Vulnerabilidades de las Redes IoT

Edgar Antonio Casarrubias Márquez
Facultad de Ingeniería
Av. Lázaro Cárdenas. S/N, Chilpancingo, Guerrero
7471264102. 39079
edancam@gmail.com

José Fernando Castro Domínguez
Facultad de Ingeniería
Av. Lázaro Cárdenas. S/N, Chilpancingo, Guerrero
7331161138. 39079
17808@uagro.mx

Rogelio Fernando Hernández Alarcón
Facultad de Ingeniería
Av. Lázaro Cárdenas. S/N, Chilpancingo, Guerrero
7471212159. 39079
15529@uagro.mx

Jorge Vázquez Galarce.
Facultad de Ingeniería
Av. Lázaro Cárdenas. S/N, Chilpancingo, Guerrero
7471243942. 39079
13216@uagro.mx

RESUMEN

IoT es un concepto tan amplio, ya que afecta a la sociedad, a las empresas y a la economía, se describe como el suceso en el que los dispositivos que usualmente utilizamos se conectan a Internet, de esta manera se logra conectar entre sí, personas y cosas, además, recopilar datos y procesarlos los cuales estan expuestos a una serie de vulnerabilidades que se pueden deber principalmente a errores de configuración de las redes donde se conectan o de los mismo dispostivos IoT, en el presente artículo se describen las buenas prácticas que se deben considerar durante su implemnetación para mitigar las amenzas y vulnerabilidades a las que pudieran estar expuestas.

Palabras reservadas

IoT, conectividad, vulnerabilidades, phishing, ransomware, ciberseguridad.

INTRODUCCIÓN

La vida cotidiana tuvo un cambio radical gracias a una revolución, llamada Internet of Things o Internet de las Cosas. El objetivo es que todo lo que este a su alrededor esté conectado, no solo su computadora o su Smartphone, sino también cualquier otro dispositivo como electrodomésticos o su automóvil, incluso su hogar u oficina, y en mayor escala, ciudades completas.

Este artículo se constituye de un total de tres capítulos, en el capítulo uno se describe el funcionamiento de la tecnología IoT, desde las redes más utilizadas hasta su estructura por niveles, además de los proveedores de plataformas y las áreas de aplicación más populares. En el segundo capítulo encontraremos las vulnerabilidades que llegan a presentarse en los dispositivos IoT, además de los tipos de ataques que realizan los ciberdelincuentes a estos, y mencionaremos algunos de los dispositivos que sufrieron ataques a gran escala. Para finalizar en el capítulo tres, describimos la estructura de ciberseguridad por capas, también mencionaremos las tres empresas especializadas en ciberseguridad, además de sugerir buenas prácticas para el usuario para aumentar la seguridad de dispositivos IoT.

1.- FUNCIONAMIENTO DE LAS REDES IOT

En los últimos años, las tecnologías IoT se han desarrollado en gran medida, la idea es que todo esté conectado, haciendo posible la comunicación de dispositivos, tales como vehículos, SmartTvs, SmartBands, lo que los hace capaces de tener una conexión a Internet. Gracias a esto, es por lo que actualmente es posible la comunicación fluida entre personas, procesos y cosas. La conectividad está presente en los diferentes aparatos electrónicos de uso cotidiano, tanto en el hogar como en la empresa, y que se les ha incorporado al hardware interno una conexión a Internet, la cual permite la transmisión de datos, entre otras funciones, tales como poder trabajar de manera remota haciendo actividades desde el hogar o incluso desde cualquier lugar.

De esta forma las tecnologías IoT son muy significativas para el uso diario, además se ha desarrollado la comunicación entre las maquinas (m2m), lo que permite que puedan comunicarse entre ellas, en caso de que ocurra alguna avería. También nos han mostrado grandes avances de monitoreo en los dispositivos que se utilizan en el área de la salud, ya que la tecnología IoT nos permite recolectar datos, y mandarlos a la red, de esta manera, los datos estarán siempre disponibles para ser visibles en las plataformas, o en cualquier otro caso, los enviaría a otro dispositivo para ser procesados. En la tecnología IoT, los dispositivos [1] se conectan a través de puertas de enlace de funcionalidad integrada, las puertas de enlace conectan los dispositivos IoT a la nube.

Todos los datos que se recopilan por los dispositivos IoT se mueven por la puerta de enlace, la antes mencionada procesa los datos y los envía a la nube donde se preparan para ser enviados a su respectivo destino.

En los tipos de redes, la conectividad que se necesita para que los dispositivos funcionen, depende de la función que los usuarios le darán, es decir, que normalmente son influenciados por la distancia que deben viajar los datos, esto determina el tipo de conectividad que se usaran, por este motivo podemos separar las redes que se usan normalmente [1] en redes de corto alcance y redes de largo alcance.

Cuando hablamos de conectividad de las tecnologías IoT tenemos que tener en cuenta que se utilizan redes como el Wifi u otro tipo, que nos permitan conectar los dispositivos a una red que nos sea factible manejar para enviar datos de manera rápida y segura, encontraremos algunos ejemplos en la Tabla 1.1.

Tabla 1.1 Redes más usadas en los proyectos IoT

Corto alcance	**Largo alcance**
Redes Wifi	Red LoRaWAN.
Red Zigbee	Red 4g Lite para IoT
Red Z-Wave.	Red 5g.
Bluetooth.	Red Sigfox

La tecnología IoT utiliza diferentes protocolos de comunicación [1], tanto en el área industrial como en el área doméstica. ¿Pero qué son los protocolos? Estos son el conjunto de reglas que determinan como se envían los datos a internet. En los proyectos IoT los protocolos garantizan que un dispositivo lea mediante sensores integrados y procese los datos recolectados. La empresa Microsoft clasifica por niveles los protocolos que se emplean en las redes IoT, como se ilustra en la Tabla 1.2.

Tabla 1.2 Protocolos empleados en redes IoT.

Niveles	Características	Ejemplo
Aplicación	El nivel de aplicación actúa como interfaz entre el usuario y el dispositivo.	Advanced Message Queuing Protocol (AMQP), Servicio de distribución de datos (DDS)
Transporte	El nivel de transporte habilita y protege la comunicación de los datos a medida que viajan entre niveles.	Protocolo de control de transmisión (TCP, Protocolo de datagramas de usuario (UDP)
Red	El nivel de red permite la comunicación entre los dispositivos individuales y el enrutador.	6LoWPAN, IPv6
Vinculo de datos	El nivel de datos transfiere los datos dentro de la arquitectura del sistema e identifica y corrige los errores que encuentra en el nivel físico.	IEEE 802.15.4, LPWAN
Físico	El nivel físico establece un canal de comunicación que permite que los dispositivos se conecten dentro de un entorno especificado.	Wi-Fi/802.11, Identificación por radiofrecuencia (RFID)

Hasta este momento, el mercado de plataformas de IoT [6] tiene cambios constantes, surgen nuevos proveedores, los líderes tienen cada vez más competencia, y cada vez más adversarios, entre los años 2019 y 2020 había 620 plataformas IoT a nivel mundial y el numero está en constante crecimiento, podemos observar algunos ejemplos de plataformas en la Figura 1.1.

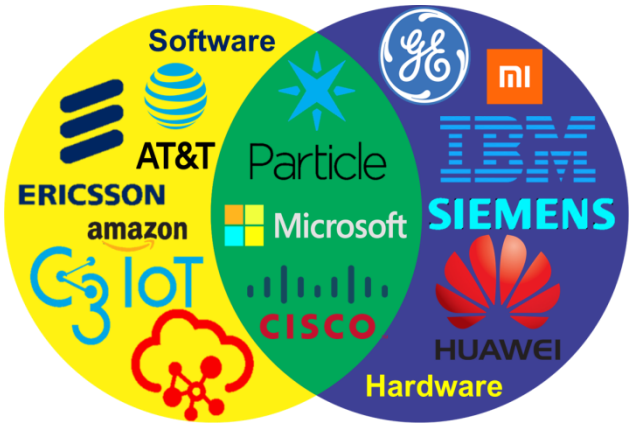

Figura 1.1 Proveedores de plataformas IoT por IoT Analytics.

Como se menciona existen muchas empresas que ofrecen plataformas IoT, pero dentro de esa gran variedad tenemos varias clasificaciones, cada plataforma desarrolla Software o Hardware, según sea lo que el proyecto requiera, nos encontraremos con opciones. Las plataformas son las piezas centrales en IoT [4], ya que conectan los mundos real y digital, lo que permite la comunicación entre dispositivos, administrar el flujo de datos, desarrollo de aplicaciones y análisis de la información recopilada por los dispositivos IoT conectados. Existen muchas empresas que son proveedores de plataformas IoT a nivel mundial, mencionaremos algunas en la Figura 1.2.

Figura 1.2 Clasificación de plataformas IoT por SECMOTIC.

Ahora es momento de hablar sobre las 5 áreas donde se desarrollan la mayoría de proyectos IoT a nivel mundial [14] en el año 2020 según estudios de IoT Analytics, las cuales se ilustran en la Figura 1.3.

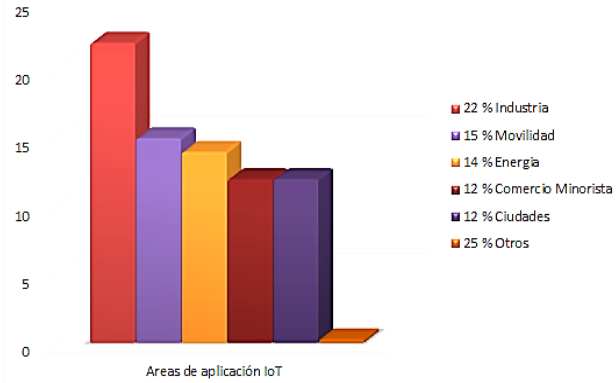

Figura 1.3 Las 5 áreas populares de desarrollo de proyectos IoT.

2.- VULNERABILIDADES

Actualmente la creciente demanda ha incrementado el número de dispositivos que se conectan a internet, la mayoría de las personas cuentan con un Smartphone y demás dispositivos en su hogar o en su empleo, estos cambiaron el estilo de vida de las personas, facilitando la comunicación, logrando conectar personas en diferentes extremos del planeta, además de optimizar procesos en las fábricas, llevando a cabo tareas cada vez más complejas, pero diferencia de una computadora [11], los dispositivos IoT no cuentan con un antivirus, además tienen integrados sensores, micrófonos, cámaras, todos estos capaces de monitorear nuestra rutina, recopilar los datos y enviarlos por internet.

El usuario se preguntará que tiene esto de malo, todo está bien siempre y cuando la información llegue a su destino definido. El problema surge cuando alguien no autorizado, quiere aprovecharse de alguna de las fallas antes mencionadas y alterar el funcionamiento de nuestro dispositivo. Podemos observar algunas vulnerabilidades en la figura 2.1.

Figura 2.1 Vulnerabilidades de IoT en base a la OSI.

A continuación, mencionaremos algunas de las vulnerabilidades a las que los dispositivos IoT están expuestos:

- Credenciales de acceso al dispositivo (usuario y contraseña) que vienen configuradas por defecto y que en algunos casos no pueden cambiarse por otras diferentes, o contraseñas muy fáciles de adivinar.
- Al acceder al software de control y configuración del dispositivo, éste usa protocolos de cifrado inseguro que provoca que se pueda ver toda la información o que se pueda acceder vía Internet (en remoto) sin establecer un filtro de seguridad.
- No hay un cifrado o esté es inseguro en las comunicaciones que realizan los dispositivos con la nube, el servidor o el usuario.
- Al facilitarse la configuración del dispositivo, hay parámetros y características de seguridad que no pueden modificarse.
- En algunos casos, no disponen de actualizaciones para corregir fallos de seguridad detectados tanto en el software, como en el firmware de los dispositivos, debido a que, por ejemplo, el soporte técnico tiene una duración determinada en el tiempo, como sucede con los sistemas operativos antiguos o con la vida útil del dispositivo.
- En determinados dispositivos IoT, se ha detectado la presencia de puertas traseras o backdoors que vienen instaladas de fábrica y que posibilitan el acceso de forma remota al dispositivo y modifican el funcionamiento del mismo.

Dependiendo del tipo de dispositivo, será la forma en la que intentaran tomar el control sobre él, podemos encontrar algunos ejemplos y una breve descripción de cada uno en la Figura 2.2.
Los ciberdelincuentes pueden llegar a usar uno o más tipos de ataques, según sean sus intereses.

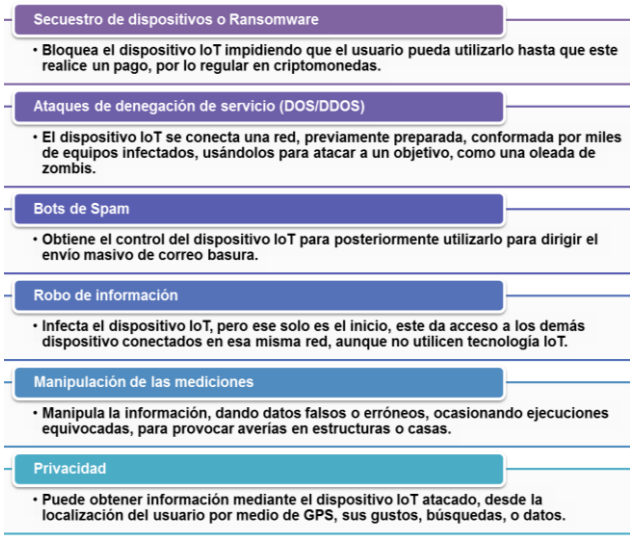

Figura 2.2 Tipos de ataques detectados por la OSI.

En ocasiones las empresas tienen problemas de seguridad debido a que dispositivos IoT no autorizados, conocidos como Shadow IoT [11], se conectan a las redes de trabajo sin contar con la protección adecuada. Les sorprendería la variedad de dispositivos atacados, algunos suenan de película de ciencia ficción, otros hasta absurdos, pero siempre que alguno cuente con una conexión a internet puede ser atacado y usado en contra del usuario u otro objetivo más grande. El hogar promedio [9] recibe cinco intentos de ataques por dispositivo diariamente a través de redes inteligentes. El malware de correo electrónico y el phishing son los tipos de ataque más comunes en Europa, mientras que el ransomware es más frecuente en los EE.UU. Además, una de cada tres personas ve un efecto directo y perjudicial en su privacidad como resultado de las débiles medidas de seguridad en sus redes domésticas.
De igual manera, se han registrado grandes ataques, un reporte informo que Microsoft [5] había detectado el hackeo de alrededor de 1400 dispositivos IoT. Las principales víctimas de este ataque han sido organizaciones políticas, gobiernos y ONGs.
El hackeo fue posible porque el grupo de ciberdelincuentes descubrió fallos en tres dispositivos IoT, en específico: una impresora conectada a través de wifi, un teléfono de voz por IP y un decodificador de video.
Este no es el único ataque que se ha registrado, otro de los grandes ataques a nivel mundial registrados [3] fue al gigante de los videojuegos Nintendo, ya que tuvo poco más 300,000 cuentas afectadas.
El objetivo fue el robo de información a sus usuarios, para después hacer compras masivas en la Shop de las consolas Nintendo 3DS, Switch y Wii U, la empresa bloqueo las cuentas afectadas, implemento algunos cambios en el inicio de sesión y realizo los reembolsos correspondientes a los usuarios afectados; pero no pudo hacer nada para recuperar la información robada, que aún está en las manos de los ciberdelincuentes.
La tecnología avanza cada día, y cada vez surgen nuevos dispositivos IoT en otros sectores, podemos encontrar una gran variedad, tales como juguetes para niños, marcapasos, cámaras de seguridad e incluso automóviles; pero desafortunadamente también han sufrido ataques.

Un caso que se hizo viral sucedió en Alemania [2] sobre una muñeca llamada Cayla, en cuanto sale de su caja hace preguntas a los niños, pregunta acerca de su nombre, el nombre de sus padres, a qué escuela asisten y el lugar en el que viven. Además, cuenta con una conexión a internet, lo que la hace capaz de contestar las diferentes preguntas que se le realizan, también cabe señalar que el micrófono utilizado en esta muñeca puede escuchar todo lo que este a 10 metros a la redonda. Al no contar con un buen sistema de ciberseguridad, algún ciberdelincuente puede tomar el control del juguete, espiar y hablar con los menores, preguntando por información más delicada. Por todo lo anterior, el gobierno de ese país lanzo un comunicado en el que indica que la muñeca debe ser destruida, ya que la considera una amenaza para la privacidad y seguridad de los niños.

Es momento de cambiar de sector, ahora hablaremos acerca a los dispositivos IoT en el área de la salud, un ejemplo de esto es un marcapasos de la empresa Medtronic [8], en un estudio realizado por investigadores en ciberseguridad, resulto que es vulnerable a ataques. Se demostró que el programador que utilizan para controlar los marcapasos no cuenta con un sistema de encriptado, al enviar alguna actualización para el dispositivo no lo envía cifrado, y no tiene manera de saber si fue instalada correctamente; esto marca una gran deficiencia, ya que un ciberdelincuente puede tomar el control del dispositivo y manipular su funcionamiento afectando la salud del paciente.

Otro caso donde tenemos que poner atención es en la evolución de los automóviles.

En un estudio realizado por Upstream [7], sobre los hackeos de los autos inteligentes, demuestra que la ciberseguridad en estos es pobre, principalmente los que abren las puertas con llaves inteligentes, ya que los robos se pueden realizar con un Smartphone, además presenta vulnerabilidades en los servidores, comprometiendo la información de los usuarios. También demostró que podrían enviar una acción a realizar al automóvil, desde los servidores o de los dispositivos que permitieron el acceso y/o control del mismo, esto representa mucho peligro y aún más si la acción es enviada cuando el auto está en marcha, causando un accidente. Cabe señalar que las actualizaciones de seguridad no se pueden realizar de manera automática o rápida, debido a la limitación de desarrollo de seguridad para estos dispositivos.

Otro estudio realizado por Tencent Security Lab Keen expuso que se han realizado ataques al software de los autos, buscando anular el piloto automático o tomando el control del volante, también dio a conocer que se realizaron ataques antagónicos, estos son métodos para engañar a los sistemas de identificación basados en el uso de redes neuronales. Son realizados a los automóviles Teslas, para confundir la red de identificación de las líneas en las carreteras, y hacerlo tomar el carril contrario, si en el otro carril se aproxima otro vehículo, ocasionaría un accidente, dañando a más personas.

Puede que las empresas que crearon esos dispositivos IoT sean los mayores responsables por la seguridad, pero también los usuarios cometemos errores que dan pie a que se aprovechen de ellos. En el siguiente capítulo conoceremos algunas medidas que nosotros como usuarios podemos implementar, además de hablar acerca de la ciberseguridad de los dispositivos IoT.

3.- BUENAS PRÁCTICAS

En esta sección se dará a conocer la arquitectura general de seguridad de IoT [12], esta se divide en varios niveles de diferentes características fusionadas [13], creando un total de 4 capas, encontraremos más características en la Figura 3.1.

Figura 3.1 Capas de seguridad IoT descritas IoT Analytics.

A. La capa de dispositivo: se refiere al nivel de hardware de la solución de IoT, es decir, la "cosa" física o el producto. Los ODM y los OEM (que diseñan y producen dispositivos) están integrando cada vez más funciones de seguridad tanto en su hardware como en el software (que se ejecuta en el dispositivo) para mejorar el nivel de seguridad en la capa del dispositivo.
B. Seguridad de comunicaciones: se refiere a las redes de conectividad de la solución de IoT, es decir, los medios a través de los cuales los datos se transmiten / reciben de forma segura. Si los datos confidenciales están en tránsito a través de la capa física (por ejemplo, WiFi, 802.15.4 o Ethernet), la capa de red (por ejemplo, IPv6, Modbus u OPC-UA) o la capa de aplicación (por ejemplo, MQTT, CoAP o sockets web) Los canales de comunicación inseguros pueden ser susceptibles a intrusiones como ataques de intermediario.
C. Seguridad de la Nube: se refiere a donde los datos de los dispositivos se ingieren, analizan e interpretan a escala para generar conocimientos y realizar acciones. Se espera que los proveedores de la nube brinden servicios en la nube seguros y eficientes de forma predeterminada, y la protección de las principales violaciones de datos o problemas de tiempo de inactividad de la solución se está convirtiendo en la norma.
D. Seguridad de Gestión de ciclo de vida: se refiere a una capa general con procesos continuos necesarios para mantener actualizada la seguridad de una solución de IoT, es decir, garantizar que existan niveles de seguridad suficientes desde la fabricación del dispositivo, la instalación inicial hasta la eliminación

de las cosas. La seguridad por diseño es solo el primer paso en el esfuerzo continuo para mantener segura una solución de IoT; los pasos adicionales a lo largo del ciclo de vida incluyen la aplicación de políticas, auditorías periódicas y control de proveedores.

La ciberseguridad va de la mano con el avance tecnológico, el incremento de ataques aprovechando las vulnerabilidades de los dispositivos IoT a lo largo del 2020 ha dado a conocer la importancia de fortalecer la seguridad, por lo que varios proveedores se están centrando en cómo mejorar y así, proteger a los usuarios. A continuación, hablaremos sobre las tres empresas líderes más populares en ciberseguridad empresarial [15] como se ilustra en la Figura 3.2.

- Cisco: El 42% de los encuestados tiene experiencia trabajando con Cisco como empresa de ciberseguridad. Esta es la proporción más alta entre todas las empresas de ciberseguridad, con más de 150 familias de productos de ciberseguridad que se ofrecen en la actualidad. Permite a la empresa ofrecer seguridad de extremo a extremo. A principios de 2020, Cisco consolidó todas sus 83 marcas de ciberseguridad individuales bajo una marca llamada Cisco Secure, que consta de 3 grupos de productos principales. La compañía también lanzó SecureX, una plataforma integrada nativa de la nube que promete poner todas las diferentes capacidades de seguridad en un solo lugar, reduciendo así la complejidad para los usuarios.
- Microsoft: El 35% de los encuestados trabaja con Microsoft para proteger partes de sus redes de IoT. Una gran parte de la oferta de ciberseguridad de Microsoft está conectada a la oferta en la nube Azure de Microsoft, que actualmente disfruta de una adopción muy sólida en las empresas. Los ejemplos incluyen Azure Sentinel, un SIEM nativo de la nube, y Azure Security Center, un sistema de administración de seguridad de infraestructura unificada. Para las implementaciones de IoT, Azure Sphere es un enfoque único que tiene en cuenta la seguridad de un extremo a otro. Permite una conectividad nativa y segura a la nube con todos los servicios de seguridad típicos, como la comunicación de dispositivo a nube, detección de amenazas y gestión del ciclo de vida.
- Palo Alto Networks: es la tercera empresa de ciberseguridad más utilizada. El 32% de los encuestados afirmó que utiliza los servicios o productos de la empresa con sede en California. Entre otras cosas, la empresa se enorgullece de ofrecer un inventario completo de los activos conectados a Internet de sus clientes.

Figura 3.2 Principales Empresas en seguridad IoT (por IoT Analytics.)

En base a todo lo anterior, podemos observar que la estructura de seguridad que implementan las empresas tiene muchos elementos y además es bastante compleja. Pero los usuarios también debemos hacer nuestra parte, a continuación, conoceremos buenas prácticas que la OSI [11] sugiere implementar en los dispositivos IoT de nuestro hogar para reducir las amenazas. Siempre que vayas a configurar un dispositivo IoT nuevo, ten en cuenta estos consejos para que este seguro:

- Siempre cambia las credenciales de acceso, no utilices las que vienen por defecto, ya que son comunes entre los dispositivos de la misma marca.
- Crea una red independiente del Wifi para estos dispositivos, si alguien llega a entrar a tu red Wifi, como se encuentran aislados, no podrá interactuar con ellos.
- Si tienes experiencia o conocimientos técnicos de computación o informática, puedes establecer un filtrado de tráfico en la red, para evitar que el tráfico no autorizado se dirija a algunos de nuestros dispositivos en específico, o hacia el exterior de nuestra red. Una herramienta muy útil y gratuita es Wireshark, disponible para plataformas Windows, Mac Os y Linux.
- La información de nuestro dispositivo IoT debe estar siempre cifrada, de esta manera se evita el robo de información, pero si aun así logran interceptar la información, el cifrado evita que la puedan manipular o modificar.
- Realizar análisis en los dispositivos con un antivirus (Avira, Avast, Malwarebytes, Kaspersky, AppBrain Ad Detector, etc.), herramientas de análisis online y cleaners de forma periódica en busca de amenazas, infecciones, vulnerabilidades, etc. Dependiendo el dispositivo IoT en la OSI [10] podemos encontrar varias opciones de herramientas gratuitas, entre ellas destaca Conan Mobil, ya que la App nos da a conocer el nivel de seguridad y en caso de encontrar vulnerabilidades, nos da consejos para corregirlos.
- Revisa los permisos concedidos a los dispositivos IoT y desactiva los que no sean esenciales para su funcionamiento.
- Lee las políticas de privacidad del dispositivo, esto sirve para saber qué información recolecta y lo que hará con ella la empresa que diseño el dispositivo.
- Siempre debes tener actualizados tus dispositivos IoT.

CONCLUSIONES

La tecnología IoT avanza imparable como una avalancha, abarcando cada vez más áreas, mejorando y desarrollando nuevos dispositivos capaces de recolectar, enviar y procesar datos a una velocidad sorprendente, todo esto siempre presente en nuestra vida cotidiana, ya sea en el hogar o a nivel empresarial.

Los beneficios que los dispositivos IoT aportan son demasiados e indiscutibles, ventajas tales como la velocidad con la que realizan las tareas, la reducción de costos al realizar los procesos, el poder comunicar personas sin importar la distancia siempre y cuando se cuente con una conexión a internet, la tecnología IoT realiza todo aquello que en algún momento el ser humano creyó imposible.

Desafortunadamente los dispositivos IoT tienen algunos inconvenientes que deben ser resueltos con urgencia, de no corregirlos, se convierten en una amenaza a la privacidad y la seguridad de sus usuarios, esta tecnología no está exenta de problemas de seguridad en sus diferentes dispositivos, y la mayoría de las medidas de seguridad no se pueden aplicar de manera habitual en estos, ya que algunos tienen estas características desde su desarrollo y fabricación. Por lo anterior, la principal recomendación para el usuario, es que al momento de adquirir el mejor dispositivo de acuerdo a sus necesidades, sea muy cuidadoso, debe elegir entre las diferentes opciones a empresas comprometidas y responsables, ya que están siempre tratando de mejorar la seguridad de sus dispositivos IoT, de preferencia que cuenten soporte técnico para apoyar a los usuarios, ya que en base a los reportes obtenidos, se detectan las vulnerabilidades críticas, para posteriormente buscar soluciones, mediante actualizaciones que puedan reparar o corregir la vulnerabilidad. De esta manera, todos juntos, podemos hacer que la tecnología IoT mejore cada vez más.

RECONOCIMIENTOS

Le agradezco a mi familia por el apoyo que me han brindado, a mi mama que me alentaba a seguir esforzándome, a mi papa que me ayudo en mi desarrollo, a mi abuela que me crio y apoyo cuando lo necesitaba, me enseñó a superarme aun cuando las cosas se pueden poner complicadas.

Le agradezco mucho a mi pareja, que me ayuda y me alienta a seguir adelante, aun cuando las situaciones se ponían difíciles, siempre contaba con su apoyo incondicional, sin ella, no habría sido capaz de llegar hasta donde estoy actualmente. De igual manera, agradezco a la familia de mi pareja, que también me apoyaron en este lapso de mi vida. Así mismo, a los amigos que conocí a lo largo del camino.

También le agradezco a la Universidad Autónoma de Guerrero por darme la oportunidad de superarme y prepararme para el futuro, y les agradezco a mis maestros, me guiaron estos años con su conocimiento y la guía para lograr culminar mi carrera profesional.

REFERENCIAS

[1] Azure Microsoft. (10 de Marzo de 2021). Azure Microsoft. Obtenido de https://azure.microsoft.com/es-mx/overview/internet-of-things-iot/iot-technology-protocols/

[2] BBC Mundo. (17 de Febrero de 2017). BBC News. Recuperado el 22 de Abril de 2021, de https://www.bbc.com/mundo/noticias-39010133

[3] Cadena Noticias. (09 de Junio de 2021). Cadena Noticias. Recuperado el 22 de Abril de 2021, de https://cadenanoticias.com/internacional/2020/06/hackeo-a-nintendo-podria-haber-comprometido-la-informacion-de-300000-cuentas

[4] Cárdenas, A. (28 de Noviembre de 2016). SECMOTIC. Obtenido de https://secmotic.com/plataforma-iot/

[5] Catalinas, A. (12 de Agosto de 2019). CyberseguridadPyme. Recuperado el 18 de 03 de 2021, de https://www.ciberseguridadpyme.es/destacado/microsoft-hackeo-iot/

[6] Lueth, K. L. (23 de Diciembre de 2019). IoT Analytics. Obtenido de https://iot-analytics.com/iot-platform-companies-landscape-2020/

[7] MERINO, M. (01 de Abril de 2019). XATACA. Recuperado el 22 de Abril de 2021, de https://www.xataka.com/inteligencia-artificial/unas-pegatinas-asfalto-bastan-para-hackear-piloto-automatico-tesla-convencerle-para-ir-direccion-contraria

[8] Michelone, M. L. (13 de Agosto de 2018). UNOCERO. Recuperado el 22 de Abril de 2021, de https://www.unocero.com/gadgets/codigo-malicioso-potencialmente-mortal-en-marcapasos-cardiacos-una-espantosa-posibilidad/

[9] Network, S. S. (12 de Junio de 2019). PRNewswire. Recuperado el 17 de 03 de 2021, de https://www.prnewswire.com/news-releases/new-research-exposes-the-vulnerabilities-of-smart-home-networks-through-security-cameras-and-smart-hubs-300866213.html

[10] Oficina de Seguridad del Internauta. (26 de Octubre de 2015). Oficina de Seguridad del Internauta. Recuperado el 24 de 03 de 2021, de https://www.osi.es/es/actualidad/blog/2015/10/26/no-hace-falta-superpoderes-para-proteger-los-dispositivos

[11] Oficina de Seguridad del Internauta. (27 de Junio de 2018). Oficina de Seguridad del Internauta. Recuperado el 24 de Marzo de 2021, de https://www.osi.es/es/actualidad/blog/2018/06/27/iot-el-universo-conectado

[12] Scully, P. (29 de Noviembre de 2016). IoT Analytics. Recuperado el 22 de Marzo de 2021, de https://iot-analytics.com/understanding-iot-security-part-1-iot-security-architecture/

[13] Scully, P. (19 de Enero de 2017). IoT Analytics. Recuperado el 22 de Marzo de 2021, de https://iot-analytics.com/understanding-iot-cyber-security-part-2/

[14] Scully, P. (08 de Julio de 2020). IoT Analytics. Obtenido de https://iot-analytics.com/top-10-iot-applications-in-2020/

[15] Wegner, P. (15 de Diciembre de 2021). IoT Analytics. Recuperado el 24 de Marzo de 2021, de https://iot-analytics.com/leading-enterprise-cybersecurity-companies-2021/