacional para Internet.

Dado que el presente pretende ser un documento de naturaleza general, en este momento no proponemos para ISOC ningún curso de acción específico sobre la IoT. Más bien consideramos que este documento es una fuente de información y un punto de partida para el debate sobre cuestiones relacionadas con la IoT dentro de la comunidad de ISOC.

ORÍGENES, IMPULSORES Y APLICACIONES



El término “Internet de las Cosas” (IoT) fue empleado por primera vez en 1999 por el pionero británico Kevin Ashton para describir un sistema en el cual los objetos del mundo físico se podían conectar a Internet por medio de sensores.¹² Ashton acuñó este término para ilustrar el poder de conectar a Internet las etiquetas de identificación por radiofrecuencia (RFID)¹³ que se utilizaban en las cadenas de suministro corporativas para contar y realizar un seguimiento de las mercancías sin necesidad de intervención humana. Hoy en día, el término Internet de las Cosas se ha popularizado para describir escenarios en los que la conectividad a Internet y la capacidad de cómputo se extienden a una variedad de objetos, dispositivos, sensores y artículos de uso diario.

Aunque el término “Internet de las Cosas” es relativamente nuevo, el concepto de combinar computadoras y redes para monitorear y controlar diferentes dispositivos ha existido durante décadas. Por ejemplo, a fines de la década de 1970 ya había en el mercado sistemas disponibles para monitorear los medidores conectados a la red eléctrica de forma remota a través de las líneas telefónicas.¹⁴ En la década de 1990, los avances en la tecnología inalámbrica permitieron la difusión de soluciones corporativas e industriales “máquina a máquina” (M2M) para monitorear y operar diferentes equipos. Sin embargo, muchas de estas primeras soluciones M2M se basaban en redes dedicadas especialmente construidas para este propósito y en estándares propietarios o específicos de la industria,¹⁵ no en redes basadas en el Protocolo de Internet (IP) y los estándares de Internet.

El uso del protocolo IP para conectar a Internet dispositivos que no son computadoras no es una idea nueva. El primer “dispositivo” para Internet —una tostadora conectada vía IP que se podía encender y apagar a través de

Internet— se presentó en una conferencia sobre Internet realizada en 1990.¹⁶ Durante los años siguientes se fueron conectando otras “cosas” vía IP, entre ellas una máquina de refrescos¹⁷ en la Universidad Carnegie Mellon en Estados Unidos y una cafetera¹⁸ en el *Trojan Room* de la Universidad de Cambridge en el Reino Unido (que permaneció conectada a Internet hasta 2001). Luego de estos coloridos inicios, una robusta área de investigación y desarrollo dedicada a las “redes de objetos inteligentes”¹⁹ ayudó a sentar las bases de la Internet de las Cosas como la conocemos hoy.

Si la idea de conectar objetos entre sí y a Internet no es nuevo, es razonable preguntar por qué la Internet de las Cosas es un tema que hoy en día está ganando popularidad.

Desde una perspectiva amplia, la confluencia de diferentes tendencias tecnológicas y de mercado²⁰ está permitiendo interconectar dispositivos más pequeños de forma económica y sencilla:

DEFINICIONES DIFERENTES, CONCEPTOS SIMILARES



A pesar del entusiasmo generalizado en torno a la Internet de las Cosas, no existe una definición única y universalmente aceptada para el término. Diferentes grupos utilizan diferentes definiciones para describir o promover una visión particular de lo que significa la IoT y sus atributos más importantes.

Algunas definiciones especifican el concepto de Internet o del Protocolo de Internet (IP), mientras que otras —quizás sorprendentemente— no lo hacen. Por ejemplo, veamos las siguientes definiciones.

El Consejo de Arquitectura de Internet (IAB) comienza la RFC 7452,³³ "Architectural Considerations in Smart Object Networking", con esta definición:

El término "Internet de las Cosas" (IoT) denota una tendencia en que un gran número de dispositivos embebidos utilizan los servicios de comunicación que ofrecen los protocolos de Internet. A estos dispositivos suelen llamarles "objetos inteligentes" y no son operados directamente por un ser humano, sino que existen como componentes en edificios o vehículos o están distribuidos en el entorno.

Dentro del Grupo de Trabajo en Ingeniería de Internet (IETF), el término "redes de objetos inteligentes" se utiliza habitualmente para referirse a la Internet de las Cosas. En este contexto, los "objetos inteligentes" son dispositivos que típicamente tienen limitaciones significativas, como por ejemplo limitaciones en cuanto a la energía, la memoria y los recursos de procesamiento, o el ancho de banda.³⁴ El trabajo en el IETF se organiza en torno a requisitos específicos para lograr la interoperabilidad entre varios tipos de objetos inteligentes.³⁵

La Recomendación ITU-T Y.2060 que publicó la Unión Internacional de Telecomunicaciones

(UIT) en 2012, *Overview of the Internet of things*³⁶, discute el concepto de interconectividad, pero no vincula a la IoT específicamente con Internet:

3.2.2 Internet de las Cosas (IoT):

Infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperatividad de tecnologías de la información y la comunicación presentes y futuras.

Nota 1 — Gracias a la identificación, la adquisición y el procesamiento de datos y a las capacidades de comunicación, la IoT hace pleno uso de los objetos para ofrecer servicios a todo tipo de aplicaciones, garantizando a su vez el cumplimiento íntegro de los requisitos de seguridad y privacidad.

Nota 2 — Desde una perspectiva más amplia, la IoT puede considerarse una noción con repercusiones tecnológicas y sociales.

Esta definición incluida en una convocatoria de trabajos para una edición de la IEEE Communications Magazine³⁷ vincula a la IoT con los servicios en la nube:

MODELOS DE COMUNICACIÓN DE LA INTERNET DE LAS COSAS



Desde el punto de vista operativo, es útil pensar en cómo se conectan y comunican los dispositivos de la IoT en términos de sus modelos de comunicación. En marzo de 2015, el Comité de Arquitectura de Internet (IAB) dio a conocer un documento para guiar la creación de redes de objetos inteligentes (RFC 7452),³⁹ que describe un marco de cuatro modelos de comunicación comunes que utilizan los dispositivos de la IoT. En la discusión siguiente se presenta este marco y se explican las principales características de cada modelo.

Comunicaciones ‘dispositivo a dispositivo’

El modelo de comunicación dispositivo a dispositivo representa dos o más dispositivos que se conectan y se comunican directamente entre sí y no a través de un servidor de aplicaciones intermediario. Estos dispositivos se comunican sobre muchos tipos de redes, entre ellas las redes IP o la Internet. Sin embargo, para establecer comunicaciones directas de dispositivo a dispositivo, muchas veces se utilizan protocolos como Bluetooth,⁴⁰ Z-Wave⁴¹ o ZigBee⁴², como se muestra en la Figura 1.

Estas redes dispositivo a dispositivo permiten que los dispositivos que, para comunicarse e intercambiar mensajes, se adhieren a un determinado protocolo de comunicación logren su función. Por lo general, este modelo de comunicación se utiliza en aplicaciones como sistemas de automatización del hogar, que habitualmente utilizan pequeños paquetes de datos para la comunicación entre dispositivos con requisitos relativamente bajos en términos de la tasa de transmisión. Los dispositivos para la IoT residenciales —bombillas de luz, interruptores, termostatos y cerraduras— normalmente se

envían pequeñas cantidades de información (por ejemplo, un mensaje del estado de bloqueo de una puerta o un comando para encender una luz) en un escenario de automatización del hogar.

Este enfoque de comunicación dispositivo a dispositivo ilustra muchos de los desafíos de interoperabilidad que se discuten más adelante en este trabajo. Según lo describe un artículo del *IETF Journal*, “muchas veces estos dispositivos se relacionan en forma directa, en general tienen [mecanismos de] seguridad y confianza integrados; además, utilizan modelos de datos específicos para cada dispositivo que requieren esfuerzos de desarrollo redundantes [por parte de los fabricantes de dispositivos]”.⁴³ Esto significa que los fabricantes deben invertir en desarrollar la forma de implementar formatos de datos específicos de diferentes dispositivos antes que métodos abiertos que permitan el uso de formatos de datos estándares.

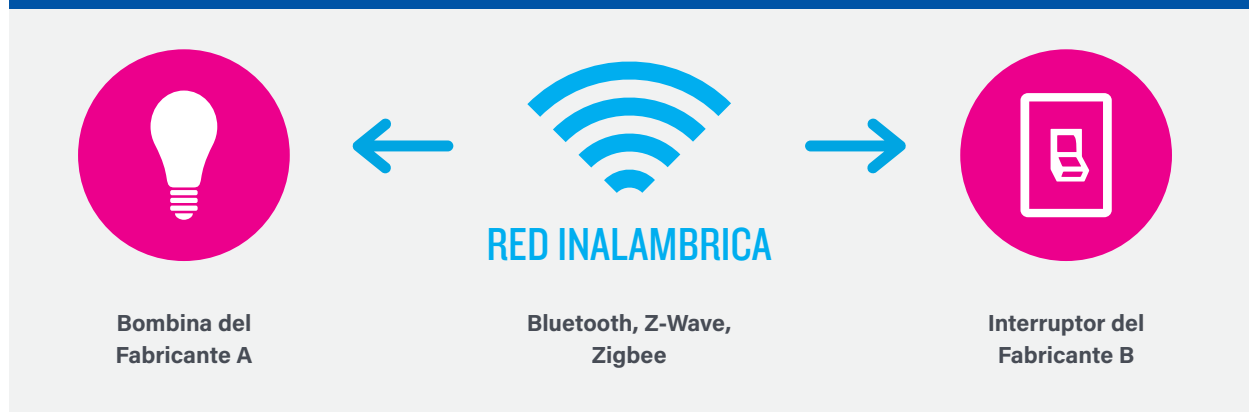
Desde el punto de vista de los usuarios, esto significa que los protocolos de comunicación dispositivo a dispositivo subyacentes no son compatibles, lo que los obliga a seleccionar una

familia de dispositivos que emplean un protocolo común. Por ejemplo, la familia de dispositivos que utilizan el protocolo Z-Wave no es compatible de forma nativa con la familia de dispositivos ZigBee. Si bien estas incompatibilidades limitan

la capacidad de elección de los usuarios a los dispositivos de una determinada familia de protocolos, los usuarios también saben que los productos de una familia determinada tienden a comunicarse bien.

FIGURA 1

Ejemplo de un modelo de comunicación dispositivo a dispositivo



Comunicaciones 'dispositivo a la nube'

En un modelo de comunicación de dispositivo a la nube, el dispositivo de la IoT se conecta directamente a un servicio en la nube, como por ejemplo un proveedor de servicios de aplicaciones para intercambiar datos y controlar el tráfico de mensajes. Este enfoque suele aprovechar los mecanismos de comunicación existentes (por ejemplo, las conexiones Wi-Fi o Ethernet cableadas tradicionales) para establecer una conexión entre el dispositivo y la red IP, que luego se conecta con el servicio en la nube. Esto se ilustra en la Figura 2.

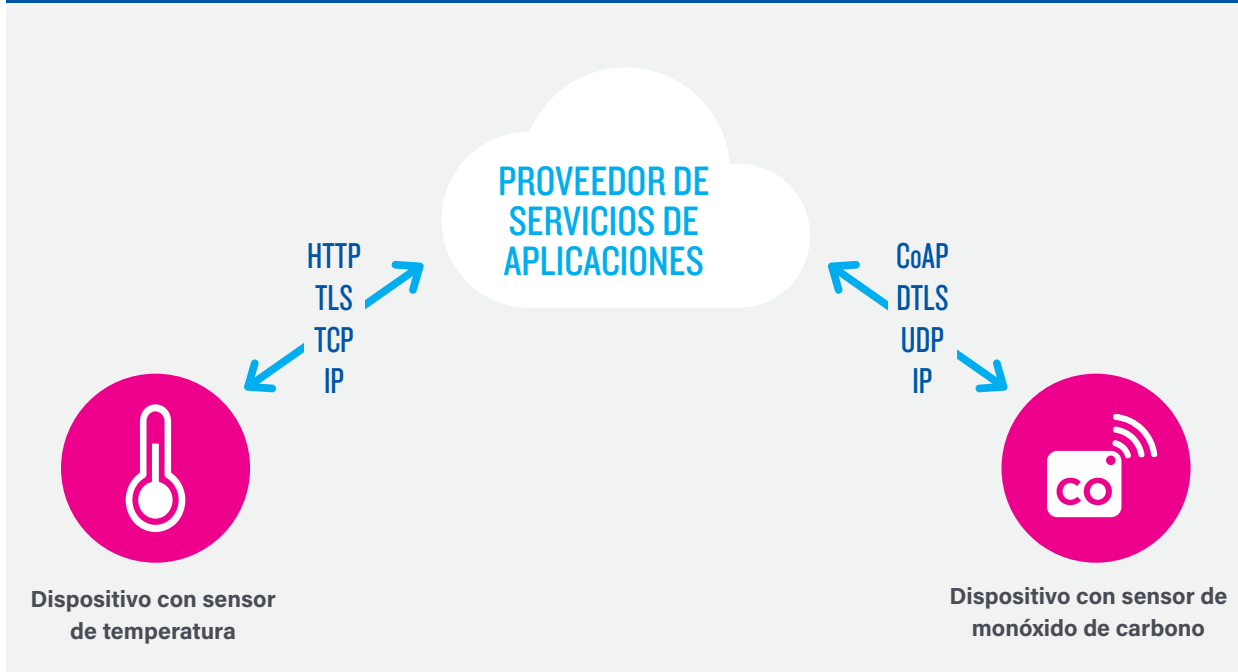
Este modelo de comunicación es empleado por algunos dispositivos electrónicos de consumo para la IoT, entre ellos el *Learning Thermostat*⁴⁴ de Nest Labs y el *SmartTV* de Samsung.⁴⁵ En el caso del *Learning Thermostat*, el dispositivo transmite los datos a una base de datos en la nube donde se pueden usar para analizar el consumo de energía en el hogar. Además, esta conexión a la nube permite que el usuario acceda a su termostato en forma remota, a través de un teléfono inteligente o una interfaz web, y también soporta las actualizaciones del software del termostato. Algo similar ocurre con la tecnología *SmartTV* de Samsung — el televisor utiliza una

conexión a Internet para transmitir información a Samsung para su análisis y para activar las funciones interactivas de reconocimiento de voz de la televisión. En estos casos, el modelo dispositivo a la nube agrega valor para el usuario final, ya que amplía las capacidades del dispositivo más allá de sus características nativas.

No obstante, al intentar integrar dispositivos de diferentes fabricantes pueden surgir problemas de interoperabilidad. Muchas veces el dispositivo y el servicio en la nube son del mismo proveedor de tecnología.⁴⁶ Si entre el dispositivo y el servicio en la nube se utilizan protocolos de datos propietarios, el dueño del dispositivo o el usuario podrían quedar atados a un servicio en la nube específico, lo que limitaría o impediría el uso de proveedores de servicios alternativos. Esto generalmente se conoce como "dependencia de un proveedor" (*vendor lock-in*), un término que abarca otras facetas de la relación con el proveedor, como por ejemplo la propiedad y el acceso a los datos. A la vez, los usuarios generalmente pueden confiar en que los dispositivos diseñados para su plataforma específica se podrán integrar.

FIGURA 2

Diagrama del modelo de comunicación dispositivo a la nube



Modelo 'dispositivo a puerta de enlace'

En el modelo dispositivo a puerta de enlace, o más generalmente el modelo dispositivo a puerta de enlace de capa de aplicación (ALG), el dispositivo de la IoT se conecta a través de un servicio ALG como una forma de llegar a un servicio en la nube. Dicho de otra manera, esto significa que hay un software de aplicación corriendo en un dispositivo de puerta de enlace local, que actúa como intermediario entre el dispositivo y el servicio en la nube y provee seguridad y otras funcionalidades tales como traducción de protocolos o datos. Este modelo se ilustra en la Figura 3.

En los dispositivos de consumo se utilizan diferentes formas de este modelo. En muchos casos, el dispositivo de puerta de enlace local es un teléfono inteligente con una aplicación para comunicarse con un dispositivo y transmitir datos a un servicio en la nube. Esto suele ser el modelo empleado con los artículos de consumo populares como los dispositivos utilizados

para llevar registro de la actividad física. Estos dispositivos no tienen capacidad nativa para conectarse directamente a un servicio en la nube, por lo que muchas veces utilizan una aplicación para teléfono inteligente como puerta de enlace intermedia.

Otra forma de este modelo tipo dispositivo a puerta de enlace es la aparición de dispositivos "hub" en las aplicaciones de automatización del hogar. Se trata de dispositivos que sirven de puerta de enlace local entre los dispositivos individuales de la IoT y un servicio en la nube, pero que también pueden reducir los problemas de interoperabilidad entre los propios dispositivos. Por ejemplo, el hub *SmartThings* es un dispositivo de puerta de enlace independiente que tiene instalados transceptores Z-Wave y Zigbee para comunicarse con ambas familias de dispositivos.⁴⁷ Luego se conecta al servicio en la nube *SmartThings* y permite que el usuario acceda a los dispositivos usando una aplicación

para teléfono inteligente y una conexión a Internet.

Desde una perspectiva técnica más amplia, el artículo del IETF Journal explica las ventajas del enfoque dispositivo a puerta de enlace:

Este modelo de comunicación se usa en situaciones donde los objetos pequeños deben interoperar con dispositivos que no utilizan el protocolo de Internet. A veces se adopta este enfoque para integrar dispositivos que solo soportan IPv6, lo que significa que se necesita una puerta de enlace para los dispositivos y servicios existentes que solo soportan IPv4.⁴⁸

En otras palabras, este modelo de comunicación se suele utilizar para integrar nuevos dispositivos inteligentes en un sistema heredado con

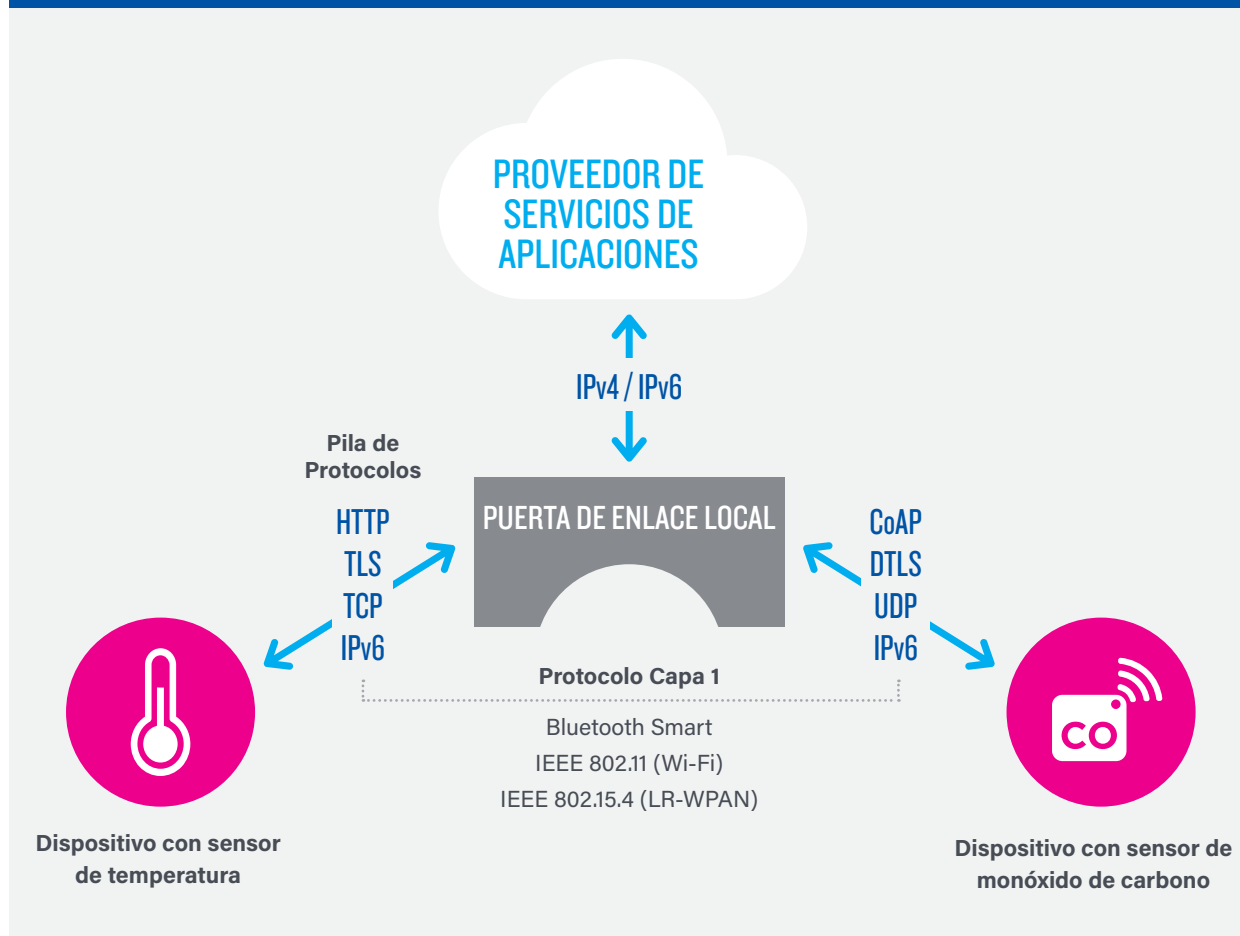
dispositivos que no son interoperables de forma nativa. Una desventaja de este enfoque es el costo y la complejidad que implican el desarrollo del software y el sistema para la puerta de enlace de capa de aplicación.

La RFC7452 del IAB sugiere una perspectiva para este modelo:

Se anticipa que en el futuro se desplegarán más puertas de enlace genéricas con menores costos e infraestructura menos compleja para los consumidores finales, las empresas y los entornos industriales. La existencia de tales puertas de enlace será más probable si el diseño de los dispositivos de la IoT utiliza protocolos de Internet genéricos y no requiere puertas de enlace de capa de aplicación para traducir un protocolo

FIGURA 3

Ejemplo del modelo de comunicación de 'dispositivo a puerta de enlace'



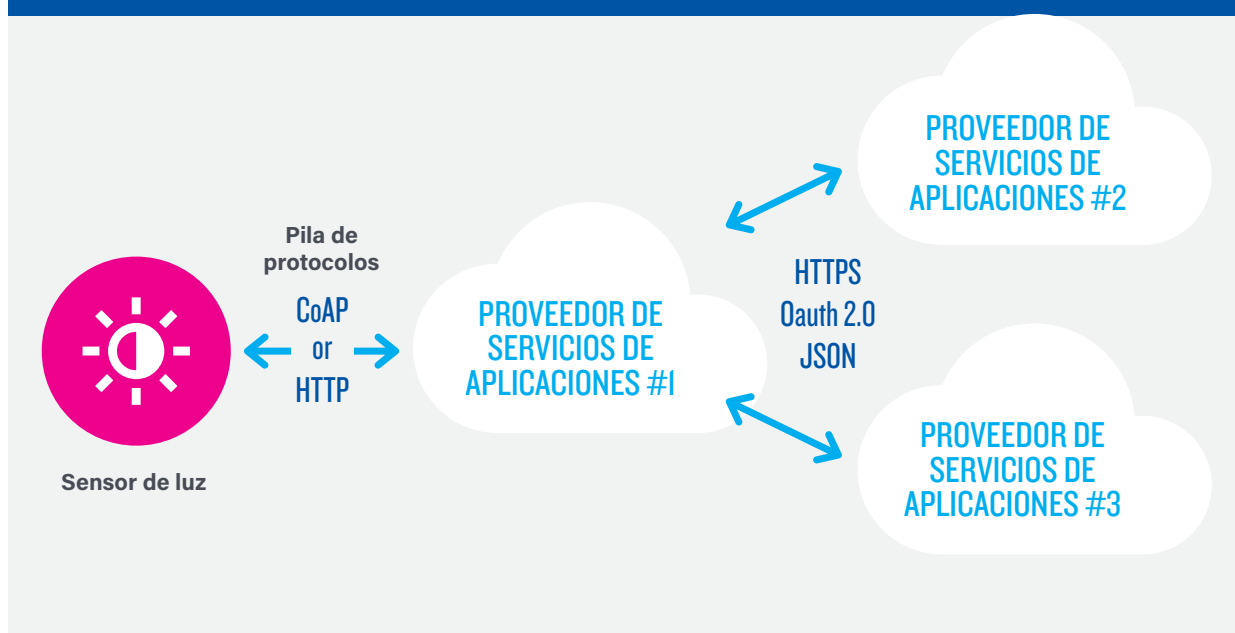
de capa de aplicación a otro. En general, el uso de puertas de enlace de capa de aplicación llevará a un despliegue más frágil, como ya se ha observado en el pasado...⁴⁹

Los sistemas que utilizan el modelo de comunicación dispositivo a puerta de enlace

y su papel más amplio en el abordaje de los problemas de interoperabilidad entre dispositivos de la IoT todavía están evolucionando.

FIGURA 4

Diagrama del modelo de intercambio de datos a través del back-end.



Modelo de intercambio de datos a través del back-end

El modelo de intercambio de datos a través del *back-end* se refiere a una arquitectura de comunicación que permite que los usuarios exporten y analicen datos de objetos inteligentes de un servicio en la nube en combinación con datos de otras fuentes. Esta arquitectura soporta "el deseo del usuario de permitir que terceros accedan a los datos subidos por sus sensores."⁵⁰ Este enfoque es una extensión del modelo de comunicación tipo 'dispositivo único a la nube', que puede llevar a la existencia de silos de datos donde "los dispositivos de la IoT suben datos a un único proveedor de servicios de aplicaciones."⁵¹ Una arquitectura de intercambio de datos a través del *back-end* permite agregar y analizar los

datos recogidos de flujos obtenidos de un solo dispositivo de la IoT.

Por ejemplo, a un usuario corporativo a cargo de un complejo de oficinas le interesaría consolidar y analizar los datos de consumo de energía y otros servicios que producen todos los sensores de la IoT y los correspondientes sistemas habilitados para Internet disponibles en las instalaciones. En el modelo 'dispositivo único a la nube', muchas veces los datos que produce cada sensor o sistema de la IoT queda en un silo de datos independiente. Una arquitectura eficaz de intercambio de datos a través del *back-end* permitiría que la empresa acceda y analice fácilmente, en la nube, los datos producidos por

toda la gama de dispositivos instalados en el edificio. Además, este tipo de arquitectura facilita la portabilidad de los datos. Las arquitecturas eficaces de intercambio de datos a través del *back-end* permiten que los usuarios muevan sus datos al cambiar de servicio de IoT, rompiendo así las barreras tradicionales de los silos de datos.

El modelo de intercambio de datos a través del *back-end* sugiere que, para lograr la interoperabilidad de los datos de dispositivos inteligentes alojados en la nube, se requiere un enfoque de servicios federados⁵² o interfaces de programación de aplicaciones (APIs) en la nube.⁵³ La Figura 4 muestra una representación de este diseño.

Este modelo de arquitectura es un enfoque para lograr interoperabilidad entre estos sistemas de *back-end*. Como sugiere el *IETF Journal*, "los protocolos estándares pueden ayudar, pero no son suficientes para eliminar los silos de datos dado que entre proveedores son necesarios modelos de información comunes."⁵⁴ En otras palabras, este modelo de comunicación es apenas tan eficaz como los diseños de los sistemas subyacentes de la IoT. Las arquitecturas de intercambio de datos a través del *back-end* no pueden superar completamente los diseños de los sistemas cerrados.

Modelos de comunicación de la Internet de las Cosas: resumen

Los cuatro modelos básicos de comunicación muestran las estrategias de diseño subyacentes utilizadas para permitir que los dispositivos de la IO se comuniquen. Además de ciertas consideraciones técnicas, el uso de estos modelos está influenciada en gran parte por la naturaleza abierta versus propietaria de los dispositivos de la IoT que se conectan en red. En el caso del modelo 'dispositivo a puerta de enlace', su principal característica es la capacidad de superar las restricciones que implica la conexión de dispositivos propietarios a la IoT. Esto significa que la interoperabilidad de los dispositivos y los estándares abiertos son consideraciones clave para el diseño y el desarrollo de sistemas de la Internet de las Cosas interconectados.

Desde el punto de vista del usuario en general, estos modelos de comunicación sirven para ilustrar la capacidad de agregar valor que tienen los dispositivos conectados en red. Al permitir que el usuario logre un mejor acceso a un dispositivo de la IoT y a sus datos, el valor global del dispositivo aumenta. Por ejemplo, en tres de los cuatro modelos de comunicación descritos, en última instancia los dispositivos se conectan a servicios de análisis de datos en un entorno de cómputo en la nube. Al crear conductos para comunicar datos a la nube, los usuarios y los proveedores de servicios pueden agregar los datos, analizar grandes volúmenes de datos y visualizar datos más fácilmente;

además, las tecnologías de análisis predictivo obtienen más valor de los datos de la IoT del que pueden obtener las aplicaciones de silos de datos tradicionales. En otras palabras, las arquitecturas de comunicación eficaces son un importante generador de valor para el usuario final, ya que abren la posibilidad de utilizar la información de formas nuevas. Sin embargo, cabe señalar que estos beneficios no vienen sin desventajas. Al considerar una arquitectura determinada, es necesario considerar cuidadosamente los costos que deben incurrir los usuarios para conectarse a recursos en la nube, especialmente en las regiones donde los costos de conectividad del usuario son elevados.

Los modelos de comunicación efectivos benefician al usuario final, pero también cabe mencionar que los modelos eficaces de comunicación de la IoT también mejoran la innovación técnica y las oportunidades para el crecimiento comercial. Se pueden diseñar nuevos productos y servicios que aprovechen los flujos de datos de la IoT que antes no existían, y estos podrían catalizar la innovación.

Sería imposible abarcar el amplio espectro de temas relacionados con la Internet de las Cosas en un solo trabajo. No obstante, a continuación ofrecemos un resumen de cinco temas que surgen muy frecuentemente en relación con la IoT. Estos incluyen: la seguridad; la privacidad; la interoperabilidad y los estándares; aspectos legales, reglamentarios y de derechos; y las economías emergentes y el desarrollo.



SEGURIDAD



PRIVACIDAD



INTEROPERABILIDAD / ESTÁNDARES



CUESTIONES LEGALES, REGLAMENTARIAS Y DE DERECHOS



CUESTIONES RELACIONADAS CON LAS ECONOMÍAS EMERGENTES Y EL DESARROLLO

Comenzamos nuestro análisis de estos temas a través del lente de las “Capacidades”, la declaración de principios fundamentales que guían el trabajo de ISOC en términos de las habilidades que creemos que todos los usuarios de Internet deben disfrutar y que se deben proteger. Estas incluyen la capacidad de **conectarse, hablar, innovar, compartir, escoger** y **confiar**.⁵⁵ Con estos principios como guía, presentamos aspectos importantes de cada tema y planteamos diferentes temas para su debate.

El desafío de seguridad de la IoT

Tal como se observa en los principios que guían nuestro trabajo, garantizar la seguridad, la confiabilidad, la resiliencia y la estabilidad de las aplicaciones y servicios de Internet es fundamental para fomentar la **confianza** y el uso de Internet.⁵⁶ Como usuarios de Internet, tenemos que tener un alto grado de confianza en que Internet, sus aplicaciones y los dispositivos conectados a la red son lo suficientemente seguros como para realizar en línea toda la gama de actividades que deseamos en relación con la tolerancia al riesgo asociado con tales actividades. En este sentido, la Internet de las cosas no es diferente y la seguridad de la IoT está fundamentalmente relacionada con la capacidad de los usuarios de confiar en su entorno. Si los usuarios no creen que los dispositivos que tienen conectados y su información están razonablemente seguros contra el mal uso o los daños, la erosión de la confianza resultante provoca una renuencia a usar Internet. Esto tiene consecuencias globales para el comercio electrónico, la innovación técnica, la libertad de expresión y prácticamente para todos los demás aspectos de las actividades en línea. En efecto, para garantizar la seguridad en los productos y servicios de la IoT, el sector debe considerar la seguridad como una de sus máximas prioridades.

A medida que conectamos cada vez más dispositivos a Internet, surgen nuevas oportunidades para explotar potenciales vulnerabilidades de seguridad. Los dispositivos de la IoT mal asegurados servir como puntos de entrada para ciberataques, permitiendo que personas malintencionadas reprogramaran un dispositivo o perjudicaran su funcionamiento. Los dispositivos de la IoT mal diseñados pueden exponer los datos de los usuarios a robos, dejando los flujos de usuarios sin una protección adecuada. Los dispositivos defectuosos o que no funcionan bien también pueden crear vulnerabilidades. Estos problemas son tanto o más graves en el caso de los dispositivos inteligentes pequeños, baratos y ubicuos en la Internet de las Cosas que en el caso de los equipos que tradicionalmente han sido los puntos extremos de la conectividad a Internet. Los desafíos que imponen la competitividad de los costos y las limitaciones técnicas de la IoT hacen que para los fabricantes de dispositivos no sea fácil diseñar funciones de seguridad adecuadas, potencialmente generando, a largo plazo, vulnerabilidades en la seguridad y dificultades en el mantenimiento superiores a las computadoras tradicionales.

Junto con posibles deficiencias en el diseño de la seguridad, el enorme aumento del número y la variedad de los dispositivos de la IoT podría aumentar las oportunidades de ataque. Sumado a la naturaleza altamente interconectada de los dispositivos de la IoT, cada dispositivo mal asegurado conectado en línea potencialmente afecta la seguridad y la resistencia de Internet a nivel global, no solo a nivel local. Por ejemplo, un refrigerador o un televisor sin protección infectado con malware que se encuentra en Estados Unidos pueden enviar miles de correos electrónicos no deseados dañinos a destinatarios de todo el mundo usando la conexión Wi-Fi de la casa.⁵⁷

Para complicar todavía más las cosas, en un mundo hiperconectado, nuestra capacidad de funcionar diariamente sin dispositivos o sistemas conectados a Internet probablemente disminuirá. De hecho, es cada vez más difícil comprar ciertos dispositivos sin conexión a Internet, ya que algunos fabricantes solo ofrecen productos conectados. Cada vez estamos más conectados y dependemos más de los dispositivos de la IoT para muchos servicios esenciales, por lo que necesitamos que los dispositivos sean seguros. Pero también reconocemos que ningún dispositivo puede ser absolutamente seguro. Este creciente nivel de dependencia de los dispositivos de la IoT y de los servicios de Internet con los cuales interactúan también aumenta las formas que tienen los delincuentes para acceder a los dispositivos. Si se ven comprometidas en un ataque cibernético, quizá podríamos desenchufar nuestros televisores conectados a Internet, pero no es tan fácil apagar un medidor inteligente de energía eléctrica, un sistema de control de tráfico o un marcapasos si estos dispositivos son víctimas de un ataque malicioso.

Esta es la razón por la cual la seguridad de los dispositivos y servicios de la IoT debe ser un importante punto de discusión y un tema crítico. Dependemos cada vez más de estos dispositivos para servicios esenciales, por lo que su comportamiento puede tener un alcance y un impacto globales.

Cada dispositivo mal asegurado conectado en línea potencialmente afecta la seguridad y la resistencia de Internet a nivel global, no solo a nivel local.

Un espectro de consideraciones de seguridad

Al pensar en los dispositivos de la Internet de las Cosas, es importante entender que la seguridad de estos dispositivos no es absoluta. La seguridad de los dispositivos de la IoT no es una proposición binaria de tipo seguro/inseguro. Por el contrario, resulta útil conceptualizar la seguridad de la IoT como un espectro de vulnerabilidad los dispositivos. El espectro va desde dispositivos totalmente desprotegidos sin ninguna función de seguridad hasta sistemas muy seguros con múltiples capas de elementos de seguridad. En un constante juego de gato y ratón, a medida que las nuevas amenazas de seguridad evolucionan, los fabricantes de dispositivos y los operadores de redes responden para hacer frente a las nuevas amenazas.

La seguridad general y la resiliencia de la Internet de las Cosas dependen de cómo se evalúen y gestionen los riesgos de seguridad. La seguridad de un dispositivo es función del riesgo de que un dispositivo se vea comprometido, del daño que tal compromiso provocaría y del tiempo y los recursos necesarios para lograr cierto nivel de protección. Si un usuario no puede tolerar un alto grado de riesgo (por ejemplo, un operador de un sistema de control de tráfico o una persona a quien se le ha implantado un dispositivo médico que está conectado a Internet implantado), puede que para dicho usuario sienta que se justifica gastar una cantidad considerable de recursos para proteger el sistema o el dispositivo contra un ataque. Del mismo modo, si a la persona no le preocupa que su refrigerador pueda ser hackeado y utilizado para enviar spam, puede que no se sienta obligada a pagar por un modelo que tenga un diseño de seguridad más sofisticado si esto hace que el dispositivo sea más costoso o complicado.

En esta evaluación y cálculo de la mitigación de los riesgos influyen diferentes factores. Estos factores incluyen una comprensión clara de los riesgos de seguridad actuales y posibles riesgos futuros, la estimación de los costos económicos y otros tipos de daño si los riesgos se hacen realidad, y el costo estimado de la mitigación de los riesgos.⁵⁸ Si bien este tipo de concesiones de seguridad muchas veces se realizan desde la perspectiva de los usuarios individuales y las organizaciones, también es importante tener en cuenta la interrelación de los dispositivos de la IoT como parte de un ecosistema mayor. La conectividad en red de los dispositivos de la IoT significa que las decisiones de seguridad que se

toman a nivel local con respecto a un dispositivo pueden tener impactos globales sobre otros dispositivos.

Como cuestión de principio, quienes desarrollan objetos inteligentes para la Internet de las Cosas tienen la obligación de garantizar que estos dispositivos no expongan los bienes de sus propios usuarios ni de otras personas a potenciales daños. Como cuestión de negocios y de economía, a los fabricantes desean reducir sus costos, su complejidad y su tiempo de comercialización. Por ejemplo, son cada vez más comunes los dispositivos de la IoT de alto volumen y bajo margen de ganancia y que ya representan un costo adicional para los productos en los que están embebidos; añadir más memoria y un procesador más rápido para implementar medidas de seguridad podría hacer que el producto ya no fuera competitivo.

En términos económicos, el resultado de la falta de seguridad en los dispositivos de la IoT es una externalidad negativa, donde una o más partes imponen un costo sobre otras. Un ejemplo clásico es la contaminación del medio ambiente, donde los costos de los daños y la limpieza (externalidades negativas) resultantes de las acciones de quien contamina son asumidos por otras partes. El hecho es que el costo de la externalidad impuesto a los demás normalmente no se considera en el proceso de toma de decisiones, a menos que, como es el caso de la contaminación, se aplique un impuesto que sirva de aliciente para reducir la contaminación. De acuerdo con Bruce Schneier,⁵⁹ en el caso de la seguridad de la información surge una externalidad cuando el proveedor que crea el producto no corre con los costos que ocasionan las potenciales inseguridades; en este caso, una ley de responsabilidad puede convencer a los vendedores para que tomen en cuenta la externalidad y desarrollen más productos de seguridad.

Estas consideraciones de seguridad no son nuevas en el contexto de la tecnología de la información, pero la magnitud de los desafíos que pueden surgir en las implementaciones de la IoT las vuelve extremadamente significativas. Estos desafíos se describen a continuación.

Desafíos de seguridad que son exclusivos de los dispositivos de la IoT

Las diferencias entre los dispositivos de la IoT y las computadoras y los dispositivos informáticos tradicionales suelen desafiar la seguridad:

Muchos dispositivos de la Internet de las Cosas (por ejemplo, los sensores y los artículos de consumo) están diseñados para ser desplegados a una escala masiva que es varios órdenes de magnitud superior a la de los dispositivos tradicionalmente conectados a Internet. Por consiguiente, la potencial cantidad de enlaces interconectados entre estos dispositivos no tiene precedentes. Además, muchos de estos dispositivos podrán establecer enlaces y comunicarse con otros dispositivos por sí mismos, de manera impredecible y dinámica. Por lo tanto, puede ser necesario considerar nuevamente las herramientas, métodos y estrategias existentes asociadas con la seguridad de la IoT.

Muchos despliegues de la IoT consistirán en colecciones de dispositivos idénticos o prácticamente idénticos. Esta homogeneidad amplifica el potencial impacto de cualquier vulnerabilidad de seguridad simplemente por la gran cantidad de dispositivos que tienen las mismas características. Por ejemplo, una vulnerabilidad en el protocolo de comunicación de una marca de bombillas de luz conectadas a Internet se podría extender a todas las marcas y modelos de dispositivos que utilizan el mismo protocolo o que comparten características clave de diseño o fabricación.

Muchos de los dispositivos de la Internet de las Cosas que se van a desplegar tendrán una vida útil anticipada muy superior a la que típicamente se espera para los equipos de alta tecnología. Además, estos dispositivos se podrían desplegar en circunstancias que los harían difíciles o imposibles de reconfigurar o actualizar; o bien estos dispositivos podrían sobrevivir a la empresa que los creó, lo que los dejaría huérfanos y sin apoyo a largo plazo. Estos escenarios ilustran que los mecanismos de seguridad que son adecuados en el momento del despliegue podrían no ser adecuados durante toda la vida útil del dispositivo y a medida que las amenazas a la seguridad evolucionen. Esta situación podría crear vulnerabilidades que podrían persistir por

mucho tiempo. Esto contrasta con el paradigma de los sistemas de computadoras tradicionales en los cuales normalmente se aplican actualizaciones al sistema operativo durante toda la vida de servicio de los equipos para hacer frente a las amenazas de seguridad. El apoyo y la gestión a largo plazo de los dispositivos de la IoT representa un importante reto de seguridad.

Muchos dispositivos de la IoT estén diseñados intencionadamente sin ninguna posibilidad de actualización; en otros, el proceso de actualización es engorroso o poco práctico. Por ejemplo, consideremos el retiro de 1.4 millones de automóviles Fiat Chrysler 2015 para arreglar una vulnerabilidad que potencialmente permitiría hackear el vehículo en forma inalámbrica. Estos vehículos se deben llevar a un concesionario Fiat Chrysler para que les realicen una actualización manual del software, o bien los propietarios deben actualizar el software por sí mismos usando una memoria USB. La realidad es que un alto porcentaje de estos automóviles probablemente no se actualizará porque el proceso de actualización representa un inconveniente para los propietarios, y esto los deja permanentemente vulnerables a las amenazas de seguridad cibernética, sobre todo porque el automóvil parece estar funcionando muy bien.

Muchos dispositivos de la IoT funcionan de modo que es escasa o nula la visibilidad que tiene el usuario de su funcionamiento interno o de los flujos de datos que producen. Si un usuario cree que un dispositivo está ejecutando ciertas funciones pero en realidad está ejecutando funciones no deseadas o recogiendo más información que lo que el usuario desea, se crea una vulnerabilidad. Las funciones del dispositivo también podrían cambiar sin previo aviso cuando el fabricante ofrece una actualización, lo que deja al usuario vulnerable a cualquier cambio que realice el fabricante.

Algunos dispositivos de la IoT probablemente serán ser desplegados en lugares donde sea difícil o imposible lograr la seguridad física. Los

atacantes pueden tener acceso físico directo a los dispositivos. Para garantizar la seguridad será necesario considerar el uso de protección contra manipulaciones y otras innovaciones de diseño.

Al igual que muchos sensores ambientales, algunos dispositivos de la IoT han sido diseñados para ser integrados discretamente en su entorno, donde los usuarios apenas se den cuenta de su presencia o monitoreen su funcionamiento. Además, los dispositivos pueden no tener una forma clara de alertar al usuario cuando surge un problema de seguridad, por lo que es difícil para un usuario saber que la seguridad de un dispositivo de la IoT ha sido vulnerada. Esta situación podría persistir por mucho tiempo antes de ser detectada y corregida; incluso podría darse el

caso de que no fuera posible o práctico implementar una corrección o mitigación. Del mismo modo, el usuario podría no ser consciente de que existe un sensor en su entorno, por lo que potencialmente un fallo de seguridad podría persistir por mucho tiempo sin ser detectado.

Los primeros modelos de la Internet de las Cosas asumen que la IoT será producto de grandes empresas de tecnología privadas y/o públicas. Sin embargo, en el futuro “construir su propia Internet de las Cosas” (*Build Your own Internet of Things, BYIoT*) podría convertirse en algo habitual, como lo demuestra el crecimiento de las comunidades de desarrolladores de *Arduino* y *Raspberry Pi*.⁶⁰ Estos despliegues podrán o no aplicar los estándares de mejores prácticas de seguridad de la industria.

Preguntas relacionadas con la seguridad de la IoT

Se ha planteado una serie de preguntas con respecto a los problemas de seguridad que plantea la Internet de las Cosas. Muchas de estas preguntas ya existían antes del crecimiento de la IoT, pero su importancia ha aumentado debido a la magnitud del despliegue de los dispositivos utilizados. Entre las preguntas más importantes podemos mencionar las siguientes:

BUENAS PRÁCTICAS DE DISEÑO

¿Cuáles son las mejores prácticas que los ingenieros y desarrolladores deben utilizar al diseñar dispositivos de la IoT para que sean más seguros? ¿Cómo se recogen y transmiten las lecciones aprendidas a partir de los problemas de seguridad de la Internet de las Cosas a las comunidades de desarrolladores para mejorar las futuras generaciones de dispositivos? ¿Qué formación y recursos educativos se pueden utilizar para enseñar a los ingenieros y desarrolladores cómo diseñar una IoT más segura?

EQUILIBRIO ENTRE COSTO Y SEGURIDAD

¿De qué manera las partes interesadas toman decisiones informadas con respecto a los dispositivos de la Internet de las Cosas considerando la relación costo-beneficio? ¿Cómo se pueden cuantificar y evaluar con precisión los riesgos de seguridad? ¿Qué motivará a los diseñadores y fabricantes de dispositivos para que acepten el costo adicional que implica el diseño de dispositivos más seguros, y, en particular, para que asuman la responsabilidad por el impacto de cualquier externalidad negativa derivada de sus decisiones de seguridad? ¿Cómo se van a conciliar las incompatibilidades entre la funcionalidad y la facilidad de uso y la seguridad? ¿Cómo nos aseguramos de que las soluciones de seguridad para la IoT soporten oportunidades para la innovación, sociales y de crecimiento económico?

ESTÁNDARES E INDICADORES

¿Qué papel desempeñan los estándares técnicos y operativos en el desarrollo y despliegue de dispositivos de la IoT seguros y de buen funcionamiento? ¿Cómo se pueden identificar y medir las características de seguridad de los dispositivos de la IoT? ¿Cómo se puede medir la efectividad de las iniciativas y medidas de seguridad en la Internet de las Cosas? ¿Cómo se puede asegurar la implementación de las mejores prácticas de seguridad?

CONFIDENCIALIDAD DE LOS DATOS, AUTENTICACIÓN Y CONTROL DE ACCESO

Cuál es el papel óptimo del cifrado de los datos con respecto a los dispositivos de la IoT? ¿Utilizar tecnologías de cifrado, autenticación y control de acceso en los dispositivos de la IoT es una solución adecuada para evitar intentos de espionaje y secuestro de los flujos de datos que producen estos dispositivos? ¿Qué tecnologías de cifrado y autenticación se podrían adaptar para la Internet de las Cosas y cómo se podrían aplicar considerando las limitaciones de costo, tamaño y velocidad de procesamiento de los dispositivos de la IoT? ¿Cuáles son los problemas de gestión que se espera deberán ser abordados como resultado del cifrado a una escala de la magnitud de la IoT? ¿Se están abordando las preocupaciones con respecto a cómo gestionar el ciclo de vida de las claves criptográficas y el período durante el cual se espera que un algoritmo dado permanezca seguro? ¿Los procesos de extremo a extremo son lo suficientemente seguros y simples como para que los utilicen los usuarios típicos?

CAPACIDAD DE ACTUALIZACIÓN EN CAMPO

Dado que se espera que muchos de los dispositivos de la IoT tendrán una vida útil prolongada, ¿estos dispositivos deben diseñarse considerando su mantenimiento y su capacidad de actualización in situ de modo que puedan adaptarse a las nuevas amenazas a la seguridad? Si cada dispositivo tiene integrado un agente de gestión de dispositivos, en los dispositivos de la IoT se podría instalar y configurar nuevos software. Pero los sistemas de gestión aumentan los costos y la complejidad; ¿habrá otros enfoques para actualizar el software de los dispositivos que sean más compatibles con el uso masivo de los dispositivos de la IoT? ¿Existe alguna clase de dispositivos de bajo riesgo y que por lo tanto no justifique este tipo de características? En general, ¿las interfaces de usuario de los dispositivos de la IoT (por lo general mínimas) se están analizando adecuadamente, tomando en cuenta la gestión de los dispositivos (por parte de cualquier persona, incluso por el usuario)?

RESPONSABILIDAD COMPARTIDA

¿Cómo se puede fomentar la responsabilidad compartida y la colaboración entre todas las partes interesadas en pos de la seguridad de la IoT?

Antecedentes de la privacidad en la Internet de las Cosas

El respeto por las expectativas y los derechos de privacidad es fundamental para asegurar la **confianza** en Internet; además, también afecta la capacidad de las personas de **hablar, conectarse** y **escoger** de formas significativas. Estos derechos y expectativas se suelen enmarcar en términos del manejo ético de los datos,⁶³ que hace hincapié en la importancia de respetar las expectativas de privacidad del individuo y el uso legítimo de sus datos. La Internet de las Cosas puede desafiar estas tradicionales expectativas de privacidad.

Es fundamental abordar estos tipos de problemas de privacidad, dado que tienen implicaciones sobre nuestros derechos básicos y nuestra capacidad colectiva de confiar en Internet.

La IoT suele referirse a una amplia red de dispositivos con sensores diseñados para recopilar datos acerca de su entorno, que muchas veces incluyen datos relacionados con las personas. Estos datos presumiblemente proporcionan un beneficio al propietario del dispositivo, pero muchas veces también benefician al fabricante o proveedor. La recopilación y el uso de los datos se convierte en una consideración de privacidad cuando las expectativas de privacidad de quienes son observados por los dispositivos de la IoT difieren de las de quienes recogerán y usarán estos datos.

También hay combinaciones de flujos de datos de la IoT aparentemente inocentes que también pueden poner en riesgo la privacidad. Cuando se combinan o correlacionan flujos de datos individuales, el retrato digital que se obtiene de las personas suele ser más invasivo que el que se puede obtener a partir de un flujo de datos individual. Por ejemplo, un cepillo de dientes con conexión a Internet puede recoger y transmitir información sobre los hábitos de cepillado de una persona, algo bastante inocuo. En cambio, si el refrigerador de este mismo usuario informa el listado de los alimentos que consume, y si

además el dispositivo que el usuario utiliza para llevar cuenta de su actividad física también informa los datos correspondientes, la combinación de estos flujos de datos pinta una descripción mucho más detallada y privada de la salud general de la persona. Este efecto de agregación de los datos puede ser particularmente potente en el caso de los dispositivos de la IoT, dado que muchos producen otros metadatos como por ejemplo marcas de tiempo e información de geolocalización, lo que aumenta aún más la especificidad del usuario.

En otras situaciones, el usuario puede no ser consciente de que un dispositivo está recogiendo datos sobre su persona y potencialmente compartiéndolos con terceros. Este tipo de recolección de datos es cada vez más frecuente en los dispositivos de consumo, como por ejemplo en los televisores inteligentes y las consolas de videojuegos. Este tipo de productos tienen características de reconocimiento de voz o de visualización que permanentemente escuchan las conversaciones u observan la actividad en una habitación y selectivamente transmiten los datos recogidos a un servicio en la nube para su procesamiento, donde a veces participa un tercero. Una persona podría estar en presencia de este tipo de dispositivos sin saber que sus conversaciones o actividades están siendo monitoreadas o que sus datos están siendo registrados. Estos tipos de características pueden ser de beneficio para un usuario informado, pero pueden plantear un problema de privacidad para quienes no son conscientes de la presencia de estos dispositivos y no pueden influir significativamente sobre la forma en que se utiliza la información recogida.

Sin importar si el usuario está al tanto de que los dispositivos de la IoT recogen y analizan sus datos, estas situaciones ponen de relieve el valor que tienen estos flujos de datos personalizados para empresas y organizaciones que buscan recoger y sacar provecho de la información obtenida a través de la Internet de las Cosas. La demanda de esta información deja al descubierto los desafíos legales y regulatorios que enfrentan las leyes de protección de datos y privacidad.

Es fundamental abordar estos tipos de problemas de privacidad, dado que tienen implicaciones sobre nuestros derechos básicos y nuestra

capacidad colectiva de confiar en Internet. Desde una perspectiva más amplia, las personas reconocen que su privacidad es un valor intrínseco y tienen expectativas con respecto a los datos personales que se pueden recoger y cómo estos datos pueden ser utilizados por terceros. Esta noción general acerca de la privacidad también vale para los datos recogidos por los dispositivos de la Internet de las Cosas,

pero estos dispositivos pueden socavar la capacidad del usuario de expresar y hacer cumplir sus preferencias de privacidad. Si el hecho de que sus preferencias de privacidad no sean respetadas por la Internet de las Cosas hace que los usuarios pierdan su confianza en Internet, entonces podría disminuir el mayor valor que tiene la Internet.

Aspectos relacionados con la privacidad que solo se aplican a la Internet de las Cosas

En general, la forma en que la Internet de las Cosas aumenta la viabilidad y el alcance de la vigilancia y el seguimiento amplifica las preocupaciones relativas a la privacidad. Las características de los dispositivos de la IoT y las formas en que se utilizan redefinen el debate sobre los temas de privacidad, ya que modifican drásticamente cómo se recogen, analizan, utilizan y protegen los datos personales. Por ejemplo:

El tradicional modelo de privacidad de "notificación y consentimiento" en que los usuarios hacen valer sus preferencias de privacidad interactuando directamente con información que aparece en la pantalla de una computadora o dispositivo móvil (por ejemplo, haciendo clic en "Acepto") deja de funcionar cuando los sistemas no le ofrecen al usuario ningún mecanismo de interacción. Muchas veces los dispositivos de la IoT no tienen una interfaz de usuario para configurar las preferencias de privacidad, y en muchas configuraciones los usuarios no tienen conocimiento ni controlan la forma en que se recogen y utilizan sus datos personales. Esto provoca una brecha entre las preferencias de privacidad del usuario y el comportamiento de recolección de datos del dispositivo. Si consideran que los datos recopilados no son datos personales, es posible que los proveedores de dispositivos de la IoT se sientan menos incentivados a ofrecer a los usuarios un mecanismo para que expresen sus preferencias de privacidad. Sin embargo, la experiencia demuestra que, en realidad, los datos que tradicionalmente no se consideran

personales podrían ser o convertirse en datos personales si se combinan con otros.

Suponiendo que se pudiera desarrollar un mecanismo eficaz que permitiera que un usuario expresara de manera informada sus preferencias de privacidad, este mecanismo debería poder manejar la gran cantidad de dispositivos de la IoT que debe controlar cada usuario. No es realista pensar que un usuario interactuará directamente con cada uno de los dispositivos con que se encuentre a lo largo del día para expresar sus preferencias de privacidad. Por el contrario, las interfaces de privacidad se deben poder escalar de acuerdo con el tamaño del problema, sin dejar de ser completas y prácticas desde la perspectiva del usuario.

La Internet de las Cosas puede poner en peligro las expectativas de los usuarios con respecto a la privacidad en situaciones comunes. Las normas sociales y expectativas de privacidad difieren en los espacios públicos

frente a los espacios privados; los dispositivos de la IoT desafían estas normas. Por ejemplo, las tecnologías de vigilancia que utiliza la IoT como las cámaras de vigilancia o los sistemas de trazabilidad de ubicación que normalmente funcionan en espacios públicos están migrando hacia espacios tradicionalmente privados como el hogar o los vehículos particulares, donde nuestras expectativas de privacidad son muy diferentes. Al hacerlo, desafían lo que muchas sociedades reconocen como el derecho a la privacidad en el hogar o los espacios privados. Además, las expectativas de las personas con respecto a su privacidad en los espacios que consideran públicos (parques, centros comerciales, estaciones de tren, etc.) también están siendo desafiadas por el aumento de la naturaleza y el alcance de la vigilancia en tales espacios.

Muchas veces los dispositivos de la IoT funcionan en contextos donde la proximidad expone a múltiples personas a una misma actividad de recolección de datos. Por ejemplo, el sensor de seguimiento por geolocalización de un automóvil podría registrar los datos de localización de todos los ocupantes del vehículo, sin importar si estas personas desean que lo haga o no. Incluso podría realizar un seguimiento de las personas que viajan en

otros vehículos cercanos. En este tipo de situaciones podría ser difícil o imposible distinguir —mucho menos respetar— las preferencias de privacidad individuales.

El análisis de datos personales consolidados a gran escala de por sí representa un riesgo sustancial de invasión a la privacidad y potencial discriminación. Este riesgo se amplifica en la Internet de las Cosas debido a la escala y a la mayor intimidad de la recolección de datos personales. Los dispositivos de la IoT pueden recoger información personal con un grado de especificidad y penetración sin precedente; agregar y correlacionar estos datos permite crear perfiles personales detallados que general un potencial para la discriminación y otros daños. La sofisticación de esta tecnología puede crear situaciones que expongan al individuo a daños físicos, penales, financieros o de reputación.

La ubicuidad, familiaridad y aceptación social de muchos dispositivos de la IoT pueden crear una falsa sensación de seguridad y alentar a las personas a divulgar información confidencial o privada sin pleno conocimiento o apreciación de las posibles consecuencias.

Preguntas relacionadas con la privacidad de la Internet de las Cosas

Estas preguntas referidas a la privacidad serían un desafío incluso si estuvieran bien alineados los intereses y motivaciones de todas las partes involucradas en el ecosistema de la IoT. Sin embargo, sabemos que las relaciones y los intereses de quienes están expuestos a la recolección de sus datos personales y quienes agregan, analizan y utilizan los datos pueden ser desequilibrados o injustos. La fuente de datos puede ver una intrusión no deseada a su espacio privado, muchas veces sin consentimiento, control, elección o incluso conciencia. No obstante, quien recoge los datos podría considerarlos un

recurso beneficioso que puede añadir valor a sus productos y servicios y proporcionar nuevas fuentes de ingresos.

Dado que la Internet de las Cosas desafía nuestras nociones de privacidad de formas nunca antes vistas, al reevaluar los modelos de privacidad en línea en el contexto de la IoT es necesario responder ciertas preguntas clave. Algunas de las preguntas que se han planteado incluyen las siguientes:

LEGITIMIDAD EN LA RECOPIACIÓN Y EL USO DE LOS DATOS

En el contexto de la IoT, ¿cómo se resuelve la relación de mercado entre las fuentes de los datos y quienes los recogen? Los datos personales tienen un valor personal y comercial diferente según se consideren desde el punto de vista de las fuentes o de los recolectores, tanto individualmente como en su conjunto; por lo tanto, ambas partes tienen intereses legítimos que podrían estar en conflicto. ¿Cómo se pueden expresar estos diferentes intereses de una manera que conduzca a reglas en materia de acceso, control, transparencia y protección que sean justas y consistentes, tanto para las fuentes como para los recolectores?

TRANSPARENCIA, EXPRESIÓN Y CUMPLIMIENTO DE LAS PREFERENCIAS DE PRIVACIDAD

¿Cómo se puede hacer que las políticas y prácticas de privacidad sean de fácil acceso y comprensibles en el contexto de la IoT? ¿Cuáles son las alternativas al modelo tradicional de privacidad de "notificación y consentimiento" que podrían abordar los aspectos únicos de la Internet de las Cosas? ¿Cuál sería un modelo eficaz para expresar, aplicar y hacer cumplir las preferencias de privacidad individuales y las preferencias multipartitas? ¿Se podría construir un modelo multipartito de este tipo? De ser así, ¿qué aspecto tendría? ¿Cómo se podría aplicar a circunstancias concretas que impliquen las preferencias de privacidad individuales? ¿Existe un mercado para tercerizar la gestión de la configuración de la privacidad a servicios comerciales diseñados para implementar las preferencias de los usuarios? ¿Es necesario que exista un proxy de privacidad que exprese y haga cumplir las preferencias del usuario a través de una serie de dispositivos, al tiempo que elimine la necesidad de interacción directa con cada uno de ellos?



La aplicación de los dispositivos de la IoT plantea una variedad de desafíos y preguntas sobre aspectos regulatorios y legales que deben ser considerados cuidadosamente. En algunos casos, los dispositivos de la IoT dan lugar a nuevas situaciones legales y regulatorias y generan preocupaciones con respecto a los derechos civiles que antes no existían. En otros casos, estos dispositivos magnifican cuestiones legales que ya existían. Además, la tecnología está avanzando a una velocidad mucho mayor que los entornos regulatorios y de políticas relacionados. A continuación se discuten algunos potenciales problemas regulatorios y legales que afectan a todo el espectro de aplicaciones de la IoT.

Protección de datos y flujos de datos transfronterizos

No se puede evitar que los datos que recogen los dispositivos de la IoT se envíen a través de los límites jurisdiccionales. Estos dispositivos utilizan Internet para comunicarse e Internet atraviesa límites jurisdiccionales a todo nivel. Los dispositivos de la IoT pueden recoger datos sobre las personas en una jurisdicción y transmitirlos a otra para su almacenamiento o procesamiento, muchas veces sin mayores obstáculos técnicos. Esto puede convertirse rápidamente en un problema legal, por ejemplo, si los datos recogidos se consideran datos personales o datos sensibles y están sujetos a las leyes de protección de datos de múltiples jurisdicciones. Para complicar aún más las cosas, las leyes de protección de datos en la jurisdicción donde residen el dispositivo y el titular de los datos podría ser inconsistente o incompatible con las leyes de la jurisdicción donde los datos se almacenan y procesan.

Estas situaciones se describen como flujos de datos transfronterizos y plantean preguntas con respecto al alcance jurídico de las normas que podrían ser aplicables. En otras palabras, ¿cuál régimen legal regula el dispositivo que recoge los datos y cuál regula el almacenamiento y el uso de los datos recogidos? Este escenario también

La Internet de las Cosas plantea nuevas preguntas regulatorias y legales y puede amplificar los desafíos legales que ya existen en torno a Internet. Promover la capacidad de los usuarios para conectarse, hablar, innovar, compartir, elegir y confiar es una consideración fundamental para la evolución de leyes y reglamentos.

plantea preguntas normativas. ¿Se pueden modificar estas leyes para reducir el grado de fragmentación de Internet que provocan y, a la vez, proteger los derechos de los usuarios? Si una jurisdicción tiene leyes de protección de datos más restrictivas en cuanto al manejo y la transmisión de determinados datos provenientes de la IoT, ¿estos requisitos legales se deberían poder proyectar a otras jurisdicciones?

Si bien muchas de estas preguntas sobre los flujos de datos transfronterizos ya se han

planteado y abordado en el marco del tráfico de datos de la Internet tradicional,⁷⁸ los dispositivos de la IoT plantean un nuevo desafío en este sentido. Cada vez más, estos dispositivos podrán conectarse automáticamente a otros dispositivos y sistemas y transmitir información a través de las fronteras sin el conocimiento del usuario. Esto

podría crear situaciones en las que un usuario se podría convertir en responsable de cumplir con los requisitos aplicables a los flujos de datos transfronterizos, incluso sin saber que esto está ocurriendo. Estos son temas complejos y lo serán cada vez más, ya que la tecnología sigue avanzando más rápido que las políticas.

Discriminación de los datos de la IoT

Los datos recogidos por los dispositivos de la IoT permiten formar una imagen detallada de las personas con que interactúan y estos datos pueden ser utilizados tanto para fines beneficiosos como para fines discriminatorios. Consideremos el caso de los dispositivos que se utilizan para llevar registro de la actividad física. Muchas veces una persona lleva uno de estos dispositivos de forma permanente durante un período de días o semanas; durante todo este tiempo, el dispositivo recoge información muy detallada sobre los movimientos de la persona y otros datos biométricos. Una aplicación analiza estos datos para determinar el estado físico de la persona, estimar las calorías que quema, llevar un registro de las horas de sueño y caracterizar la calidad del sueño. Este análisis es claramente beneficioso para el usuario, ya que le ofrece una manera de cuantificar su actividad física mientras intenta alcanzar un objetivo de pérdida de peso o aptitud física.

Pero estos mismos datos se pueden utilizar en formas potencialmente discriminatorias. En Estados Unidos, algunos planes de seguro médico están incentivando a los participantes para que permitan que el asegurador acceda a los datos del dispositivo a cambio de primas de seguro más bajas.⁷⁹ Esta práctica puede ser vista como positiva: ofrecer precios preferenciales a quienes estén dispuestos a entregar sus datos biométricos a cambio de un descuento. Por otra parte, potencialmente podría ser discriminatoria, en especial para quienes se encuentran en desventaja económica. En palabras de un comentarista:

Imaginemos un esquema de precios [de pólizas de seguros] que castiga a los padres solteros privados de sueño o a los hábitos alimenticios de los trabajadores más pobres. Los incentivos financieros para permitir que las aseguradoras y otros interesados accedan a la información sobre su salud podrían

Los datos que recogen los dispositivos de la IoT permiten formar una imagen detallada de las personas con que interactúan. Estos datos pueden ser utilizados para propósitos y productos muy valiosos que benefician a los usuarios. Sin embargo, estos mismos datos podrían ser utilizados en forma discriminatoria.

llegar a ser tan convincentes que “escoger” participar sería la única opción viable.⁸⁰

Los escenarios como este son cada vez más frecuentes. Los vehículos más nuevos están equipados con transpondedores equipados con GPS y enlaces de datos que comunican información de geolocalización y hábitos de conducción (por ejemplo, excesos de velocidad y fuerza de frenado) a sistemas remotos, o que se utilizan para proporcionar asistencia o servicios de viaje al conductor. Si bien estas características le proporcionan ventajas al usuario, los datos podrían llegar a ser utilizados en formas potencialmente discriminatorias. Por ejemplo, los operadores de flotas pueden utilizar estos datos para monitorear el desempeño de sus conductores sin que los conductores puedan optar por no ser observados. Estos son ejemplos bastante directos de cómo se pueden utilizar los datos de la IoT de forma discriminatoria, pero no queda claro cómo se podrían utilizar las diferentes combinaciones de datos para discriminar en el futuro.

Además, la calidad, la especificidad y el volumen de los datos producidos por la IoT podría magnificar el potencial de que se generen prácticas de precios discriminatorias y servicios ilegítimos. Con frecuencia los datos de la IoT se pueden etiquetar con metadatos (marcas de fecha y de tiempo, etiquetas de geolocalización) que aumentan dramáticamente la calidad de los datos desde el punto de vista de su análisis. Además, los sensores de la IoT suelen realizar muy pocas funciones. Esto significa que los datos de los sensores suelen asociarse con una situación operativa específica, que permite un alto grado de especificidad a la hora de correlacionar los datos con una persona o con un grupo de personas. De hecho, el dispositivo se podría llegar a asociar con la persona en la que está implantado, como en el caso de un marcapasos o una bomba de insulina conectados a Internet. En otros casos, este nivel de especificidad no es deseable y accidentalmente puede provocar resultados discriminatorios. Los sensores de la IoT pertenecientes o gestionados por terceros pueden recoger datos identificables sobre las personas sin su conocimiento o consentimiento. Estos datos se podrían utilizar de formas que perjudicarían a la persona monitoreada.

Por último, estos dispositivos crean importantes flujos de datos continuos sin intervención humana. La combinación de estas cualidades hace que los análisis de los datos de la IoT sean muy descriptivos y útiles para la investigación, el desarrollo de productos y también en otras áreas. Los algoritmos de *Big Data* pueden examinar cantidades enormes de datos y buscar correlaciones estadísticas y semánticas

para así determinar grupos de usuarios con características afines. A su vez, estos algoritmos podrían categorizar injustamente a los usuarios y explotar sus características.

Este tipo de usos de los datos de la IoT plantea cuestiones prácticas, legales y reglamentarios. En primer lugar, ¿cómo podemos detectar las prácticas discriminatorias o injustas contra los usuarios? ¿Existen prácticas discriminatorias virtualmente imposibles de detectar? ¿Existe alguna diferencias legal en caso que la decisión de discriminar sea tomada por una persona o por una máquina? El desarrollo de herramientas para detectar prácticas algorítmicas injustas es un desafío para la investigación académica, sobre todo porque la mayoría de los algoritmos de análisis de datos son secretos empresariales y no son del dominio público. ¿Cómo podemos equilibrar los enormes beneficios comerciales y sociales del análisis de datos de la IoT con la probabilidad de que se generen prácticas discriminatorias contra los usuarios? ¿Cómo podemos fomentar la adopción de los principios de la innovación sin pedir permiso (*permissionless innovation*) en el ámbito de la IoT y a la vez proteger a los usuarios contra las prácticas ilegítimas? ¿Cómo podemos mejorar la transparencia? ¿Las leyes de privacidad y de protección del consumidor existentes alcanzan para hacer frente a este escenario? ¿Qué recursos deberían estar disponibles en caso de discriminación? ¿Los dispositivos de la IoT se deberían categorizar y regular en función de la naturaleza de los datos que producen, especialmente cuando los datos son propensos a ser mal utilizados?

Los dispositivos de la IoT utilizados como ayudas para las agencias de aplicación de la ley y la seguridad pública

Los dispositivos de la IoT podrían servir como ayudas para las agencias de aplicación de la ley y la seguridad pública, pero en este caso es necesario considerar cuidadosamente las ramificaciones legales y sociales. Indudablemente, los dispositivos de la IoT y los datos que generan pueden ser utilizados como herramientas eficaces para luchar contra el crimen. Muchos comercios minoristas han instalado cámaras de seguridad para recoger imágenes de video y realizar un seguimiento de la actividad de los compradores, algo que ha resultado de gran valor como prueba en los procesos penales y como elemento de disuasión de la delincuencia.⁸¹ Más recientemente, On-Star Corporation, una subsidiaria de General Motors, puede proporcionar datos de los sensores que se encuentran en el automóvil de la policía para ayudar en la recuperación de vehículos robados y puede desactivar de forma remota un vehículo robado.⁸² El Departamento de Policía del Condado de Nassau (Nueva York) utiliza una red de sensores de sonido llamada *ShotSpotter* que permite detectar y localizar la fuente exacta de un disparo en los barrios donde han sido desplegados.⁸³ Todos estos son ejemplos de los beneficios que la tecnología de la Internet de las Cosas puede ofrecer a la policía para combatir la delincuencia y mejorar la seguridad pública.

Sin embargo, el despliegue y uso de este tipo de tecnologías provocan preocupación entre algunos defensores de los derechos civiles y otras personas. Entre las posibles causas de preocupación se incluyen la omnipresencia de las actividades de monitoreo de los datos, las políticas sobre su conservación y destrucción,

los usos secundarios que los gobiernos pueden darles, así como la potencial exposición accidental de los datos a actores maliciosos. Además, se deben considerar cuidadosamente los efectos potencialmente negativos sobre las actividades beneficiosas de las comunidades y sociedades monitoreadas.

Otras situaciones de orden y seguridad públicos son más complejas. Por ejemplo, al lanzar el iPhone 6 y su sistema operativo iOS 8, Apple Corporation eliminó un método de acceso tipo “puerta trasera” que existía en versiones anteriores de su teléfono. La función de puerta trasera permitía a la policía acceder a los datos que se encontraban en el teléfono de un usuario. Apple eliminó esta característica en el nuevo iPhone y ahora encripta el contenido interno del teléfono de una manera difícil de vulnerar y para la cual Apple no tiene las claves, por lo cual no tiene forma de permitir el acceso.⁸⁴ Esto hace que solo el propietario del teléfono pueda acceder a su contenido. Las agencias federales de seguridad sostienen que esto hace que sea más difícil procesar los comportamientos criminales,⁸⁵ mientras que los partidarios de los derechos civiles ven en esto una victoria para la protección de la privacidad de los datos de los usuarios.⁸⁶ Esta controversia con respecto al cifrado de los dispositivos también se aplica a otros dispositivos de la IoT. ¿Qué papel debe desempeñar el cifrado de los dispositivos en la protección de los dispositivos de la IoT contra los ataques criminales? ¿Cómo se puede equilibrar esto con el legítimo acceso a los datos del usuario en interés de la aplicación de la ley y la seguridad pública?

Responsabilidad por los dispositivos de la IoT

Los dispositivos de la IoT plantean interrogantes con respecto a la responsabilidad desde el punto legal que invitan a la reflexión. Una de las preguntas fundamentales subyacentes en lo que respecta a los dispositivos de la IoT es la siguiente: Si alguien se ve perjudicado como consecuencia de la acción u omisión de un dispositivo de la IoT, ¿quién es el responsable? En muchos casos la respuesta es complicada y a veces todavía no existe demasiada jurisprudencia para sustentar una posición determinada. Los dispositivos de la IoT funcionan de forma más compleja que un producto independiente y esto sugiere que será necesario considerar escenarios de responsabilidad más complejos.

Por ejemplo:

Puede que los dispositivos de la IoT sean utilizados en formas nunca previstas por su fabricante. No es razonable suponer que un fabricante de dispositivos pueda realizar pruebas de control de calidad para todos los potenciales casos de uso de los dispositivos de la IoT.

Quizás los dispositivos de la IoT se conecten e interactúen con otros de formas no anticipadas y para las cuales no se realizaron pruebas. A medida que aumente la interoperabilidad, estos dispositivos podrán formar entre sí conexiones de red *ad hoc*. Por lo tanto, antes de desplegar estos dispositivos, es difícil para un fabricante o usuario tener en cuenta todos los escenarios potencialmente perjudiciales que podrían llegar a surgir.

Una vez instalados, estos dispositivos pueden tener una larga vida útil y serán susceptibles a futuras amenazas a la seguridad que hoy en día son desconocidas. Esto significa que estos dispositivos podrían verse comprometidos y ser reprogramados maliciosamente para dañarse a sí mismos o a otros dispositivos, o bien para revelar información sensible en forma no intencionada e inadvertida.

Los dispositivos de la IoT se integrarán en sistemas autónomos (por ejemplo, automóviles sin conductor) que incorporan algoritmos de

aprendizaje adaptativo para controlar su comportamiento sobre la base de la información aportada por los sensores de tales dispositivos. Es imposible conocer y probar con anticipación las acciones de estos sistemas.

Estos y otros escenarios plantean interrogantes. Si uno de uno de estos escenarios genera daños, ¿las leyes de responsabilidad existentes abordan adecuadamente la culpabilidad legal y aclaran la responsabilidad de las partes involucradas? ¿Es necesario repensar las leyes de responsabilidad para los dispositivos inteligentes de la IoT que aprenden de su entorno y se modifican a sí mismos a medida que pasa el tiempo? Si un sistema autónomo recibe instrucciones del usuario y no de sus algoritmos internos, ¿qué pasa en caso de error del usuario? ¿Los dispositivos de la IoT deberían ser lo suficientemente inteligentes como para tener una instrucción de tipo "haz lo que quise decir"? ¿En qué medida se pueden ampliar las leyes de responsabilidad que existen para los productos convencionales de manera que abarquen los productos que se van conectando a Internet? Como comunidad, ¿qué podemos hacer para informar mejor a los legisladores y a los formuladores de políticas de modo que no sean tan susceptibles frente a la enorme cantidad de información errónea y consejos sesgados que reciben? ¿Qué podemos hacer para informar mejor a los usuarios y compradores de estos dispositivos de modo que entiendan todos los factores que afectan su uso?

Proliferación de dispositivos de la IoT utilizados en acciones legales

Los datos que recogen los dispositivos de la IoT muchas veces pueden servir como prueba en una variedad de procedimientos legales. A medida que estos datos se vuelvan más frecuentes, es probable que se utilicen cada vez más en este tipo de procedimientos. Por ejemplo, algunos abogados en Estados Unidos han utilizado durante un juicio de divorcio los datos de hora y localización obtenidos de los dispositivos de peaje electrónico instalados en los automóviles

actúen como garantía en caso de incumplimiento de las obligaciones de pago. Si un conductor no para el *leasing* o el crédito de su automóvil, el arrendatario o prestamista puede inactivar el vehículo de forma remota usando el dispositivo instalado hasta que se realice el pago.⁸⁹ Estos dispositivos ya se han instalado en más de dos millones de automóviles en Estados Unidos.⁹⁰

Este tipo de escenarios plantean nuevas preguntas legales y reglamentarias con respecto a los dispositivos de la IoT. ¿Deberían los fabricantes de dispositivos incluir en estos dispositivos tecnologías como el cifrado para restringir el acceso a los flujos de datos como lo ha hecho Apple en el iPhone? A la inversa, ¿deberían los fabricantes estar diseñando dispositivos de la IoT que faciliten el uso de los datos en un procedimiento judicial? ¿Es necesario desarrollar estándares que especifiquen requisitos de diseño para que los datos de la IoT soporten la cadena de custodia de los datos en los procesos judiciales? ¿Se deberían establecer regulaciones que protejan al consumidor de ciertos dispositivos de la IoT?

proceedings? Are standards needed to specify design requirements for IoT data to support legal chain of custody of data in legal proceedings? Should there be consumer protection regulations placed on certain IoT devices?

Los dispositivos de la IoT funcionan de forma más compleja que un producto independiente y esto sugiere que será necesario considerar escenarios de responsabilidad más complejos.

para demostrar que un cónyuge engañaba al otro.⁸⁷ En 2014, una mujer canadiense utilizó los datos de su propio dispositivo de actividad física en apoyo de su reclamo en una demanda por lesiones personales.⁸⁸

En cuanto a usos más deliberadas de los dispositivos de la IoT para procedimientos legales, en los automóviles se pueden instalar dispositivos conectados a Internet de manera que

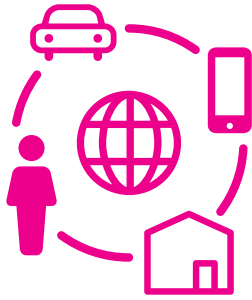
Garantizar que las oportunidades de la IoT sean globales

La propagación y el impacto de Internet tienen un alcance global: ofrecen oportunidades y beneficios a las regiones desarrolladas y las regiones en desarrollo por igual. A la vez, muchas veces en las regiones en desarrollo se plantean desafíos únicos relacionadas con el despliegue, el crecimiento, la implementación y el uso de la tecnología, incluso de Internet. Es razonable esperar que esto también sea válido para los potenciales beneficios y desafíos asociados con la Internet de las Cosas.

Desde la perspectiva de los principios de la Internet Society, creemos que Internet debe ser una fuente de empoderamiento a nivel global, sin importar la ubicación, la región o el estado de desarrollo económico del usuario, y que toda la gama de habilidades y principios⁹⁷ que impulsan nuestro trabajo y el éxito de Internet se aplican a nivel global. Desde los primeros tiempos de Internet, la comunidad técnica, la sociedad civil, las organizaciones gubernamentales y la industria privada, entre otros actores, se han centrado en las oportunidades y los desafíos relacionados con Internet en las economías emergentes. De modo que esto también debería ser cierto con respecto a las oportunidades y desafíos relacionados con la Internet de las Cosas.⁹⁸

La IoT encierra una gran promesa como habilitador del desarrollo social, incluyendo el logro de los Objetivos de las Naciones Unidas para el Desarrollo Sostenible.

CONCLUSIÓN



Aunque el concepto de combinar computadoras, sensores y redes para monitorear y controlar diferentes dispositivos ha existido durante décadas, la reciente confluencia de tecnologías clave y tendencias de mercado está marcando el comienzo de una nueva realidad para la “Internet de las Cosas”.

La IoT promete abrir la puerta a un mundo revolucionario, un mundo “inteligente” totalmente interconectado en el cual las relaciones entre los objetos y su entorno y las personas se entrelazarán aún más. La perspectiva de la Internet de las Cosas como una matriz omnipresente de dispositivos conectados a Internet podría cambiar radicalmente la definición de lo que significa estar “en línea”.

Aunque las potenciales ramificaciones son significativas, hay una serie de problemas que podrían interponerse en el camino de esta visión, particularmente en las áreas de la seguridad; la privacidad; la interoperabilidad y los estándares; temas legales, reglamentarios y de derechos; y la inclusión de las economías emergentes. La Internet de las Cosas implica un complejo conjunto de consideraciones tecnológicas, sociales y políticas en constante evolución y que atraviesa un conjunto diverso de partes interesadas. La Internet de las Cosas está sucediendo ahora mismo, por lo que es necesario hacer frente a sus desafíos, maximizar sus beneficios y simultáneamente reducir sus riesgos.

A la Internet Society le importa la IoT, ya que representa un componente cada vez mayor de la manera en que las personas y las instituciones probablemente interactuarán con Internet e incorporarán la conectividad en sus vidas personales, sociales y económicas. Un debate polarizado que enfrente a las promesas de la IoT contra sus posibles peligros no permitirá encontrar soluciones que maximicen los beneficios de la IoT y a la vez minimicen sus riesgos. Por el contrario, para definir las formas más eficaces de avanzar, se necesitará la participación informada, el diálogo y la colaboración de una variedad de partes interesadas.

Manual de instalación de prototipo inteligente de luminarias

En este manual encontraremos las recomendaciones y las herramientas Qué necesitamos para hacer una instalación de manera segura y funcional

Dentro de las herramientas que necesitaremos está

1 desarmador Phillips



Figura 1: Desarmador Phillips

1 desarmador plano



Figura 2: Desarmador Plano

Una tabla de madera



Figura 3: Tabla de madera

Un tomacorriente



Figura 4: Tomacorriente

1 interruptor de dos puntos



Figura 5: Interruptor de dos puntos

Un foco LED



Figura 6: Foco LED

Cable eléctrico calibre número 14



Figura 7: Cable eléctrico calibre 14

Un arduino wemos D1



Figura 8: Arduino wemos d1

Un relay



Figura 9: Relay

Una fuente de 5 voltios



Figura 10: Fuente de 5 voltios

Un cable mini usb



Figura 11: Cable mini USB

tenaza eléctrica



Figura 12: tenaza eléctrica

Tornillos



Figura 13: tornillos

Una computadora portátil



Figura 14: Computadora portátil

Un celular



Figura 15: Celular

Un router



Figura 16: Router

Instalación de Arduino al ordenador portátil y móvil

Pasó 1

En este paso necesitará conectar la fuente de 5 voltios hacia el arduino wemos D1 con esto verificaremos si llega la electricidad desde la Fuente hacia el arduino wemos D1.

Pasó 2

Conecta el arduino con el cable mini usb Asia el portátil y verifica que el portátil reconozca el arduino e instale los controladores que el sistema operativo brinda.

Pasó 3

Descargue la aplicación de blynk para Android o IOS. Desde la página web <https://www.blynk.cc/> o desde play store en Android y app store para iphone

Pasó 4

Para conectar la aplicación blynk y el Hardware se necesita un AUTH TOKEN (NUMERO DE AUTORIZACION).

Después crearemos en aplicación un nuevo proyecto la cual enviaremos un toque hacia nuestro correo electrónico donde Tendremos que revisar nuestra bandeja de entrada del correo electrónico para poder abrir el token de autenticación.

Pasó 5

Debemos descargar la biblioteca de blynk y se tiene que instalar manualmente a la computadora portátil Tendremos que descargar la última versión de un archivo comprimido luego Tendremos que descomprimirlo y copiar las bibliotecas en el sketchbook de arduino después de tener la librería lista Tendremos que pegar el toque de autenticación en el sketchbook.

<https://www.blynk.cc/>

<https://www.blynk.cc/getting-started/>

Pasó 6

Tenemos conexión entre el arduino wemos D1 con la aplicación blynk la cual permitirá tener acceso hacia el router automáticamente con esto podemos tener conexión inalámbrica mente desde el router hacia el arduino.

Instalación física del Arduino a la red eléctrica.

Pasó 7

Colocamos el relay al arduino.

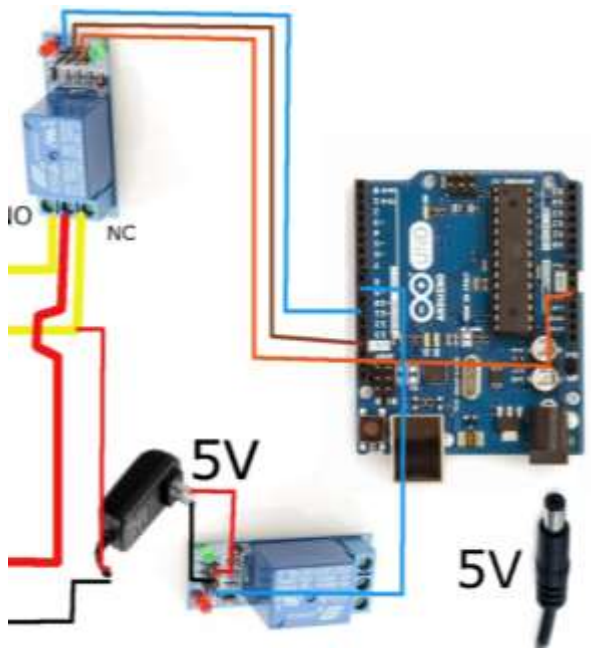


Figura 17: conexión de relay al arduino

Pasó 8

Colocamos el relay hacia el interruptor de doble vía.



Figura 18: conexión de relay hacia interruptor de doble vía

Pasó 9

Conectamos el interruptor hacia la luminaria LED.

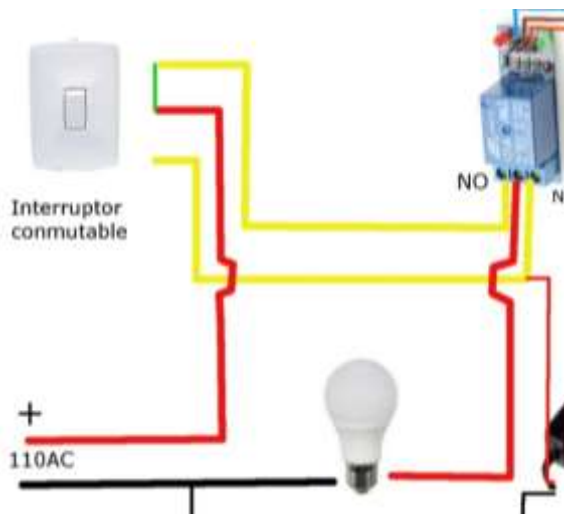


Figura 19: conexión de interruptor hacia luminaria LED

Pasó 10

Instalar el relay hacia el tomacorriente 120 voltios a través de una extensión desde la maqueta hacia el tomacorriente de pared.

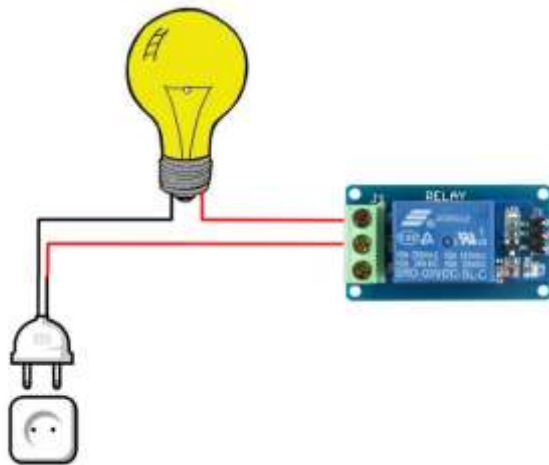


Figura 20: Conexión de relay hacia corriente 120 voltios

Pasó 11

Procedemos a abrir la aplicación blynk en nuestro móvil. Ya en la aplicación deberá crear y asignarle nombre al nuevo proyecto. Se tiene que seleccionar el tipo de Arduino que se utiliza en el proyecto. También tendremos que asignar el tipo de conexión que tendrá y deberá de ser internet .luego se preciona el botón CREATE(crear)



Figura 21: Creación de proyecto

Luego aparece una ventana llamada widget box. Que significa caja de elementos. Ahí seleccionaremos el boton

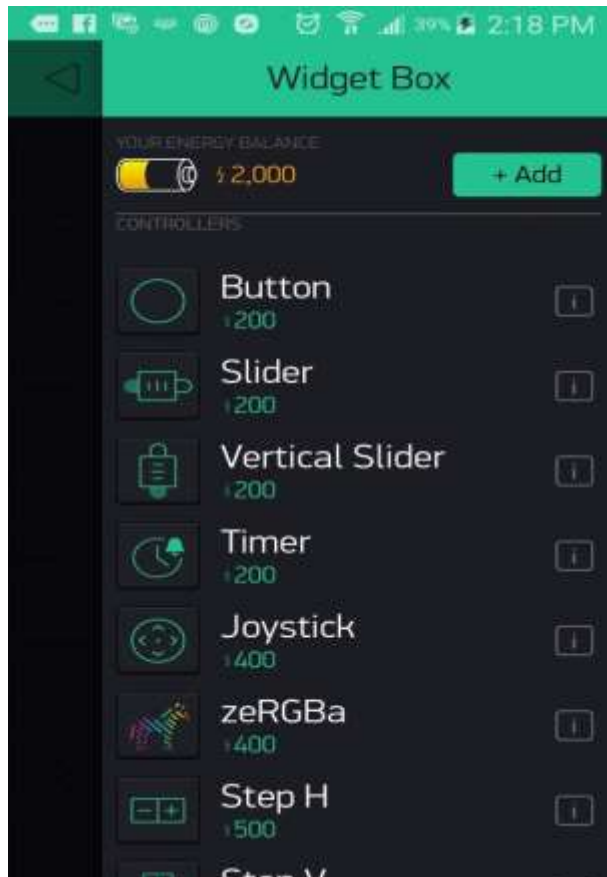


Figura 22: Widget box

Tendremos que configurar el botón seleccionado en este caso será asignado en el d2 de nuestra placa de Arduino y 0 apagado y 1 como encendido seleccionaremos el método de encendido como switch

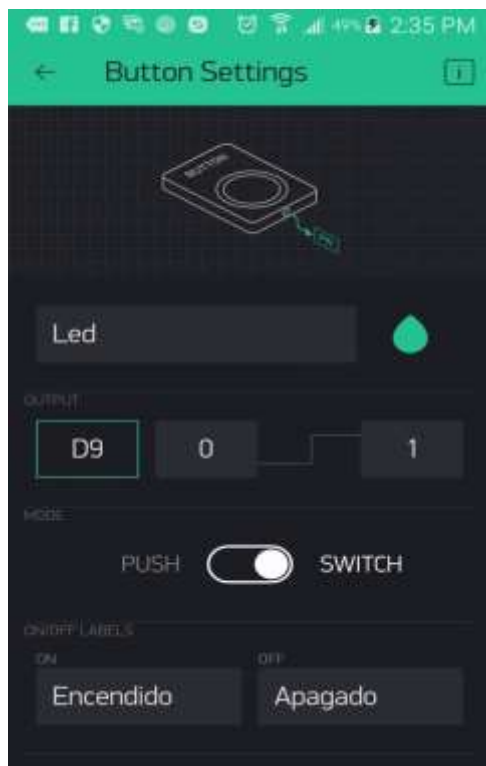


Figura 23: Configuración de botones

Pasó 12

Movemos el switch de On a Off en la aplicación para poder apreciar que enciende y apaga la luminaria LED de nuestro producto.



Figura 24: Manejo de botones