CENTRO UNIVERSITARIO TECNOLÓGICO

CEUTEC

FACULTAD DE INGENIERÍA

PROYECTO DE GRADUACIÓN

ANÁLISIS DE SOLUCIONES DEBIDO A LA GENERACIÓN DE INFORMACIÓN POR DISPOSITIVOS INTELIGENTES DE DOMOTICA EN EL INTERNET DE LAS COSAS

SUSTENTADO POR

FERNANDO ENRIQUE VASQUEZ LOPEZ, 31751180

PREVIA INVESTIDURA AL TÍTULO DE INGENIERÍA ELECTRÓNICA

TEGUCIGALPA HONDURAS, C.A.

OCTUBRE, 2021

CENTRO UNIVERSITARIO TECNOLÓGICO

CEUTEC

INGENIERÍA EN ELECTRÓNICA

AUTORIDADES UNIVERSITARIAS

RECTOR

MARLON ANTONIO BREVÉ REYES

SECRETARIO GENERAL

ROGER MARTÍNEZ MIRALDA

VICERRECTORA ACADÉMICA CEUTEC

DINA ELIZABETH VENTURA DÍAZ

DIRECTORA ACADÉMICA CEUTEC

IRIS GABRIELA GONZALES ORTEGA

TEGUCIGALPA HONDURAS, C.A.

OCTUBRE, 2021

ANÁLISIS DE SOLUCIONES DEBIDO A LA GENERACIÓN DE INFORMACIÓN POR DISPOSITIVOS INTELIGENTES DE DOMOTICA EN EL INTERNET DE LAS COSAS

TRABAJO PRESENTADO EN EL CUMPLIMIENTO DE LOS REQUISITOS

EXIGIDOS PARA OPTAR AL TÍTULO DE:

INGENIERÍA EN ELECTRÓNICA

ASESOR:

KARIO ALEXANDRO VILLAFRANCA REYES

TERNA EXAMINADORA:

MANUEL ALEJANDRO ELVIR OSORIO

LUCY ALEXANDRA LOPEZ QUINTANILLA

TEGUCIGALPA HONDURAS, C.A.

OCTUBRE, 2021

RESUMEN EJECUTIVO

Las casas inteligentes y las ciudades inteligentes se aproximan a la vida cotidiana, pero no se está preparado para proteger estos dispositivos inteligentes de ataques por medio de internet. En este momento los dispositivos se ven expuestos a riesgos, vulnerabilidades y amenazas, pero aún se está a tiempo de tomar estos aspectos y transformarlos en el desarrollo de oportunidades de mejora y solución. El objetivo de esta investigación se centra en el análisis de las soluciones disponibles para mejorar la privacidad y seguridad de dispositivos inteligentes conectados al Internet de las Cosas mediante un proceso sistematizado de análisis de solución de problemas. Donde además de las soluciones se verán los problemas como tal, las soluciones viables en el mercado, leyes de prevención de ciberdelincuencia y precauciones para usuarios. Mediante la evaluación de la metodología en cuatro casos en las ramas más problemáticas de dispositivos inteligentes, (Protocolos de transporte, Seguridad de Hardware, Confiabilidad de Software, y Leyes de Seguridad de Datos), se verificará la causa de estos problemas, se observarán las características y se recomendarán planes de acción para solucionar el problema subyacente.

Palabras Clave: Domótica, Internet de las cosas, Ciberseguridad

ABSTRACT

Smart homes and smart cities are coming into our lives, but we are not prepared to protect these smart devices from attacks over the internet. At this time, devices are exposed to risks, vulnerabilities and threats, but we still have time to take these aspects and transform them into the development of opportunities for improvement and solutions. The objective of this research is focused on the analysis of the solutions available to improve the privacy and security of smart devices connected to the Internet of Things through a systematized problem-solving analysis process. Where in addition to the solutions and the problems as such, the viable solutions in the market, cybercrime prevention laws and precautions for users will be seen. By evaluating the methodology in four cases in the most problematic branches of intelligent devices, Transport protocols, Hardware Security, Software Reliability, and Data Security Laws, the cause of these problems will be verified, the characteristics will be observed and action plans will be recommended to fix the underlying problem.

Key Words: Home Automation, Internet of things, cybersecurity.

TABLA DE CONTENIDO

Índice de tablas

Índice de Ilustraciones

GLOSARIO

Automatización	Control autónomo de máquinas o sistemas para controlar procesos.
Autonomía	Capacidad de un sistema de tomar decisiones sin intervención humana.
Ciberseguridad	Conjunto de elementos, medidas y equipos a controlar la seguridad informática.
Ciber Privacidad	Control que ejerce un usuario sobre su información para limitar la cantidad de personas autorizadas a obtenerla.
Dispositivo Inteligente	Un dispositivo electrónico, por lo general conectado a otros dispositivos o redes a través de diferentes protocolos.
Domótica	Conjunto de técnicas orientadas a automatizar una vivienda, que integran la tecnología en los sistemas de seguridad, gestión energética, bienestar o comunicaciones.
Estándar	Patrón, modelo o punto de referencia para medir o valorar cosas de la misma especie.
IEEE	Instituto de Ingenieros Eléctricos y Electrónicos
Internet de las Cosas	La red de objetos físicos (cosas) que incorporan sensores, software y otras tecnologías con el fin de conectar e intercambiar datos con otros dispositivos y sistemas a través de Internet.

Hardware	Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.
Normalizado	Que cumple con las reglas o normas establecidas.
M2M	Engloba a toda aquella tecnología que admita el intercambio de información entre dispositivos, es decir, que envíen datos y se comuniquen.
Malware	Software malicioso
Paquete	Conjunto de datos o información que viajan a través de la red como una unidad.
PLC	Control Lógico Programable
Protocolo	Reglas que permiten que dos sistemas se comuniquen para transmitir información.
Ransomware	Software de secuestro de datos.
Software	Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.
UIT	Unión Internacional de Telecomunicaciones

CAPITULO I. INTRODUCCION

Los dispositivos inteligentes ya no son la tecnología del mañana sino del hoy. La revolución digital ya está en auge y muchos países ya han optado por automatizar muchas de las actividades triviales del día. Aun el conducir ya es una tarea que una maquina es capaz de realizar. Pero qué pasaría si alguien tuviera acceso al GPS independiente del automóvil y en vez de llevar al usuario a su hogar lo llevara a un lugar desconocido donde este puede ser secuestrado. Este es un de los riesgos potenciales presentes en la actualidad debido a protocolos de seguridad poco confiables.

Por lo tanto, es necesario que se mitiguen los riesgos potenciales que rodean los aparatos conectados al internet de las cosas, para proteger tanto al usuario como a su información privada. En el mundo ya hay más de 20 mil millones de dispositivos inteligentes conectados al internet de las cosas y por medio de ellos pasa información privada. Hoy en día, hay mínimo 6 o 7 dispositivos por persona, sin contar los que se comparten en el hogar.

Pero los usuarios omiten que tan segura esta su información al ser generada por dispositivos inteligentes como Amazon Echo o su asistente virtual Alexa. Muchas de las empresas que prestan servicios en línea recopilan la información personal y la almacenan en sus servidores, aunque los usuarios lo borren de sus cuentas. Así como es posible que información sea interrumpida, interceptada o bloqueada por un protocolo de comunicación inestable o inseguro. Por otro lado, podemos ver que los actuales diseños a nivel de hardware de la tecnología IoT impone dificultades para aplicar los protocolos de seguridad tradicional.

Es necesario mejorar la infraestructura de los aparatos y mejorar el software para incrementar su complejidad de autenticación, como lo que es el inicio de sesión de dos etapas. La aplicación de comunicación inalámbrica, una frecuencia publica, como lo que es el WIFI o el Bluetooth, redes vitales en el presentes tiempo, no suelen ser las más adecuadas debido a sus deficiencias de seguridad.

Por otro lado, el uso de normativas y leyes de datos no están perfectamente desarrolladas para ser aplicadas en el lugar de aplicación del objeto de IoT, un reto que debe ser solucionado lo más prontamente posible.

Por todo ello, se apunta la necesidad de que los dispositivos inteligentes se construyan de una forma que garantice su seguridad sin reducir la facilidad de control para el usuario, evitando los riesgos contra su seguridad personal y su privacidad.

CAPITULO II. PLANTEAMIENTO DEL PROBLEMA

2.1 Antecedentes

La comunicación a larga distancia viene desde hace muchos años. Desde la invención de la carta y el telegrama, las personas han podido intercambiar información y datos, pero este era un trabajo arduo y largo. Sin embargo, con la invención del teléfono esto cambio drásticamente y el intercambio de información explotó dentro de las regiones, pero aún no era posible transmitir información a extremas distancias sin que el mensaje tocara varios operadores humanos.

La revolución de la información comenzó con el internet que ha evolucionado de distintas maneras como las conocemos hoy; Computadoras, celulares, televisores, relojes, todos capaces de transmitir información alrededor del globo terráqueo en cuestión de segundos. Hoy en día ya no es necesario ir a recoger los exámenes médicos después de dar la muestra. Ahora una maquina examinara los resultados de la prueba, recopilara un reporte de resultados, revisara la base de datos del paciente y enviara los resultados a su correo personal autónomamente.

Además, ya no es necesario formar parte de una organización con grandes recursos para poder observar estos avances tecnológicos. Gracias a la domótica estos beneficios están al alcance de todas las personas en la comodidad de sus hogares a precios mucho menos elevados en comparación a la maquinaria vista en fábricas y empresas automatizadas. El precio en este momento es elevado, pero en un futuro con el avance de la tecnología esto será accesible para familias de ingresos medios. Igual como cuando los celulares y cámaras entraron con precios exorbitantes, pero ahora es una necesidad de todos.

En base a estos avances podemos decir que el futuro de la comunicación es donde muchas tareas mecánicas y triviales podrán ser contralados sin intervención humana dentro de la casa. Ya no será necesario encender las luces dentro de la casa, abrir la regadera a agua caliente, o hacer un reporte a la policía en caso de alguien se adentre a nuestro hogar.

La comunicación automática entre maquinas mejorara la calidad de vida de las personas y facilitaran aquellas actividades que no requieran de una decisión humana que no haya sido preprogramada o actividades de especial atención. Tejero (2017) nos dice que al estar conectado

a Internet y estar comunicándose con otros objetos, los dispositivos inteligentes se vuelven vulnerables a amenazas de seguridad externas. Entre estos problemas de seguridad tenemos deficiencias de diseño de hardware, simplicidad de infraestructura de software, debilidad en comunicaciones inalámbricas y falta de consentimiento de recopilación de información por dispositivos inteligentes.

Romero (2020) destaca problemas de seguridad presentados por la compañía de antivirus ESET que pueden ser solucionados por acciones del usuario al instalar los aparatos de IoT cuya estabilidad es bastante vulnerable. Entre estos podemos encontrar el cambio de contraseñas por defecto, deshabilitar la vista remota y usar filtros MAC.

2.2 Definición del Problema

Con la aparición del internet ha explotado la conexión entre dispositivos y personas, esto llevando a la difusión masiva de información y con ello un nuevo mundo de posibilidades. Entre ellos los dispositivos de domótica junto al internet de las cosas. Sin embargo, esto conlleva varios problemas asociados que deben ser resueltos para mantener una experiencia más agradable para los usuarios.

La seguridad y privacidad son temas muy controversiales en la domótica ya que para estos dispositivos conocen mucha información personal. Es relativamente fácil que, si no se aplican controles a la privacidad y seguridad de la información, esta sea vendida a terceros o utilizada por las empresas que prestan el servicio en la nube para el procesamiento de los datos y/o abusar de los mismos para proveer mejor mercadeo.

Se necesitan soluciones para los varios problemas de privacidad y seguridad que se tienen por medio de la comunicación entre dispositivos Inteligentes por medio de IoT. Los dispositivos de Domótica generan mucha información personal y confidencial que pueden sufrir ataques cibernéticos por entes con intenciones dañinas a las personas. Entre estos actos se puede encontrar el robo de información confidencial ya sean configuraciones de puertas, autos o ventanas, cuentas bancarias, contraseñas de tarjetas de crédito, historial médico, y hasta datos que no se quieren hacer públicos.

Por lo tanto, es necesario hacer un análisis de las posibles soluciones disponibles para mejorar y asegurar la comunicación de dispositivos inteligentes conectados a internet de las cosas. Entre estas soluciones podemos encontrar ciertas como las mencionadas por Tejero (2017) donde se puede mejorar la Ley de Propiedad Intelectual (LPI) y la Protección de Datos (LOPD). También se pueden realizar mejoras al firmware del ámbito lógico para mantener el sistema al día con protocolos de seguridad.

2.3 Preguntas de investigación

1. ¿Cuál es la situación de ciberseguridad y ciber privacidad de Honduras?
2. ¿De qué forma se puede mejorar la ciberseguridad y ciber privacidad de Honduras?
3. ¿Podrá el ajuste de infraestructura, software, leyes de protección de datos y prevención de datos facilitar la digitalización de Honduras?

2.4 Hipótesis y variables de investigación

2.4.1 Hipótesis General

Los problemas de seguridad a través de IoT de dispositivos inteligentes pueden ser solucionados por medio de actualizaciones a nivel de software y físico, mejoramiento de las leyes de protección de datos y precaución de los usuarios de dispositivos inteligentes.

2.4.2 Hipótesis Secundarias

La situación de ciberseguridad de Honduras no es apropiada para la digitalización de dispositivos inteligentes por las múltiples deficiencias en el área jurídico y técnico.

La ciberseguridad de Honduras se puede optimizar mediante la mejorar de infraestructura y software de dispositivos inteligentes y las leyes que los rodean.

El mejoramiento de infraestructura, software, leyes de protección de datos y prevención de datos facilitara la digitalización de Honduras.

Variable	Definición Conceptual	Definición Operacional
Problemas de seguridad	Los dispositivos se conectan a Internet a través de unas redes Wifi domésticas que son fácilmente atacables, y más desde que en ellas hay dispositivos domóticos y electrodomésticos conectados, que han abierto nuevas puertas a los ciberataques. (Doménech, 2020)	Los problemas de seguridad son identificados de los reportes de problemas provistos por investigadores profesionales.
Dispositivos Inteligentes	La domótica se aplica a la ciencia y a los elementos desarrollados por ella que proporcionan algún nivel de automatización o automatismo dentro de la casa. (Moyr, 2010)	Dispositivos capaces de transmitir y recibir información a través de una conexión por cable o IoT

Nivel de software de dispositivos	Software se define según la RAE como el conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora. (RAE, Definicion.de, 2021)	Problemas de software que involucren deficiencias o vulnerabilidades a nivel de configuración.
Nivel físico de dispositivos	La RAE define al hardware como el conjunto de los componentes que conforman la parte material (física) de una computadora	Problemas de hardware que involucren malos diseños físicos de un dispositivo y generen una vulnerabilidad o deficiencia.
Leyes de protección de Datos	El artículo 3, numeral 8 de la ley de protección de datos personales define de la siguiente manera: "Cualquier información numérica, acústica, alfabética, biométrica, gráfica, fotográfica, de imagen, o de cualquier otro tipo concerniente a una persona natural identificada o identificable". (Tomé, 2019)	Leyes hondureñas que involucren el manejo de información y datos digitales, así como leyes que involucren la privacidad y seguridad digital o la falta de las mismas.
Precaución de Usuarios	La RAE define la precaución como la "reserva, cautela para evitar o prevenir los inconvenientes, dificultades o daños que pueden temerse." (RAE, RAE, 2021) Esto aplicado al cuidado a la	La deficiencia de estándares y practicas básicas de seguridad de usuarios al momento de instalar y configurar dispositivos inteligentes a la red.

	seguridad informática de dispositivos inteligentes.	

Tabla 2.1 Operacionalización de variables (Autoría Propia,2021)

2.5 Justificación

La presente investigación se enfocará identificar y proveer soluciones a los principales problemas de seguridad y privacidad del internet de las cosas aplicado a la domótica. En la época actual la domótica es el futuro de la comodidad del hogar, por lo tanto, es imperativo tener conocimiento de las ventajas, desventajas y riesgos que trae esta nueva tecnología.

La problemática de la seguridad y privacidad radica en que el IoT debe estar conectado al internet para tener intercomunicación con otros objetos. Esto crea múltiples instancias donde se puede filtrar un virus que afecte de manera directa a la confidencialidad, autenticidad e integridad. Los diseños a nivel hardware imponen grandes dificultades para aplicaciones de seguridad tradicional, el software carece de suficiente complejidad, si se depende de conexiones inalámbricas tiende a haber inestabilidad de conexión y deficiencias de seguridad.

Por lo tanto, es necesario realizar una investigación sobre los protocolos, software y otras partes esenciales de la domótica que se les puedan presentar soluciones para mejorar la seguridad de la privacidad en dispositivos inteligentes.

CAPITULO III. OBJETIVOS

3.1 Objetivo general

Proponer soluciones a las deficiencias de seguridad y privacidad en el manejo de información generada por aparatos inteligentes conectados al internet de las cosas por medio de mejoras en el sistema físico, lógico y de transporte de dispositivos inteligentes, las leyes de protección de datos y educación del usuario para reducir los riesgos potenciales de la ciberdelincuencia.

3.2 Objetivos específicos

- Conocer la situación de ciberseguridad y ciber privacidad en Honduras.
- Identificar los casos que se pueden usar como marco para la mejora de ciberseguridad y ciber privacidad de Honduras.
- Analizar si las soluciones de infraestructura, software, protocolo de transporte, las leyes de protección de datos podrán facilitar la digitalización de Honduras.

CAPITULO IV. MARCO TEORICO

4.1 DISPOSITIVOS INTELIGENTES

Cuando se mencionan dispositivos inteligentes lo primero que se viene a la mente es un teléfono celular o un smartphone y esta percepción no es incorrecta. Si buscamos una definición más exacta podemos consultar la Rae que define “Inteligente” como “un sistema, de un edificio, de un mecanismo, etc.: Que están controlados por computadora y son capaces de responder a cambios del entorno para establecer las condiciones óptimas de funcionamiento sin intervención humana.” (RAE, DLE RAE, 2021)

Con esto podemos observar que los dispositivos inteligentes son más que aquellos que interactuamos todos los días, sino que es cada parte de un sistema automatizado con un algoritmo o una inteligencia artificial para regular las condiciones de operación a un nivel óptimo. A nivel industrial, esto revoluciono la manera en que operaban las fábricas y maquilas. Ahora una docena de máquinas hacen el trabajo de que cientos de obreros hacían antes y lo hacen mejor, más rápido y sin agotarse.

Dejando de lado a la industria, tenemos los dispositivos inteligentes enfocados en el mejoramiento de calidad de vida de una persona. A esto dispositivos les podemos llamar casas inteligentes, hogares digitales, o simplemente domótica.

Ilustración 4.1 Dispositivos inteligentes (Vadisco,2021)

La domótica introduce hardware y software en el hogar, creando una red y cambiando aquellos dispositivos que considerábamos análogos en dispositivos inteligentes para facilitar la comunicación entre todos los aparatos domésticos. Bombillos, cafeteras, refrigeradoras, estufas y

cualquier otro electrodoméstico han sido rediseñados a medida que, por medio de la domótica, los usuarios puedan tener el control de ellos de manera remota, con el solo objetivo de crear la casa ideal. (Paz, 2020)

4.1.1 Historia

La domótica no siempre ha sido lo que es hoy y esta ha venido desde muy lejos para llegar al estado que posee. La domótica comenzó en los años setenta cuando se deseaba adaptar tecnología para operación de edificios, pero esta no vio grandes avances hasta los años ochenta cuando dispositivos adaptables a hogares fueron comercializados utilizando una combinación de sistemas eléctricos y electrónicos. Estos dispositivos eran más sistemas automatizados que dispositivos inteligentes, tecnología que se expandió en los países más avanzados como Alemania, Japón y Estados Unidos.

En 1990 la Universidad Tecnológica de Eindhoven comenzó con estudios para aplicarlos en casas como parte de una disciplina de Gerontecnologia. Un estudio que luego se conocería como Domótica. Durante los primeros años de estudio nadie creyó el que el proyecto llegaría a ser. Ya que, aunque habían PC's, el futuro ilimitado de la telefonía y el internet aun no estaban claros como en la actualidad.

En 1998, Corien van Berlo comenzó con la fomentación de la domótica instalando casas inteligentes, para apoyar la normalización de las mismas. Este proyecto se culminó entre el año 2000 y 2001 exitosamente. La tecnología fue bien recibida por el grupo objetivo del proyecto, los adultos mayores. A tal nivel que después del proyecto Corien empezó a contratar personal calificado para mejorar y construir las primeras casas domóticas en los Países Bajos. (Arquitectura, 2001)

4.1.2 Tecnología Disponible

Actualmente en Honduras solo existe una empresa constituida que ofrece un sistema para una casa inteligentes. Megatk es una empresa nicaragüense con oficinas en Tegucigalpa y San Pedro Sula. Actualmente, La empresa dispone de una sola marca de sistema de automatización de casas. HDL, Es una empresa china que ofrece cuatro tipos de productos:

- Sistema HDL autobús

- HDL serie Home Solution
- Automatización de edificios
- Sistema de iluminación de teatro HDL y HDL serie Luces

Ilustración 4.2 Smart Home Solution (HDL,2021)

> La serie Home Solution es la única que cumple para ser un sistema de domótica, ya que los otros productos se aplican a edificios o autobuses. Esta ofrece una completa construcción residencial que incluye iluminación, control de cortinas, control LED, música de fondo, control de electrodomésticos, gestión de energía, seguridad, control remoto por teléfono móvil. (MEGATK, 2021)

Así mismo Megatk (2021) asegura lo siguiente:

> "Incluso se trata de un sistema de control de automatización que podríamos pensar que es complicado y costoso; en realidad es un sistema simple y flexible para el instalador, programador y usuario final, diferentes presupuestos están disponibles para todos los niveles de ingresos y estilo de vida."

El manual de Smart Home Solutions de HDL nos da una nueva perspectiva más allá sobre los dispositivos inteligentes ofrecidos por la empresa. Es un sistema distribuido que puede acomodar hasta 60,000 equipos y es fácil de configurar cada producto proveído por HDL. No requiere incrementar el cableado para mejorar el rendimiento, sino que este depende de la cantidad de módulos conectados.

También podemos encontrar el esquema de conexión de todo el sistema de Home

Solution que se muestra en la siguiente imagen:

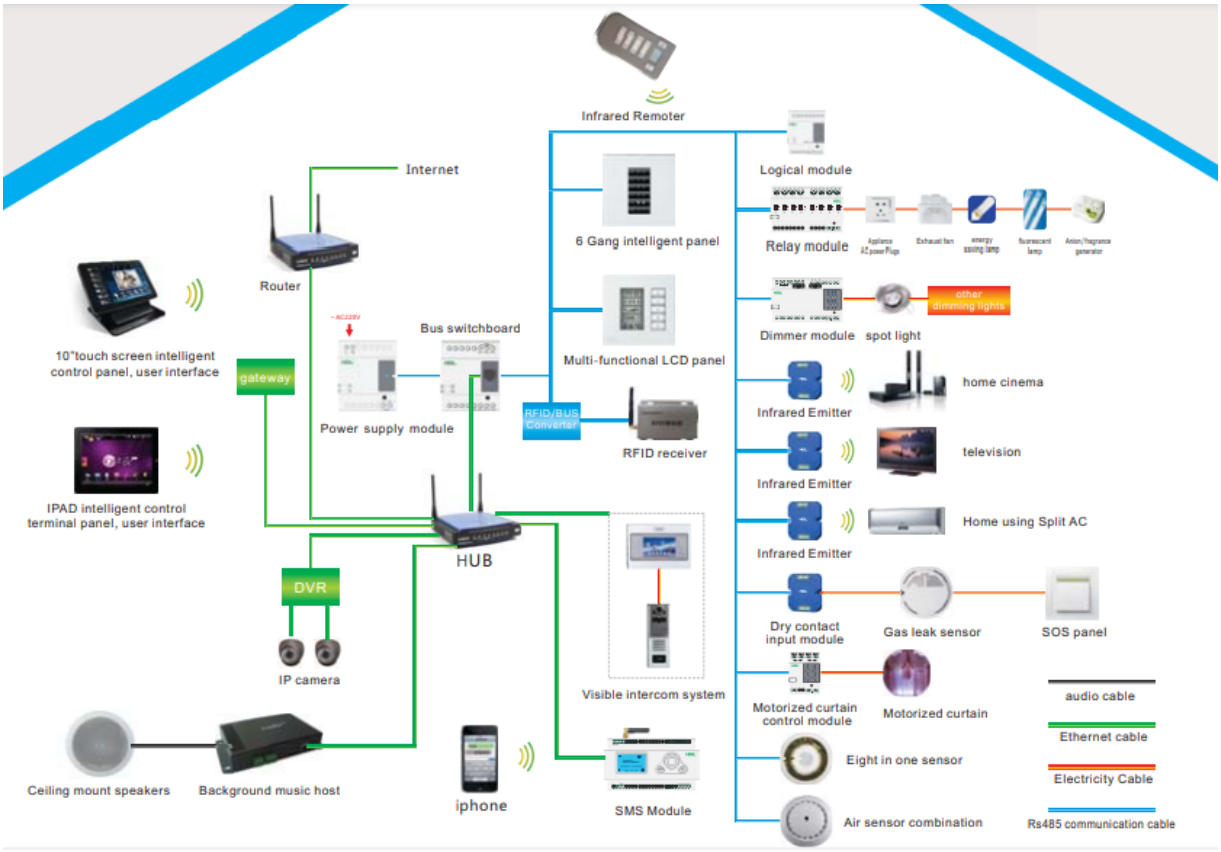


Ilustración 4.3 Esquema de conexión de Home Solution HDL (HDL,2011)

Entre los dispositivos incluidos en el sistema viene:

- Un controlador GPRS/SMS
- Una interface de usuario de 7” táctil
- Un Panel multifuncional inteligente
- Software I-life para control inteligente
- Servidor de Música de Fondo Z-Audio
- Un módulo de control de Seguridad HDL
- Un sensor multifuncional (HDL, 2011)

Este sistema de domótica es del tipo Cable Bus (KNX) que funciona por medio de la integración de cable BUS. Se conoce como un sistema estable, seguro y muy eficiente. Los cables dedicados BUS hacen que el sistema no comparta funciones para evitar problemas de saturación e interferencias para proveer una óptima señal. Sin embargo, este tipo cableado

trabaja para el sistema de manera exclusiva y única. Como otro punto tenemos que este precisa de una instalación importante que puede ser costosa en muchos casos. En ocasiones, el tipo de inmueble juega un importante rol en la estalación del sistema domótico por cable. (Sistemas, 2021)

Este tipo de sistema se encuentra como un sistema de propietario o cerrados, que, aunque seguro corre otros riesgos. Este sistema está diseñado para ser utilizado por una sola marca de manera que solo el fabricante puede realizar mantenimiento, ajustes, cambios o agregar dispositivos debido que solo el proveedor tiene dispositivos que tengan el mismo lenguaje de la máquina. Esto limita grandemente al usuario si desea hacer evoluciones del sistema en comparación a los sistemas estándares abiertos. De igual manera que se corre el riesgo de que la empresa desaparezca o deje de distribuir sus productos en el país dejando al sistema vulnerable y prontamente obsoleto.

4.1.3 Ventajas

Las ventajas de los dispositivos inteligentes son prescindibles para muchas personas. Se alega que para qué hacer que una máquina haga lo que uno mismo puede hacer. Pero lo mismo aplica al inverso. ¿Porque hacer algo cuando una máquina puede hacerlo por nosotros? El factor tiempo es uno de los mayores impulsadores de la domótica. Los dispositivos inteligentes ahorran mucho tiempo que se puede perder las labores triviales. El tiempo es dinero. Y esto no puede ser más verdad para aquellos que viven en una sociedad donde hay que estar en constante movimiento.

Además, en la sociedad que hoy vivimos no siempre es seguro pagar una persona para hacer los quehaceres del hogar. El cual también incluye un sueldo que no deja nada más que el servicio que se requerirá al día siguiente. El diseño de la domótica se basa en la idea de que las personas ahorren dinero y tiempo, los recursos más escasos en la corta vida que se posee.

Por ejemplo, hoy en día ya no hay que medir el aceite del motor para saber que ya requiere un cambio. Con los dispositivos inteligentes hay un sensor que constantemente mide la viscosidad del aceite y manda una alerta cuando esta debajo de los niveles requeridos y cuando llega a un nivel crítico. Por otro lado, un refrigerador puede ser capaz de proveer la información

de los productos almacenados dentro, cuáles han sido agotados y cuales están por terminarse. Facilitando una visita al supermercado con una lista siempre a la mana y evitar hacer varios viajes o tener un ingrediente faltante para la cena.

En el área de la salud personal, tenemos chips implantados bajo la piel con sensores biológicos que monitorean los signos vitales, enfermedades, estado emocional y hasta historial clínico. Estos chips pueden estar enlazados a la red inteligente de la casa y fácilmente medir los niveles hormonales y hacer un recordatorio de que la medicina prescrita no ha sido ingerida. También se puede llamar a una ambulancia en caso de una emergencia o incluso se puede cambiar la luz de ambientación y el ritmo de la música en los sistemas de entretenimiento para relajar un estado de ánimo alterado.

¿Viajar por el mundo está en muchas listas de cosas que hacer, pero que pasa con los hogares cuando las personas salen a descubrir el vasto planeta? Estas quedan desprotegidas y deshabitadas. Un sistema domótico puede evitar muchos de los riesgos que corren los hogares no habitados. Los sistemas de seguridad emulan la presencia humana encendiendo y apagando luces, comprobando si no hay alguna anomalía en los alrededores, y revisando si las alarmas de fugas, incendios o de intrusos estén activadas y enlazadas a las autoridades respectivas.

Otro punto es la innovación técnica de la propiedad al momento de vender. Una casa inteligente se cotiza por mucho más en el mercado y esta cuenta con características que la competencia no cuenta. Además, este es un valor añadido a medida que las tendencias avanzan.

Las máquinas inteligentes tienen mucho potencial por explotar y mientras se usen con conciencia el mundo podrá avanzar a un mundo donde todos tengan dispositivos que faciliten las tereas diarias.

4.1.4 Desventajas

Todo objeto, trabajo y servicio tiene sus beneficios y problemas. El que tenga problemas no significa que sea malo, sino que uno debe estar preparado cuando uno de estos se presente, si es que la necesidad se muestre.

La domótica no es la excepción y no es un tema que podamos evitar si deseamos tener una perspectiva concreta sobre el tema.

No todos los países cuentan con grandes avances de tecnología sobre la domótica, esto siendo especialmente para muchos países de Latinoamérica. Por lo tanto, es posible que no se encuentren instaladores autorizados para realizar proyectos de domótica. En ciertos casos pueden ser poco precisos o muy improvisados en sus instalaciones porque tampoco existen instituciones reguladoras de esta área de profesión. Por otro lado, nos podemos encontrar con servicios muy costosos debido al monopolio del servicio que generalmente no incluyen mantenimiento después de la instalación.

Aunque la domótica tenga el propósito de facilitar la vida del usuario, esta requiere un cierto nivel de conocimiento sobre los aparatos y controles a utilizar para poder realizar los ajustes. Muchas instalaciones por terceros pueden no incluir un manual de instrucción de uso o no dar una explicación de cómo funcionan los distintos botones u opciones que posee el controlador.

Otro problema técnico es la falta de centros de servicio en caso de un desperfecto o daño al sistema. Si bien la empresa que lo instalo puede ser una opción, no siempre tendrán una solución ya que muchas de estas compañías compran los productos en el extranjero y siguen un manual de instalación. En ningún momento presentan el conocimiento de reparar un dispositivo que ellos no diseñaron y nunca han conocido internamente. (Constantino, 2011)

4.1.5 Impacto Social

Como toda tendencia en el mercado, la domótica tiene un impacto en la sociedad, pero esta es una tendencia que vino a quedarse. La tecnología no es buena ni mala, pero esta se diseña para actividades específicas en mente y está más allá de los fabricantes las aplicaciones que los usuarios le pueden dar a sus creaciones. Tomando esto en cuenta, no está demás siempre incluir protocolos y permisos que prevean el uso mal intencionado de la tecnología.

El impacto más notorio que ha tenido la domótica es la comodidad de vida que sus usuarios pueden percibir. Mas allá de las tareas que se pueden realizar por los dispositivos, tenemos la seguridad de poder controlar todo a través de nuestro teléfono celular. Esto les da tranquilidad y más tiempo a los beneficiados de realizar nuevas actividades o pasar más tiempo en familia. (Araico, 2019)

Como siguiente punto tenemos los avances en la seguridad y asistencia. Mediante la combinación de la domótica y el internet de las cosas es posible tener un hogar bajo control aun estando a miles de kilómetros de distancia. Estos dispositivos inteligentes pueden trabajar simultáneamente con las autoridades por medio de grabaciones directamente transmitidas a la policía, alarma de intrusos silencios y alarmas de gases o incendios conectadas al número de emergencia de los bomberos.

Otro punto positivo a cubrir es el ahorro a largo plazo. La factura de electricidad es algo que atormenta a muchas personas a final de mes. Pero, si las luces solo encienden cuando detectan movimiento, los tomacorrientes funcionen solo cuando hay algo conectado y las ventanas estén abiertas en vez del aire acondicionado, estas aportan a reducir el gasto energético al máximo, reduciendo el desembolso a final de mes.

Sim embargo, no todos los cambios son buenos, estos dispositivos inteligentes tienen dos dependencias irrevocables, electricidad y conexión a internet. Si bien son cosas que suenan muy obvias, si el usuario vive en una zona donde hay constantes bajas de flujo eléctrico, los dispositivos inteligentes no funcionaran como se debe debido al constante reinicio del sistema, así como pueden llegar a dañarse o quemarse por una sobrecarga en la línea.

Así mismo, el internet no siempre es estable y las compañías que prestan el servicio tampoco pueden ser las mejores. Un dispositivo inteligente con una conexión inestable puede causar problemas o quedar inutilizables. Gracias a una mala conexión, a veces el informe se puede imprimir tres veces y la ropa puede quedar solo enjabonada.

Si bien la domótica trae ahorros a largo plazo, el costo de vida incrementa. Los dispositivos inteligentes no son baratos y hacer una transición completa puede llegar a costar una

pequeña fortuna. Los precios de sus contrapartes análogas no se pueden comparar, tal y como pasa con la transición de focos fluorescentes a bombillos LED actualmente en Latinoamérica.

Por último, muchos dispositivos inteligentes son vulnerables a ataques cibernéticos en comparación a la reacción que poseen a ataques físicos antes mencionados. Una casa inteligente no siempre es el objetivo de un ciberdelincuente, pero no es de más estar al tanto de los riesgos que se corren. Adicionalmente, la divulgación de información y la disminución de privacidad, usualmente acompañan esta tecnología. Si bien en la mayoría de casos no afecta directamente, es relativamente preocupante que empresas recolecten la información de los usuarios y posean una base de datos completa con los intereses para vender mejor.

4.2 INTERNET DE LAS COSAS

El internet de las cosas se puede simplificar a la interconectividad masiva de dispositivos. El IoT nos afecta a todos queramos o no. Ya es parte de la vida cotidiana como se conoce. Desde lo simple que es comprar una recarga desde el celular móvil hasta los países más desarrollados que poseen redes de conexión bluetooth Audio para poder transmitir los comentarios de obras de arte directo a los audífonos en un museo.

Este cambio es gradual, y aún tiene mucho por crecer. El mundo avanza a tal punto que se está transitando a una sociedad que no depende del almacenamiento físico. Sino que todo se almacenada en una nube y se puede acceder desde cualquier dispositivo con acceso a la información y una conexión a internet.

Por un lado, este es un gran avance para un mundo interconectado, donde podremos tener toda la información que queramos a un clic, pero as mismo puede estar en contra de la misma sociedad que la creo. Esta puede ser utilizada para bien y mal. Para salvar vidas y ponerlas en peligro. Como toda cosa construida por los seres humanos, debe ser utilizado de una manera responsable y con precaución para evitar caer en las trampas de personas maliciosas.

4.2.1 Antecedentes

El termino Internet de las cosas provino de una máquina expendedora de bebidas que estaba conectada a Internet y esta transmitía si todavía había refrescos o no disponibles en la

máquina. Pero no fue hasta el año 2005 que este término fue añadido al reporte UIT por la Unión internacional de telecomunicaciones.

Para el año 2010 el número de aparatos físicos cotidianos y dispositivos conectados a internet fuera de aproximadamente doce mil millones. En su informe de 2014, la IEEE definió el IoT como "Una red de elementos dotados de sensores los cuales están conectados a internet". Incluidos en esta categoría se puede encontrar casi cualquier cosa desde teléfonos celulares, edificios, marcapasos, calzado y hasta ropa. Para el año 2020 se estimó que habían más de cincuenta mil millones de estos dispositivos inteligentes.

El IoT vino a cambiar la sociedad que se conocía. El internet introdujo la comunicación a distancia de una manera sencilla y rápida, pero el Internet de las cosas vino y conecto todo de una manera muy radical. Este cambio elevó la calidad y el lujo de vida de las personas y la industria. Llego a aumentar la productividad de las empresas y presentó nuevas oportunidades para la educación, seguridad, transporte dejando muchos nuevos puestos centrados en IT. (Salazar, 2016)

4.2.2 Aplicación en Domótica

Los beneficios del internet de las cosas son evidentes con el cambio del tiempo. Este mismo ha permitiendo la creación de la automatización y la domótica. Ahora los hogares pueden ser inteligentes, ya no solo automatizados. Antes el bombillo se encendía en las noches porque un sensor foto resistivo percibía que la cantidad de lumen, la intensidad de luz, se disminuía y este reducía la resistencia para que la corriente fluya y este bombillo se encienda. Lo contrario sucedía en la mañana, donde el sensor percibe la luz y apaga el bombillo.

Sin embargo, en ningún momento el bombillo estaba al tanto de porque se encendía o apagaba, si no que solo reaccionaba al cambio en su circuito interno. Ya en un Hogar inteligente el bombillo sabe que oscurece y él se debe encender la fuente de luz. Este mismo proceso ocurre con muchos aparatos cotidianos que mejoran el consumo eléctrico, la calidad del aire en una habitación y hasta la limpieza del suelo.

La domótica es una de las ramas en donde más podemos ver el progreso del internet de las

cosas. Dentro de una casa inteligente toda clase de aparatos generan información que se distribuye alrededor de la casa para mantener el hogar acondicionado de una forma óptima para el usuario. Entre estos dispositivos encontramos:

- Iluminación y ambientación
- Control de energía
- Climatización
- Control de puertas y ventanas
- Limpieza
- Seguridad y Acceso
- Sistemas de entretenimiento
- Electrodomésticos

Todos estos aparatos funcionan en conjunto para mejorar el estilo de vida del usuario por medio de la recolección de información. Una cafetera puede estar programada para hacer el café a las seis de la mañana todos los días de trabajo y por medio de su conexión con el calendario electrónico del teléfono móvil, puede saber que días son libres o feriados para no realizar la acción predeterminada.

Esta experiencia de recolectar, compartir y analizar información hace que la administración de un hogar sea más sencillo y agradable. Aun, no es necesario tener un hogar inteligente para poder enlazar un Smart Tv a su red wifi sin necesidad de un módulo especial para internet, a comparación con los televisores LED o LCD de hace unos años. Los dispositivos ahora vienen diseñados para ser anexados a una casa domótica. Esto es posible mediante la comunicación de cableado eléctrico PLC. Este es capaz de transmitir señales de radio por medio de la infraestructura presente de líneas de energía eléctrica. Permitiendo así la comunicación de dispositivos sin adaptación alguna.

4.3 PRIVACIDAD Y SEGURIDAD

Todo país, legislativamente, garantiza los derechos a la intimidad personal, la libre expresión y la seguridad de las comunicaciones. Teóricamente, al menos. En realidad, la protección en tiempo real que puede proveer un país es limitado, sobre todo en un país con el

nivel de seguridad pública como Honduras. La constitución hondureña promete garantizar la imagen pública e intimidad personal, pero a diario se puede ver en noticieros personas capturadas por cometer delitos comunes expuestos en los medios de comunicación, mientras que otros casos se van impunes sin cobertura alguna.

Sin embargo, la constitución a la fecha no consta de una Estrategia de Ciberseguridad que vele por los derechos de los cibernautas de Honduras. El BID reporta que, en 2020, Honduras cuenta con más de tres millones de personas con acceso a internet, representando un 32% de penetración de internet. Esta cifra no representa solo el progreso de la tecnología, sino, la cantidad de personas desprotegidas por la ley.

El congreso Nacional en el año 2018 aprobó la ley de Seguridad Cibernética, pero esto es una Ley de ciberseguridad y medidas de protección ante los actos de Odio y Discriminación en Internet y Redes sociales. Ley de mucha importancia, pero que, al nivel actual de esta sociedad tecnológica, deja mucho que desear. (BID, 2020)

Esto nos conlleva a exhortar que los usuarios tomen parte activa en la privacidad y seguridad digital personal antes de comprar dispositivos inteligentes.

4.3.1 Privacidad Digital

Dia a día, millones de personas acceden a docenas sino cientos de páginas web desde su dispositivo móvil o computadora y en la mayoría de casos, inevitablemente estas personas pierden su ciber privacidad al aceptar todas las cookies en páginas desconocidas. El silencio total de información al estar conectado al internet es imposible, pero al navegar, el usuario está protegido de robos maliciosas de información personal. Mas allá de un riesgo, se podrá ver las búsquedas más recientes en el futuro anuncio de Facebook y dará prioridades a la inteligencia artificial de YouTube para catar de mejor manera los videos que se muestran.

Pero, ya en un dispositivo inteligente en una casa inteligente con acceso a toda la información personas, de trabajo y cualquier otra red conectada pone en riesgo mucho más que anuncios. El ransomware es una práctica de ya hace muchos años, pero con el avance tecnológico estos siguen evolucionando y por el mejor de los esfuerzos, es muy difícil evitar que sucedan.

Ilustración 4.4 Ransomware (Kirkpatrickprice,2019)

En agosto de 2020 la privacidad digital de la empresa BlackBaud fue penetrada por un ataque de ransomware. Esta empresa contaba con un técnico de IT que, con la cooperación de la policía, y un buen departamento de respuesta a ciberataques, lograron evitar que los atacantes cifraran los datos y los bloqueara en los sistemas de la empresa. Sin embargo, esto no evitó que el atacante exigiera un rescate por la información personal extraída de los servidores durante el ataque. Este hecho se dio a conocer gracias a las leyes sobre la protección de la privacidad de Inglaterra, que obligo a la empresa a informar a los clientes y organismos reguladores sobre el incidente. (Anscombe, Welivesecurity, 2020)

Este incidente es uno de los cientos ataques a la privacidad pública y privada por ciber delincuentes, algo que se ha vuelto una profesión muy lucrativa. Una razón más por la cual es país debe actualizar sus pólizas de seguridad cibernética y los usuarios deben mantenerse al día para protegerse a sí mismos y a su información.

4.3.2 Seguridad Digital

Con la aparición del internet la seguridad de la información personal ha caído en un serio dilema que no se puede comparar al robo de información a su predecesor análogo. Antes, la información se almacenaba en una institución custodiada por la misma. Hoy en día, las bases de datos se encuentran en la nube y miles de personas pueden acceder a ellas, incluso anónimamente. Ya no es necesario presentarse a una locación y arriesgar ser capturado para conseguir datos de otros usuarios.

Los delincuentes cibernéticos evolucionan al mismo ritmo que la tecnología y por lo tanto

la seguridad digital debe seguir el ritmo de las tendencias. Pero que conlleva la ciberseguridad. La seguridad social es un ámbito de la informática que se dispone a la protección de la infraestructura computacional, comprendiendo ambos softwares, bases de datos, nubes, archivos, meta data y el hardware. Cualquier persona o entidad que signifique un riesgo para cualquiera de estas áreas se debe identificar, aislar y eliminar para evitar que afecte el resto o todas las demás áreas.

En el ámbito de los dispositivos inteligentes esto es aún más crítico debido a la naturaleza de estos en generar y transmitir información dentro del hogar. Es una práctica común dejar que los técnicos se encarguen de toda la configuración y los usuarios no estén al tanto de los protocolos de seguridad, formato de las contraseñas y muchos otros aspectos de seguridad.

Si bien se espera una ética laboral concreta de parte de los técnicos, nunca hace falta tener conocimiento de todos los procesos que se llevan dentro de la casa y que van a proteger la integridad de la misma por los años subsiguientes.

Así mismo es importante saber que Honduras actualmente no cuenta con una CSIRT (Equipo de respuesta de incidentes de seguridad informática) y las leyes actuales de ciberseguridad no están lo suficiente maduras para cubrir incidentes relacionados con Hogares inteligentes.

El Banco interamericano de Desarrollo (2020) público su nuevo reporte sobre avances, riesgos y destino de la ciberseguridad en América Latina en donde Honduras postula entre los participantes. En este reporte se puede apreciar las estadísticas actuales del país.

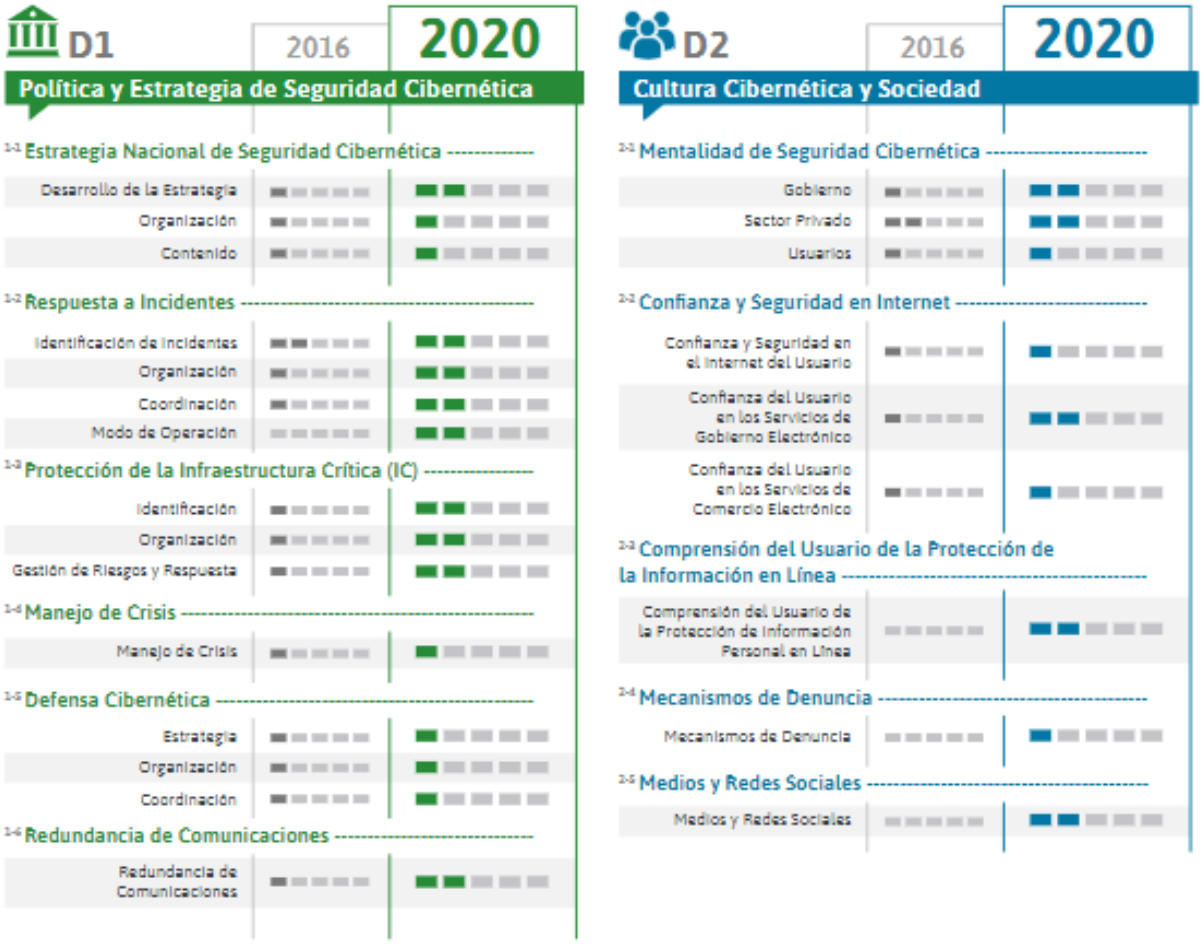


Ilustración 4.5 Estatus de Política, Estrategia y Cultura de Ciberseguridad. (BID,2020)

Ilustración 4.6 Estatus de Regulación, formación y Estándares de ciberseguridad (BID,2020)

Honduras ha progresado considerablemente desde el año 2016 en asuntos de seguridad digital, pero no es progreso similar al de países aledaños en las mismas condiciones. Honduras es uno de los pocos países mencionados que no tienen una estrategia Nacional de ciberseguridad o una en desarrollo, ni forman parte de la convención de Budapest o están invitados. Esto deja a los usuarios de Dispositivos inteligentes y usuarios de la red igualmente desprotegidos.

Por lo tanto, está en las manos de los proveedores y usuarios en mejorar el sistema de protección personal lo mejor posible en caso de ataques cibernéticos.

4.4 GENERACION DE INFORMACION

Los dispositivos de IoT, nacen de la generación y transmisión de información de un punto a otro. De lo contrario, sería imposible transmitir que ya está oscureciendo desde el sensor hasta el servidor centrar para que el actuador encienda las luces del estacionamiento y la puerta de entrada. Esto se complica mucho más si le ordena al asistente virtual que ordene la cena predeterminada número cinco por medio de un servicio de Entregas Genérico y que la entreguen directo a la mesa en el comedor; todo sin mover un solo dedo. Este proceso involucra mucho más que un simple comando nos permite observar.

Ante todo, un asistente virtual debe tener acceso a la cuenta de envíos, tarjeta de créditos, lista de ordenes predeterminada, restaurantes favoritos, preferencias, dirección de vivienda y control automático de puertas. Toda esta información se puede clasificar en dos categorías, sensible o personal. Sin embargo, sin cerciorarnos de ello, esta información puede estar en las manos de otros con malas intenciones.

Uso sin consentimiento de datos comerciales, robo de identidad, uso no permitido de tarjetas de crédito, y publicación de información privada son ciertas de las cosas que pasan en el mundo del IoT por la generación de Información.

Esto no quiere decir que generación información sea negativo, por el contrario, es una necesidad. Por lo tanto, los usuarios de dispositivos IoT deben estar al tanto de los problemas, consecuencias y otros aspectos de la generación de información por los dispositivos IoT.

4.4.1 Protocolos de comunicación

El protocolo de comunicación es lo que permite a nuestros dispositivos aledaños, actuadores, sensores y centrales de comando transmitir información de ida y venida. El IoT consiste de una gran cantidad de dispositivos que van desde el servidor central hasta el bombillo del garaje y para ello necesitamos que los dispositivos estén conectados entre sí. Lo que no nos permite tener un protocolo de uno a uno, sino que debemos tener protocolos capaces de manejar comunicación de varios a varios, buenos niveles de interoperabilidad, un nivel bajo de acoplamiento entre dispositivos y que sean escalables.

Entre estos protocolos se pueden encontrar los mundialmente conocidos protocolos WIFI

y Bluetooth que se pueden encontrar en todo celular inteligente.

El bluetooth es una tecnología de corto alcance de 2.4 GHz el cual es caracterizado por su bajo consumo de energía y que funciona por medio de una red PAN (Red de Área Personal) lo cual puede evitar el ataque remoto a dispositivos. Sin embargo, este cuenta con una tasa baja de transferencia de datos y una seguridad cuestionable contra ataques de fuerza bruta y una transmisión poca segura de datos.

Por otra parte, el WIFI es abiertamente popular en el ámbito del IoT. El WIFI es capaz de transmitir grandes cantidades de datos a una velocidad dependiente del contrato de internet. Sin embargo, ¿qué tan seguro es el WIFI? Este protocolo es capaz de conectar docenas de dispositivos y a red dándole acceso a atacantes a poder conectarse a los distintos dispositivos presentes en la red. Debido a su naturaleza de uso masivo y su conexión permanente al internet, el WIFI es muy vulnerable a ataques remotos y no dispone de la seguridad necesaria para manejar redes de dispositivos IoT.

Pero la industria no se queda atrás creando una solución.

Actualmente el protocolo en auge en la industria 4.0 es el M2M (maquina a máquina) un protocolo de comunicación específico para IoT. Esta estructura está basada en las capas del modelo OSI (Modelo de Interconexión de Sistemas Abiertos), enfocados en las últimas cuatro capas de aplicación, presentación, sesión y transporte donde se garantiza la fiabilidad y la seguridad de la comunicación durante la transferencia de datos provenientes de dispositivo a dispositivos.

Entre los M2M se pueden mencionar los que más fuerza toman en la industria actualmente:

MQTT (Message Queuing Telemetry Transport) es un protocolo de mensajería que actúa sobre TCP. Entre sus características se destaca por ser ligero, sencillo de implementar para dispositivos de baja potencia. Óptimo para routing con varios dispositivos en la red. Como desventaja tenemos que monitorización de la conectividad y control de dispositivos remotos no son posibles. (Muelaner, 2021)

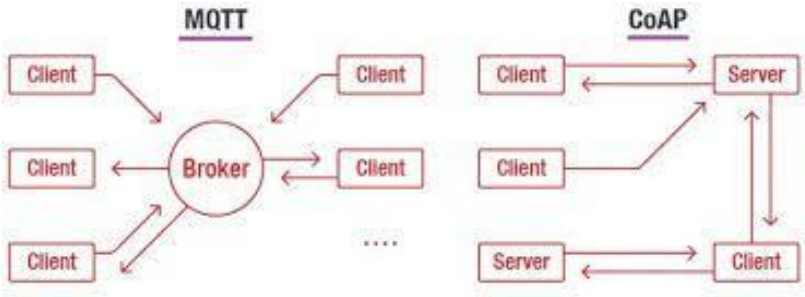


Ilustración 4.7 MTQQ vs CoAP (rasberryvalley,2021)

CoAP (Constrianed Application Protocol) es otro protocolo diseñado para dispositivos IoT de baja capacidad. Este se basa en el modelo REST de HTTP con cabeceras reducidas muy similar a la conexión de dispositivos con la API web. (Muelaner, 2021)

Cabe recalcar que estos protocolos no están totalmente adaptados para Dispositivos IoT para Hogares inteligentes, sino para la industria, pero es un punto de partida que pronto veremos en el ámbito habitacional.

4.4.2 Deficiencias de Hardware

La naturaleza de la tecnología nos dice que día a día tenemos nuevas invenciones en todas las áreas ya sea en el campo industrial, el área de la salud o bien sea la automatización de hogares, sin contar las muchas nuevas teorías que aún no dejan el cuaderno. Esta forma de ser, de superarse a sí misma cada día le permite a la tecnología tener un futuro sin fronteras. De tal forma que a medida que nuevos materiales, nuevas piezas y técnicas se usan, los costos y precios de la tecnología bajan, llegando a un mercado más extenso, y difundiéndose por las masas.

Como testamento a esto, podemos dirigirnos a la historia de la cámara digital. En el año 1991 la primera cámara digital Kodak de 1.3 MP costaba alrededor de trece mil dólares americanos mientras que ahora se puede entrar a Amazon y por ochenta y uno dólares americanos se puede obtener una cómoda cámara Kodak de 16 MP.

Pero no todo es buenas noticias con el rápido avance de la tecnología. A medida que nuevos dispositivos aparecen en el mercado, la competencia busca superar la misma tecnología a un menor costo, usualmente reduciendo la calidad de los materiales originales. Para la domótica a

la cual le entregamos nuestra seguridad, es un defecto fatal.

Muchos fabricantes de empresas pequeñas prefieren crear sistemas físicos poco robustos que permiten a los atacantes llegar a información sensible o hasta tomar control local del dispositivo.

Anscombe (2018) nos presentó un estudio impulsado por la compañía de antivirus ESET donde se analizaron doce dispositivos IoT presentes en el mercado y los cuales todos presentaban problemas de privacidad y otros tipos de vulnerabilidad. Entre estos dispositivos encontramos el popular Amazon Echo, un asistente virtual de manos libres al cual se le pueden realizar millones de preguntas por comandos de voz. No es una sorpresa que toda esta información se almacene en tu cuenta de Amazon como Datos comerciales. Alarmante seria que un ciberdelincuente acceda a la cuenta de Amazon y obtenga datos sensibles.

Otros problemas de hardware que viene con el tiempo es que la IoT es cambiante y son pocas las tecnologías que sobrevivan el paso del tiempo. En la actualidad son pocos los dispositivos que tienen una vida útil de largo plazo y son menos los que se mantienen al nivel de las nuevas tecnologías emergentes. Es posible que, por ahorrar en no comprar el modelo más reciente, el consumidor obtenga un modelo que pronto ya sea descontinuado por el fabricante y, de una forma, sea estafado con tecnología obsoleta.

4.4.3 Deficiencias de Confiabilidad

Uno de los componentes más importantes al momento de elegir convertir un hogar en un hogar inteligente, más allá del confort debe ser la confianza en el sistema que estamos instalando, así como quien mete sus joyas en una caja fuerte y sabe que están sanas y salvas. Especialmente, fuera del alcance de ladrones de joyas. El mismo caso aplica a dispositivos inteligentes conectados a IoT.

La seguridad de IoT está relacionada con la capacidad de sus usuarios en confiar en su entorno. Si los usuarios no creen en la seguridad de su hogar, esto resultara en la renuncia del usuario en mantener un hogar inteligente. A un plazo más largo esto vendría afectando el comercio electrónico y el desarrollo tecnológico. Para el sector de dispositivos de IoT, la

seguridad debe ser un sector de máxima prioridad. (Rose, 2015)

Por ello debemos ver las principales deficiencias de software o confiabilidad presentes en los dispositivos vistos en una casa domótica. Los dispositivos inteligentes poseen muchas ventajas, sin embargo, muchos dispositivos poseen características de software débiles que pueden ser explotados por ciberdelincuentes.

La falta de encriptación a nivel de transporte es un riesgo al momento que nuestra información viaje a través del internet por medio de un dispositivo IoT, este está propenso a ser atacado por malwares que, por falta de encriptación, pueden comprometer o infectar la información presente.

El protocolo de autenticación no siempre está lo suficientemente preparado para los ataques cibernéticos, y al utilizar llaves de encriptación el hacker puede lograr hacerse pasar por el usuario y acceder a información sensible. Esto también es posible por sesiones prolongadas y mecanismos de recuperación de contraseñas inseguras.

As mismo puede ocurrir que el sistema de seguridad de un disponible no posea flexibilidad al momento de configurar la seguridad de dicho dispositivo. Al no poder ver que opciones están disponibles sobre el manejo de nuestros datos comerciales, configuraciones de acceso a redes wifi, tipo de encriptación de contraseña y políticas de privacidad y manejo de datos un usuario se ve vulnerable ante cualquier defecto de seguridad que el dispositivo pueda tener oculto.

Por último, sin disminuir su importancia tenemos inseguridad en el firmware de los dispositivos. Ya sea por defecto del modelo, desactualización del sistema o falta de conexión a la red. El firmware es uno de los problemas de confiabilidad más llamativos para los ciberdelincuentes. Un firmware viejo puede abrir puertas a los hackers a conectarse a la red wifi y alterar configuraciones del hogar, tomar grabaciones del interior de la casa, así como robo de información personal. Un dispositivos descontinuado o ya muy viejo también pueden ser causante de un firmware inseguro. (Tejero, 2017)

4.4.4 Leyes de Protección de Datos de Honduras

En la actualidad, Honduras no cuenta con una ley de protección de datos actualizada que abarque apropiadamente lo que es la protección de datos personales digitales o regulación alguna sobre el tráfico de datos generado por casas inteligentes controlados por sistemas autónomos.

En el año 2013 se agregó la lista de recurso Habeas Data a la constitución hondureña la cual no es suficiente para velar por la seguridad informativa de la población hondureña. Uno de los artículos de interés presente en la constitución hondureña determina el derecho de privacidad de datos personales:

> Artículo 182. No 2 "Toda persona tiene el derecho de acceso a la información sobre si misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros Públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o suprimirla. No podrá afectarse el secreto de las fuentes de información periodística. Las acciones de Hábeas Corpus o de Hábeas Data se deben ejercer sin necesidad de poder ni de formalidad alguna, verbalmente o por escrito, utilizando cualquier medio de comunicación, en horas o días hábiles e inhábiles y libres de costas." (Honduras, 2013)

Este es un derecho no siempre respetado ya que muchas de las acciones de empresas privadas violan estos artículos con la malversación de información privada. Acción que la Corte Suprema de Justicia debería cesar inmediatamente ya que es una violación de los derechos de honor, intimidad personal o familiar y a la propia imagen.

En el año 2015 se propuso una ley de protección de datos personales. Sin embargo, esta estuvo en debate legislativo durante muchos años en el congreso, el ultimo se llevó a cabo en año 2018. Un retraso sin precedente tomando en consideración que solo se aprobaron 19 de 97 artículos presentes en la Ley.

Dentro de la Ley de Protección de Datos Personales en el artículo 3, numerales 8 y 9 encontramos la definición de datos personales y datos sensibles.

> Datos Personales: “Cualquier información numérica, acústica, alfabética, biométrica, gráfica, fotográfica, de imagen, o de cualquier otro tipo concerniente a una persona natural identificada o identificable.” (Honduras, 2013)
>
> Datos sensibles: “Aquellos que se refieran a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada, tales como: Los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud, físicos o psíquicos y preferencias sexuales, así como cualquier otra información considerada como tal por ley; y, cualquier otro dato respecto de la libertad individual protegido por la Constitución de la República o en Convenios Internacionales suscritos por Honduras”. (Honduras, 2013)

Este articulo contribuye a la protección de datos digitales de una persona debido a la amplia gama que presentan los datos personales. Sin embargo, no hay ninguna especificación de información generada por sistemas autónomos como configuraciones de seguridad, generación de información y otros datos generados por dispositivos inteligentes. Lo que deja vulnerable a usuarios frente a ataques cibernéticos. (Tomé, 2019)

4.4.5 Precaución de Usuarios

Las casas inteligentes van mejorando cada vez más, volviendo a los hogares un lugar de mayor comodidad, pero al mismo tiempo un mayor peligro. La piratería informática, el control remoto de dispositivos que exponen nuestros datos personales son un riesgo potencial. Los aparatos que generan muchas facilidades pueden, también, provocar inconvenientes y hasta poner vidas en riesgo. Hay muchos casos desde bots que niegan el servicio DDoS para acceder a webcams y routers hasta ataques de dispositivos contra los servidores de grandes empresas.

Se han dado casos donde el diseño con defectos de un aparato puede permitir a los hackers ingresar a la red wifi de una casa. Bombillos, juguetes, servicios, cafeteras y refrigeradoras están entre los aparatos más afectados por los ciberdelincuentes.

Este fue el caso del bombillo Phillip Hue que por decir lo menos, tiene más de un desperfecto de seguridad. Investigadores del instituto de ciencia Weizmann y la Universidad Dalhousie en Halifax, pudieron hackear remotamente el bombillo desde su automóvil a una distancia de 70 metros. El proceso involucra en engañar a las luces a aceptar una actualización de firmware maliciosa y desde allí controlarlos remotamente. Esto no suena grave pero un ataque masivo en un área densamente poblada puede dañar el cableado eléctrico de una cuidad. (Ronen, 2018)

Otro caso alarmante es el presentado por un bombillo LIFX Mini White en 2019. Investigador de LimitedResults presenta la descomposición de un bombillo para poder acceder al WIFI de un hogar desde el dispositivo.

Inicialmente se asume que el bombillo está conectado a la red y la app de LIFX está en instalada y funciona de manera normal. Luego el agresor toma el bombillo y empieza el ataque de hackeo de hardware.

Ilustración 4.8 Desensamble de Bombillo LIFX (LimitedResults,2019)

El investigador alega que la parte más complicada es limpiar la tarjeta y remover el pegamento aprueba de fuego. Luego de obtener la tarjeta, se identifica el ESP32D0WDQ6, un SoC del ESPRESSIF. Luego unos pines se conectan a la tabla FT2232H. Las conexiones de arriba hacia abajo son el GND, VCC, 3.3V, ADBUS0, ADBUS1.

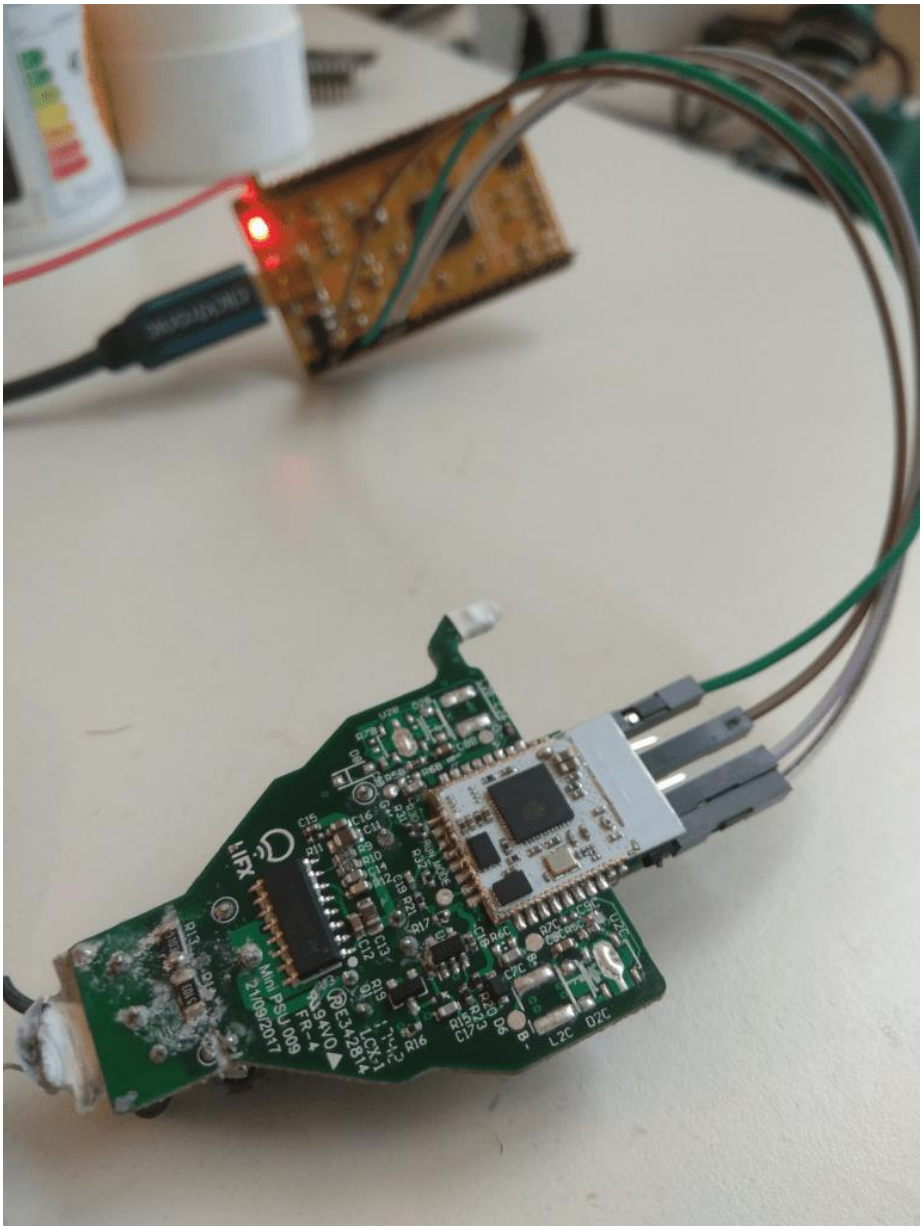


Ilustración 4.9 Conexiones (LimitedResults,2019)

Una vez la tarjeta tiene corriente, el LFFX LCM3 se reinicia y esto nos lleva directo al SSID.

```
LIFX LCM3 Booting.
Built on Thu Mar 29 19:07:10 2018
LIFX Timestamp: 1522310830000000000
Version: 3.40
Chip Rev: 1
PID: 0x0033
HW Ver: 007
MAC: d0:73:d5:30:bc:d1
[FATAL]  pairingkey.c:631:lx_hk_otp_paircode_get() Failed to Lock Row 0
HomeKit Setup Code: 729-42-992
Device Name: LIFX Mini W
I (530) wifi: wifi firmware version: f204566
I (530) wifi: config NVS flash: disabled
I (531) wifi: config nano formating: enabled
I (532) wifi: Init dynamic tx buffer num: 16
I (535) wifi: Init data frame dynamic rx buffer num: 16
I (540) wifi: Init management frame dynamic rx buffer num: 16
I (546) wifi: wifi driver task: 3ffccd64, prio:23, stack:3584
I (551) wifi: Init static rx buffer num: 4
I (555) wifi: Init dynamic rx buffer num: 16
I (559) wifi: wifi power manager task: 0x3ffcf20c prio: 21 stack: 2048
ESP-IDF Ver: v3.40-20180326-RC6
I (1708) wifi: mode : sta (d0:73:d5:30:bc:d1)
I (1711) wifi: sleep enable
I (1712) wifi: type: 1
I (11713) wifi: flush txq
I (11713) wifi: stop sw txq
I (11713) wifi: lmac stop hw txq
AJ_ConnectWifi returned 014
I (11732) wifi: mode : sta (d0:73:d5:30:bc:d1)
I (11733) wifi: sleep enable
I (11733) wifi: type: 1
I (11854) wifi: n:1 0, o:1 0, ap:255 255, sta:1 0, prof:1
I (13547) wifi: state: init -> auth (b0)
I (13549) wifi: state: auth -> assoc (0)
I (13554) wifi: state: assoc -> run (10)
I (13789) wifi: connected with KabelBox-0570, channel 1
I (16554) wifi: pm start, type:1

AJ_ConnectWifi returned 000
W (16621) mDNS: Configured IPV4 Multicast address 224.0.0.251
W (16621) mDNS: Configured IPV4 Multicast interface address 192.168.0.12
W (16627) mDNS: Configured IPV6 Multicast address FF02::FB
W (16630) mDNS: Configured IPV6 Multicast interface address FE80::D273:D5FF:FE31
[WARN]   /home/sam/lifx/esp/lifx-firmware-lcm3/src/platform/./os_platform.c:2172
[FATAL]  wan.c:734:lx_wan_stop() WAN teardown complete
[WARN]   /home/sam/lifx/esp/lifx-firmware-lcm3/src/platform/./os_platform.c:2173
[WARN]   /home/sam/lifx/esp/lifx-firmware-lcm3/src/platform/./os_platform.c:2177
Get IP address of host v2.broker.lifx.co
IP address is 146.148.44.137
```

Ilustración 4.10 Log boot (LimitedResults,2019)

Aquí se pueden encontrar tres vulnerabilidades. Primero, las credenciales del WI-FI están almacenadas como texto en el firmware. Un poco de investigación sobre archivos binarios flash.bin usando un editor de hex es lo único necesario para obtener las credenciales.

```
001f0000  fe ff ff ff 0b 00 00 00-ff ff ff ff ff ff ff ff-ff ff ff ff ff ff ff ff-ff ff ff ff 54 83 ce 56  ............................T..V
001f0020  aa aa aa aa aa aa aa aa-aa aa aa aa aa aa aa aa-aa aa aa aa aa aa aa aa-aa aa fa ff ff ff ff ff  ................................
001f0040  02 41 21 ff da fb 6a 15-72 77 5f 64 61 74 61 00-00 00 00 00 00 00 00 00-fc 03 ff ff 15 3a a4 44  .A!...j.rw_data.............:.D
001f0060  02 80 44 00 61 64 36 63-35 35 30 62 34 34 36 34-38 30 38 30 62 63 65 38-32 35 65 30 34 39 33 63  ..D.ad6c550b44648080bce825e0493c
001f0080  37 39 63 37 00 00 00 00-00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  79c7............................
001f00a0  00 00 00 00 00 ff ff ff-01 80 14 00 00 00 00 00-00 00 00 00 00 00 00 00-00 00 00 00 01 00 00 00  ................................
001f00c0  00 00 a4 00 4b 61 62 65-6c 42 6f 78 2d 30 35 37-30 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ....KabelBox-0570..............
001f00e0  00 00 00 00 00 33 32 33-32 33 36 33 38 33 34 33-33 33 31 33 39 33 36 33-38 33 38 33 32 33 34 33  .....3232363834333133936383832343
001f0100  31 33 37 33 35 33 34 33-38 33 32 33 34 00 00 00-00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  1373534383234..................
001f0120  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................................
001f0140  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................................
001f0160  00 00 00 00 00 00 fd ff-00 00 04 00 01 ff ff ff-e8 13 a4 00 4b 61 62 65-6c 42 6f 78 2d 30 35 37  ....................KabelBox-057
001f0180  30 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00-33 32 33 32 33 36 33 38  0...............32323638343
001f01a0  33 33 31 33 39 33 36 33-38 33 38 33 32 33 34 33-31 33 37 33 35 33 34 33-38 33 32 33 34 00 00 00  331393638383234313735343832 34...
001f01c0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................................
```

Ilustración 4.11 Llave WPA2 almacenada como texto (LimitedResults,2019)

Segundo, No hay configuraciones de seguridad. Según las configuraciones este dispositivo no tiene reinicio de seguridad, no encriptación de flash y el JTAG está desactivado.

```
xisco@E7440:~/esp/LIFX$ espefuse.py --port /dev/ttyUSB0 summary
espefuse.py v2.4.0-dev
Connecting.....
Security fuses:
FLASH_CRYPT_CNT         Flash encryption mode counter                    = 0 R/W (0x0)
FLASH_CRYPT_CONFIG      Flash encryption config (key tweak bits)         = 0 R/W (0x0)
CONSOLE_DEBUG_DISABLE   Disable ROM BASIC interpreter fallback           = 1 R/W (0x1)
ABS_DONE_0              secure boot enabled for bootloader               = 0 R/W (0x0)
ABS_DONE_1              secure boot abstract 1 locked                    = 0 R/W (0x0)
JTAG_DISABLE            Disable JTAG                                     = 0 R/W (0x0)
DISABLE_DL_ENCRYPT      Disable flash encryption in UART bootloader      = 0 R/W (0x0)
DISABLE_DL_DECRYPT      Disable flash decryption in UART bootloader      = 0 R/W (0x0)
DISABLE_DL_CACHE        Disable flash cache in UART bootloader           = 0 R/W (0x0)
BLK1                    Flash encryption key
  = 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 R/W
BLK2                    Secure boot key
  = 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 R/W
BLK3                    Variable Block 3
  = 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d1 bc 30 d5 73 d0 ff R/W

Efuse fuses:
WR_DIS                  Efuse write disable mask                         = 0 R/W (0x0)
RD_DIS                  Efuse read disablemask                           = 0 R/W (0x0)
CODING_SCHEME           Efuse variable block length scheme               = 1 R/W (0x1)
KEY_STATUS              Usage of efuse block 3 (reserved)                = 0 R/W (0x0)

Config fuses:
XPD_SDIO_FORCE          Ignore MTDI pin (GPIO12) for VDD_SDIO on reset   = 1 R/W (0x1)
XPD_SDIO_REG            If XPD_SDIO_FORCE, enable VDD_SDIO reg on reset  = 1 R/W (0x1)
XPD_SDIO_TIEH           If XPD_SDIO_FORCE & XPD_SDIO_REG, 1=3.3V 0=1.8V  = 0 R/W (0x0)
SPI_PAD_CONFIG_CLK      Override SD_CLK pad (GPIO6/SPICLK)               = 0 R/W (0x0)
SPI_PAD_CONFIG_Q        Override SD_DATA_0 pad (GPIO7/SPIQ)              = 0 R/W (0x0)
SPI_PAD_CONFIG_D        Override SD_DATA_1 pad (GPIO8/SPID)              = 0 R/W (0x0)
SPI_PAD_CONFIG_HD       Override SD_DATA_2 pad (GPIO9/SPIHD)             = 0 R/W (0x0)
SPI_PAD_CONFIG_CS0      Override SD_CMD pad (GPIO11/SPICS0)              = 0 R/W (0x0)
DISABLE_SDIO_HOST       Disable SDIO host                                = 0 R/W (0x0)

Identity fuses:
MAC                     MAC Address
  = 30:ae:a4:3e:6c:20 (CRC c5 OK) R/W
CHIP_VER_REV1           Silicon Revision 1                               = 1 R/W (0x1)
CHIP_VERSION            Reserved for future chip versions                = 0 R/W (0x0)
CHIP_PACKAGE            Chip package identifier                          = 0 R/W (0x0)

Calibration fuses:
BLK3_PART_RESERVE       BLOCK3 partially served for ADC calibration data  = 0 R/W (0x0)
ADC_VREF                Voltage reference calibration                    = 1100 R/W (0x0)

Flash voltage (VDD_SDIO) set to 1.8V by efuse.
```

Ilustración 4.12 Dispositivo Abierto (LimitedResults,2019)

Ultimo, La llave privada RSA y el certificado de Root son extraíbles. La llave RSA está presente como texto en el firmware y se usa para conectarse a la nube de LIFX.

Ilustración 4.13 Llave privada RSA (LimitedResults,2019)

El investigador se detiene aquí y contacto a LIFX sobre el asunto. La empresa luego presentó un reporte que las vulnerabilidades habían sido parchadas y rectificadas. (Limitedresults, 2019)

En la mayoría de ocasiones las empresas presentan una nueva versión de firmware para los dispositivos cuando estos defectos son encontrados por clientes afectados o su propio equipo de desarrollo. Sin embargo, muy pocos usuarios están al tanto de esta información y no adquieren la nueva versión. Por lo tanto, dejando una ventana abierta a aquellos que buscan hacer daño.

Lamentablemente la mayoría de dispositivos inteligentes no fueron diseñados con la seguridad como prioridad, aun siendo altamente sofisticados y costosos. Incluyendo los altamente riesgos dispositivos IoT. Muchos fabricantes deciden reducir gastos en protocolos de seguridad para reducir precios y así poder competir con grandes empresas, pero esto termina afectando a los usuarios.

Por lo tanto, los usuarios de dispositivos conectados a IoT deben seguir buenas prácticas al adquirir dispositivos inteligentes y entregarles su privacidad indiscriminadamente:

Ante todo, lo básico debe ser investigar los dispositivos antes de comprarlos. No solo se debe observar los precios y marcas conocidas. Se debe averiguar si ha habido incidentes de

seguridad y si hubo solución. También, si la empresa actualmente proporciona actualizaciones constantes de software y si son abiertas a todos los usuarios.

La vieja practica de mantener el usuario y contraseña por defecto tiene que ser destruida y olvidada. 15% de los ataques a dispositivos IoT son efectivos debido a que los usuarios no cambian esta información que es primer intento bruto de un hacker. Otra práctica que se debe eliminar es colocar todos los dispositivos, actuadores y IoT, en una sola red wifi, así evitando el contagio total de todos los dispositivos.

Entre otras prácticas se tiene que desactivar los permisos de privacidad y seguridad que usualmente incluyen la recolección de información comercial activa por defecto. Activar las actualizaciones automáticas y descargar aplicaciones solo desde tiendas oficiales. (Boros, 2020)

CAPITULO V. METODOLOGIA

5.1 Enfoque y Métodos

5.1.1Enfoque

La presente investigación dispondrá de un enfoque cuantitativo para realizar un análisis de las deficiencias de dispositivos inteligentes y la efectividad de la seguridad y privacidad que estos disponen.

5.1.2 Método

La metodología a seguir en la investigación será de inducción-deducción basada en la lógica de relacionar los problemas de generación de información.

5.2 Población y Muestra

La población de esta investigación está formada por los problemas de dispositivos IoT relacionados con generación de información y la muestra se enfocará en problemas de generación de información involucrando problemas de seguridad de hardware, software, leyes de protección de datos, y configuración de usuarios.

La presente investigación cuenta con una muestra no probabilística/ Dirigida. Las muestras elegidas han sido seleccionadas basadas en las distintas categorías de problemas de seguridad.

5.3 Unidad de análisis y respuesta

La unidad de análisis de esta investigación está compuesta por los dispositivos inteligentes, domótica.

5.4 Técnicas e instrumentos aplicados

La técnica aplicada en esta investigación será el análisis cuantitativo de los datos obtenidos de problemas de generación de información y sus soluciones respectivas como resolución viable. Adicionalmente, se utilizará la metodología MASP (Método de Análisis para Solución de Problemas) para evaluar cada una de los casos presentados en la investigación.

5.5 Fuentes de información

5.5.1 Primarias

Banco Interamericana de Desarrollo (BID) – Reporte de ciberseguridad 2020

Internet Society – Internet de las cosas

Height Dedicated Leading (HDL) – Smart Home Solutions

Instituto Panameño de Derecho y Nuevas Tecnologías (IPANDEC) – Estudio Centroamericano de Protección de Datos

ESET – Protección completa para un hogar inteligente

ESET – Tendencias en Ciberseguridad para el 2021

Constitución Nacional de Honduras

5.5.2 Secundarias

Eyal Ronen (2018) Creating an IoT Worm

Checkpoint (2017) The dark side of smart Lighting

Diego Solís (2016) La privacidad de la información generada por dispositivos de domótica

Alberto Tejero (2017) Metodología de análisis de riesgos para la mejora de la seguridad del internet de las cosas.

Carlos Raudales (2017) La brecha existente en la ciberseguridad en Honduras

Miguel Paz (2020) Analizar el uso de la domótica y su influencia en la comodidad de los hogares arequipeños

5.6 Cronología de trabajo

Tareas	Fecha de inicio	1	2	3	4	5	6	7	8	9	10
Actividades											
Revisión de Literatura	27/7										
Discusión de Idea de Proyecto	1/8										
Capitulo II parcial	8/8										
Capitulo II completo	15/8										
Capitulo III y IV	22/8										
Capítulo V y VI	5/9										
Capitulo VII, VIII, IX, y X	12/9										
Investigación completa	19/9										
Compromiso de desarrollo detallado	21/9										

Tabla 5.1 Cronograma de Trabajo (Autoría Propia,2021)

CAPITULO VI. RESULTADOS Y ANÁLISIS

Los dispositivos inteligentes están diseñados para mejorar el estilo de vida de los usuarios basados en ciberseguridad prevista por el fabricante y la confianza del usuario. Sin embargo, las medidas de seguridad de los dispositivos no siempre están a los estándares necesarios.

Para que un dispositivo inteligente conectado al internet de las cosas posea la seguridad y privacidad deseada por los usuarios este debe tener las siguientes características al general la información:

- Mantener la integridad de la información
- Asegurar la confidencialidad de la información
- Garantizar la disponibilidad de la información
- Proteger la propiedad de la información
- Cumplir con los objetivos de su diseño por instrucción del usuario

Es importante señalar que la información al estar conectada al internet de las cosas, siempre va a estar en un riesgo potencial por la naturaleza evolutiva del internet y sus asociados. No siempre se puede controlar o impedir todos los riesgos identificados ya sea por costo, uso, o tecnología, pero si es necesario mitigar los riesgos lo más posibles para mantener la confianza de los usuarios.

Para poder evaluar si un dispositivo está cumpliendo con las soluciones a problemas de generación de datos, el proceso se basará en la metodología MASP (Método de Análisis y Solución de Problemas) para poder identificar los problemas en cuestión y las acciones correctivas que se han presentado para mitigar los riesgos de pérdida o robo de información.

Este método ayudara a garantizar la uniformidad del análisis de ambos el problema y la solución provista. El método propone el siguiente orden para la solución de problemas:

1. Identificar le problema
2. Observar las características
3. Analizar las causas principales

4. Diseñar el plan de acción y ejecutarlo
5. Verificar la eficacia de la acción
6. Recapturar las acciones realizadas y planificar para el futuro.

Siguiendo esta metodología podremos evaluar los problemas existentes y las soluciones provistas para los distintos casos y se distinguirá la efectividad de las mismas.

6.1 Caso 1: Protocolos de Comunicación

Etapa	Descripción
Identificar el problema	Transmisión poco segura de datos Canales inalámbricos vulnerables
Observar las características	Transmisión de datos por medio de WI-FI y Bluetooth. Niveles bajos de interoperabilidad Acoplamiento de dispositivos Baja estabilidad de dispositivos
Analizar las causas	Dispositivos físicos con baja seguridad pueden ser atacados por medio de IoT debido a que los protocolos de comunicación no están desarrollados para información de dispositivos inteligentes.
Plan de Acción	Transición a protocolos de comunicación M2M diseñados para comunicación para dispositivos IoT.
Verificar la eficacia	El uso de los protocolos MQTT y CoAP como aplicación de baja capacidad pueden reemplazar los protocolos actuales transmisión de datos.
Conclusiones	El uso de protocolos M2M es la solución ideal desarrollado por la industria 4.0 para la automatización de maquinaria.

Tabla 6.1 MASP Protocolos de comunicación (Autoría Propia,2021)

Al aplicar la metodología a los protocolos de comunicación podemos ver que el este problema radica en la falta de un protocolo de comunicación dedicado a IoT enfocado en aparatos inteligentes. Y la verdad es que aun estos no se desarrollan por completo. El protocolo M2M está en una etapa de desarrollo por grandes empresas transnacionales como Tecnocom, UPS y FCC

Aquilia. En Honduras, Tigo apoya el desarrollo de IoT con M2M para empresas que deseen mejorar su negocio mediante la optimización de procesos.

M2M actualmente está implementado y diseñado para la automatización industrial de baja capacidad por medio del protocolo MQTT (Message Queuing Telemetry Transport) para una comunicación cableada ligera con una conectividad sin acceso remoto para procesos internos. Es ideal para la seguridad de transmisión de datos personales Al adaptar la tecnología M2M a un nivel residencial, problemas como la monitorización de la conectividad y el no poder controlar los dispositivos de manera remota pueden ser solucionados adaptando las características de la misma para redes más pequeñas.

La distribución de instrucciones generadas del HUB principal a otros dispositivos IoT desde una red aislada a la red principal no necesariamente debe ser controlada remotamente por los usuarios por la naturaleza autónoma de las instrucciones proporcionadas. Además, contrario al no ser un sistema altamente saturado como la maquinaria industrial, la conectividad no requerirá de monitorización prolongada.

6.2 Caso 2: Problemas de hardware

Etapa	Descripción
Identificar el problema	Sistemas físicos poco robustos y de baja calidad para reducir costos. Almacenamiento de datos comerciales Descontinuación de modelos
Observar las características	Fabricantes reducen costos de seguridad para reducir costos. Empresas en proceso de desarrollo quiebran y sus productos salen del mercado Nuevas tecnologías son desarrolladas y nuevos modelos salen al mercado Fabricantes incluyen permisos de recolección de datos activados para mejorar su mercadeo
Analizar las causas	La tecnología de dispositivos inteligentes está en el alza en los recientes años, debido a esto, los precios de modelos

	más recientes poseen precios elevados de construcción. Empresas emergentes con diseños similares a los originales reducen costos para competir con fabricantes de mayor nivel.
Plan de Acción	Creación de sistemas de estándares abiertos que pueden ser enlazados a dispositivos que hablan un lenguaje universal. Desactivar cualquier permiso de recolección de datos al momento de la instalación. Investigación previa de los usuarios al momento de realizar la compra de sistemas de dispositivos inteligentes.
Verificar la eficacia	No todos los sistemas pueden ser abiertos debido a que un lenguaje cerrado es más seguro que uno abierto, pero sistemas abiertos que no operen en radiofrecuencias de 2.4GHz pueden ser la solución viable.
Conclusiones	No es posible saber cuáles productos van a salir del mercado en el futuro, pero al realizar un sondeo antes de la instalación de dispositivos provee una imagen clara si el fabricante aun provee actualización de firmware, posee modelos más recientes o directamente si el fabricante salió del mercado.

Tabla 6.2 MASP Problemas de Hardware (Autoría Propia,2021)

Los principales causantes de este caso son inevitables de evitar debido a que el comercio progresa al mismo tiempo que evoluciona la tecnología. En 2016 se aproximó que habían más de 6 mil millones de dispositivos IoT conectados a la red. Para 2020, esta suma incremente 20.4 mil millones de unidades triplicando la cantidad de dispositivos presentes en el mercado. Esta cifra solo seguirá creciendo a medida que todos los aparatos domésticos y laborales se van modernizando y reemplazando.

Así como los televisores tradicionales fueron reemplazados con las pantallas planas y el cable análogo por cajas digitales. La mayoría de personas solo incrementan la cantidad de dispositivos inteligentes dentro de sus hogares. Pero no todos los países y sus habitantes son capaces de mantener un estilo de vida que vaya al mismo ritmo al que se van desarrollando nuevas tecnologías y modelos.

Al notar esta discrepancia y mercado disponible, fabricantes previos introducen productos de menor gama en comparación a sus productos estrella, así como nuevos inversionistas diseñan productos con menores especificaciones de procesamiento, memoria y tecnología menos reciente para satisfacer las necesidades de clientes que no pueden pagar los productos de primera línea. Esta práctica es buena para el comercio y para los usuarios que no son capaces de cubrir el costo de estos dispositivos, pero aun así desean una vida tecnificada.

Pero a medida que la competencia incrementa, el solo reducir componentes superficiales como el material de las coberturas, el vidrio de las pantallas táctiles y la capacidad del microprocesador no es lo suficiente para cumplir la rebaja de costos esperada. Allí es cuando los fabricantes comprometen la seguridad física de un dispositivo. Los sistemas se vuelven incapaces de resistir los ataques de fuerza bruta y permiten que entidades fuera del usuario tengan acceso a la información, así como la modificación o deterioro de la misma.

Ilustración 6.1 LIFX Mini White (LIFX,2021)

Este es el caso del foco inteligente LIFX Mini White el cual posee sistemas físicos cuestionables. Los investigadores al realizar el ataque al dispositivo afirman que no es necesario tener un equipo más caro de cien dólares americanos para poder entrar a las credenciales de WI-

FI que están escritas en los archivos como texto sin encriptación.

No hay configuraciones de seguridad disponibles para la mayoría de acceso físico al dispositivo, así como encriptación flash, no reinicio seguro o JTAG dejando al dispositivo vulnerable por muchos ángulos.

La seguridad física de un bombillo puede parecer trivial, pero no es el valor material del objeto, sino, la información de los enlaces dentro del dispositivo. Se debe estar al tanto que la ciberdelincuencia es desigual a la delincuencia física. Un asaltante cibernético atraca no con un cuchillo, sino con su cerbero, habilidades, experiencia e ingenio. Este incidente fue reportado al equipo técnico de LIFX, el cual confirmo las vulnerabilidades, y afirmo que han sido revocadas. (LIFX, 2019)

La empresa de dispositivos electrónicos afirmo que las credenciales del WIFI ahora están encriptadas, se agregaron nuevas configuraciones de seguridad y la llave privada RSA y el certificado Root también están encriptados. Todos los usuarios pueden acceder a estos cambios por medio de una actualización de firmware en su aplicación de LIFX. Como extra, alientan a sus usuarios a cambiar sus contraseñas y usuarios para que cualquier información vulnerable ya no sea relevante.

Este es uno de los casos de problemas de hardware que han sido solucionados y el fabricante le ha puesto un fin al asunto. Sin embargo, no siempre se tiene la fortuna de que un investigador haga una revisión de los sistemas de seguridad o de autenticación para ubicar estos problemas que aparentemente están bien hasta que fue demostrado lo contrario por terceros. Por lo tanto, es imperativo no reducir costos en asuntos de seguridad física.

Ilustración 6.2 Amazon Echo (Amazon,2021)

Lo mismo no se puede afirmar de la recolección de datos comerciales. Al adquirir un producto de este ámbito es la práctica que en el contrato y el manual de instrucciones se incluya la cláusula que se aprueba la recolección de los datos comerciales. Sin embargo, la línea entre datos comerciales y datos personales es delgada. En muchos casos varios de estos datos se pueden desactivar, pero es acción muy común solo aceptar lo que ocurre y seguir con la vida. Tal como en muchas páginas web, se aceptan todas las cookies, en vez de rechazar las posibles.

Esta práctica no es invasiva, pero nos estamos exponiendo a que terceros sepan nuestras preferencias, gustos, y registros de búsqueda, así como Alexa le puede enviar información no deseada a un contacto por accidente. Tal como ocurre con las conversaciones con el asistente virtual Amazon Echo que almacena toda esta información en la cuenta de Amazon.

Es posible eliminar esta información manualmente, pero no es una práctica totalmente segura porque al ser presionados por un senador, Amazon en 2019, admitió que los archivos también se almacenan en sus servidores y no siempre son completamente borradas de los servidores después de una solicitud de eliminación y a veces son utilizadas para el entrenamiento de sus inteligencias artificiales. Practica implementada también por empresas como Facebook, Apple y Uber para mencionar.

CNET nos explica los pasos para eliminar la mayoría de los archivos almacenados en la base de datos de Amazon. Para iniciar es necesario eliminar los registros vía la app, buscador o pedirle a Alexa que los elimine en la configuración de historial de grabaciones de voz.

Adicionalmente se debe contactar al servicio al cliente de Amazon para hacer una orden formar de remover tus registros. (Profis, 2019)

Por último, es muy difícil decir que empresas van a estar en funcionamiento dentro de 10 años, así como que productos se van a volver una sensación y cuales se van a hundir entre los miles de dispositivos presentes en el mercado. En la mayoría de casos, los compradores no tienen tanta suerte al adquirir un producto y dentro de pocos años este entra en obsolescencia y el usuario se ve con dos opciones. Reemplazar todo el sistema o aceptar un dispositivos o dispositivos obsoletos sin actualizaciones de funcionalidad ni parches de seguridad.

Pero no todo siempre está perdido, para todo problema planteado, hay más de una persona que desea resolverlo. Fundado en 2016 por David Puron e Isidro Nistal, Barbara IoT es una empresa que busca minimizar el impacto de la obsolescencia a las instalaciones de IoT. Aceptar entrar al internet de las cosas rotas ya no es necesario debido a los costos inasumibles o tener que comprometer el futuro del negocio.

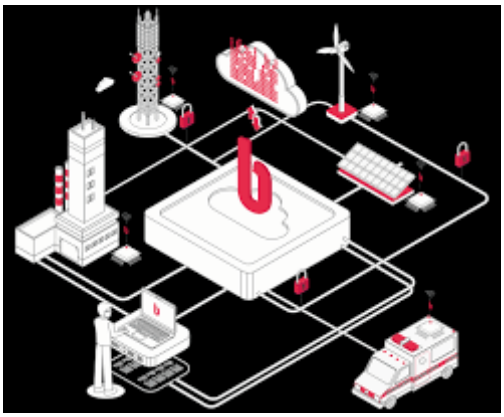


Ilustración 6.3 Barbara IoT (barbaraIoT,2021)

Esta empresa afirma que ataca los problemas de obsolescencia usando estándares de comunicación abiertos, haciendo mantenimientos correctivos periódicos para mejorar características y parches de seguridad e incluso reviviendo dispositivos heterogéneos y/o ya obsoletos.

Esto le da flexibilidad a la tecnología para poder conectar todos los dispositivos a la misma red IoT sin grandes inversiones cada cierta cantidad de años. Las ventajas del uso de

tecnología abierta son muchas. Yendo desde mayor disponibilidad, adaptaciones más sencillas, no depender de terceros y ciberseguridad más rápida y confiable son algunas de las más notorias.

Cabe hacer nota de que siempre es recomendable hacer una investigación previa de la empresa responsable por la instalación de las redes IoT y cuáles son sus productos en el mercado. Algunas de las señales que no debes adquirir estos dispositivos esta:

- No hay actualizaciones de firmware
- Muchas reseñas negativas sobre el producto
- No hay parches de seguridad
- El precio es muy inferior comparado a la competencia
- No hay soporte técnico

6.3 Caso 3: Problemas de confiabilidad de software

Etapa	Descripción
Identificar el problema	Protocolos de autenticación poco actualizados Poca flexibilidad de configuración Inseguridad de firmware Encriptación débil a nivel de transporte
Observar las características	La confiabilidad es el corazón de la protección de los datos digitales almacenados en un dispositivo. Softwares de protección estándar no siempre suelen ser seguros y pueden ser desencriptados por ciberdelincuentes. El firmware de dispositivos debe ser actualizados periódicamente por los fabricantes para obtener parches de seguridad por cualquier vulnerabilidad descubierta.
Analizar las causas	El firmware es uno de los primeros objetivos de los ciberdelincuentes.

	Reducción de configuraciones de seguridad para ahorrar costos y tiempo Uso de llaves de encriptación. Uso de ransomware
Plan de Acción	Uso de protección en tiempo real Actualización automática de Firmware Chequeo de vulnerabilidades periódico Bloqueo de router en caso de que el router se vea comprometido
Verificar la eficacia	El firmware y los protocolos de seguridad se deben actualizar constantemente para mantener la protección en tiempo real. El fabricante debe incluir todas las opciones de seguridad al meno de opciones y el usuario debe conocer y saber operar estas elecciones.
Conclusiones	La batalla de proteger el firmware es una guerra constante y larga. Mientras que se pueda acceder a la red por medio de un dispositivo inteligentes, el firmware del mismo estará bajo ataque.

Tabla 6.3 MASP Confiabilidad de Software (Autoría Propia,2021)

Una de las practicas comunes de muchos usuarios de PC o Laptops es descargar los Microsoft office y desbloquear la cuenta pagada por medio de un generador de llaves. Esta práctica hackea el firmware del programa para que este piense que una llave legitima fue introducida y se pueda hacer un bypass a todas las opciones de uso y este queda funcional.

Dejando de lado los riesgos legales, las personas, al realizar, esto están poniendo en riesgo toda la información en su dispositivo, porque esta llave aparentemente inocente puede contener una puerta trasera para acceder al dispositivo o bien puede recopilar toda la información que pase por el programa. Esto es con una llave encriptada diseñada para desbloquear un programa, pero los ataques no siempre son redundantes y sigilosos como el ejemplo anterior.

El malware diseñado para atacar el sistema de las computadoras avanza tan rápido como

evolucionan los parches de seguridad. Cualquier dispositivo IoT puede ser vulnerable a estos ataques y lo mejor es prevenir antes de tener que corregir estos asuntos. CHIPSEC es un framework de código abierto que funciona como una herramienta para poder probar el firmware de un sistema. Este framework, prueba varias vulnerabilidades conocidas y las notifica para que puedan ser prontamente parchadas por los fabricantes.

No es de sorprender que Adobe flash fuera retirado de los navegadores, ya que según el reporte de ciberseguridad de McAfee Labs, este represento casi un tercio de los ataques descubiertos por empresas de seguridad en los años 2014 y 2015. Ya bien fue que Adobe neutralizo el popular método de ataque Vector Spray y aumento la seguridad de Flash Player, este no incremento la calidad y complejidades del código de Flash. Ultimadamente en diciembre de 2020 se detuvo el soporte de Flash y en enero de 2021 la aplicación de Flash Player bloqueo el contenido Flash.

A nivel de dispositivos inteligentes el firmware puede tener vulnerabilidades de confiabilidad por motivos de defectos de modelo, código obsoleto, desactualización de sistema o aislamiento de la red. Así como este puede verse vulnerable ante ataques dirigidos a la capa de transporte por medio de malware o a la capa de aplicación en la autenticación de credenciales por medio de llaves maliciosas, robo de identidad o explotación de sistemas de recobro de contraseña y sesiones prolongadas.

Podemos ver el caso de bombillo Philip Hue, que puede causar grandes daños en zonas densamente pobladas con dispositivos IoT. El ataque funciona como una reacción en cadena donde el malware salta de un dispositivo al siguiente de una manera acelerada. 15, 000 bombillos conectados en una zona son los necesarios para que el daño se esparza a una ciudad completa, cifra que es muy fácil de superar en ciudades pobladas.

Ilustración 6.4 Philips Hue Bulb (Philips,2021)

El atacante envía un ataque remoto a la lampara y el usuario pierde el control de dispositivo. Siguiendo la rutina de si no funciona apague y vuelva a enconderlo. El usuario desconecta la lampara de la red. El atacante reemplaza la señal del bombillo con una actualización de firmware falsa y esta entra cautelosamente a la red dándole acceso al atacante al servidor por medio del bombillo. Ahora el ciber atacante tiene acceso a la laptop por una vulnerabilidad de un bombillo.

Este problema fue notificado a la empresa Philips Hue y en noviembre de 2019 este problema de firmware fue parchado. Philips Hue es una empresa que constantemente envía actualizaciones de firmware a sus clientes, aproximadamente una mensual. La mayoría siendo para mejorar el desempeño y eficacia del sistema.

Un problema similar apareció en el controlador Z-Wave Zipabox de Zipato, el cual es su modulo base ara adicionar otros módulos de control. En este dispositivo es posible desbloquear una puerta remotamente sin tener acceso a información previa, tomar la información del dispositivo para desbloquear otras puertas enlazadas a la red y, si fuera un apartamento residencia, desbloquear todas las puertas frontales de todos los vecinos.

Ilustración 6.5 Zipabox 2 (Zipato,2021)

Las vulnerabilidades se encontraron en la llave privada SSH, en el Pass-the-hash de Local API, y en el Pass-the-hash de Remote API. Todas las vulnerabilidades son criticas porque le dan acceso al atacante al dispositivo. Sin embargo, la autenticación API remota es la más preocupante. Dependiendo de la estructura y la extensión de implementación de dispositivos Zipato, es posible controlar todos los dispositivos en la red.

El investigador Charles Dardaman luego contacto a Zipato para informar sobre la vulnerabilidad. Zipato luego respondió que las vulnerabilidades habían sido parchadas y que se agregarían en la siguiente actualización de firmware. (Dardaman, 2019)

6.4 Caso 4: Leyes de protección de datos

Etapa	Descripción
Identificar el problema	No hay leyes de protección de datos digitales No hay estrategia nacional de ciberseguridad ni tampoco está en desarrollo No se cuenta con una CSIRT
Observar las características	La constitución nacional debe actualizarse a la situación actual para la protección de los habitantes. Al no tener planes de ciberseguridad el país es excluido de convenciones de importancia.

	El país se encuentra vulnerable contra ataques cibernéticos.
Analizar las causas	El alza de las casas inteligentes y las ciudades inteligentes atraerá ciberdelincuentes Todo país debe contar con una Estrategia nacional de ciberseguridad La constitución debe velar por la seguridad de todos los habitantes Es un derecho ciudadano a la privacidad
Plan de Acción	Proponer el desarrollo de una estrategia de ciberseguridad basado en países aledaños Formación de un CSERT Implementación de decretos para una ley que regule la protección de datos personales Convertirse en un país signatario de convenios contra la ciberseguridad
Verificar la eficacia	Se requieren de varios años de implementación para poder verificar la eficacia de las propuestas. Sin embargo, estas actividades no son cosa nueva, sino procesos por los que han pasado muchos países.
Conclusiones	La creación de una estrategia nacional de ciberseguridad, firmar convenios, y pasar decretos no es actividad sencilla y rápida. Esta puede tomar años en aprobarse, pero es de carácter urgente que Honduras comience a poner en práctica dichos proyectos. Ante todo, un grupo de respuesta puede ser construido para apoya a sus habitantes desprotegidos.

Tabla 1.4 MASP Leyes de Protección de Datos (Autoría Propia,2021)

Informar a una empresa de que su producto existente tiene vulnerabilidades y que pueden incurrir perdidas y/o demandas por los daños causados es distinta a hacer una propuesta a un gobierno de que publique un nuevo decreto. La ley de un país debe ser absoluta, aunque no siempre se cumpla, y este no es un proceso que se tome a la ligera. Una ley de protección de datos personales debe ser equitativa para todas las partes involucradas y cualquiera que haga una

propuesta pueden o no tomar ventaja de la misma para sus propios fines.

Esta es una de las razones por la cual el Congreso ha tomado tanto tiempo en revisar la ley de seguridad cibernética. Un nombre no tan apropiado cuando no encapsula completamente lo que es toda el área cibernética. La ley actual va por el nombre de "Ley Nacional de Ciberseguridad y Medidas de protección ante los actos de odio y discriminación en Internet y redes sociales". De esta ley, se han aprobado solo 19 de los 97 artículos para el año 2018.

Una de las razones del retraso de aprobación es la falta de un equipo de respuesta de ataques cibernéticos, globalmente conocidos como CSERT para que defiendan la población de la ciberdelincuencia. Honduras cuenta con una Fiscalía Especial de Protección a la Propiedad Industrial y Seguridad Informática (FEPROSI). Esta institución está a cargo de realizar investigaciones y formular los cargos para quienes quebrantes las leyes conexas a la regulación de la materia.

Honduras no posee una estrategia nacional de ciberseguridad, pero según el BID en su reporte de Ciberseguridad Honduras está en marcha a realizar este proyecto. Hasta que este sea aprobado, Honduras no cuenta con una ley vigente que regule la protección de datos personales. Se ha hecho el esfuerzo con la previa Ley mencionada, pero no es una ley que diferencia los diferentes tipos de penales que un país se debe adherir. Estas leyes propuestas no siempre se pueden encapsular dentro de Seguridad cibernética y sin una legislación centralizada, solo son distintas leyes que lo regulan.

Estas leyes conexas son:

Disposiciones específicas:

- Interferencia en los Datos: Artículos 214, Código Penal.
- Abuso de Dispositivos: Artículo 254, Código Penal.

Derecho Procesal

Procedimientos para la investigación de Delitos Informáticos:

- Código Procesal Penal

Disposiciones específicas:

- Interceptación de Datos sobre el Contenido: Artículo 223, Código Procesal Penal

Como parte del esfuerzo del gobierno para apoyar el desarrollo cibernético, Honduras tiene un capítulo de la Sociedad de Internet donde la academia, la empresa privada, y servidores públicos pueden intercambiar opiniones sobre ciberseguridad nacional. Esto con el objetivo de desarrollar mecanismos para la prosperidad y la seguridad del internet.

Aunque Honduras no es signatario en la convención de Budapest. El cuál es el primer tratado internacional que busca enfrentar los delitos informáticos y de internet mediante la armonización de leyes entre naciones. Mejorando las técnicas de investigación y la cooperación entre las naciones firmantes. El país ha buscado cooperación con Israel para la prevención, defensa y reacción antes ciberataques a institutos gubernamentales. Así como también han firmado un acuerdo con México para mejorar la cooperación en términos de educación naval y militar, por medio del adiestramiento y capacitación en temas de seguridad y defensa nacional, ciberseguridad y ciberdefensa.

Lastimosamente, en ningún momento se han mencionado los dispositivos inteligentes, ya sea como parte de las funciones de un instituto responsable por su administración o como una ley pasada para su regulación. Lo más cercano a esta es el Instituto Hondureño de ciencias, Tecnología e Innovación (TIC) que forma parte del sistema nacional para organizar actividades para la armonía entre la relación gobierno-academia-sector privado. Este ayuda al establecimiento de la infraestructura necesaria para avances de ciencia y tecnología, la mejora del sector productos y al acceso a mercados regionales y globales.

Sin embargo, hacer que esto se haga una realidad no es un solo un sueño. El país vecino, El Salvador, ha presentado su estrategia nacional de ciberseguridad en abril de 2021 y se puede usar como referencia para dar el primer paso a una Honduras más segura. El gobierno salvadoreño se ha enfocado en cinco dimensiones:

1. Política y estrategia
2. Cultura y sociedad
3. Educación, capacitación y habilidades
4. Marcos legales y regulatorios
5. Estándares, organizaciones y tecnologías

Ejes que funcionaran para desglosar los múltiples factores de la ciberseguridad de una manera progresiva por medio de estrategias que fortalezcan la capacidad cibernética del país.

Como principal estrategia se creará la entidad coordinadora de ciberseguridad (CSERT) para buscar apoyo en todos los sectores interesados, establecerá a líneas de acción y desarrollar las acciones necesarias. Entre las otras estrategias estará la concientización de materia de ciberseguridad, el reforzamiento en ciberseguridad ante las amenazas, el reforzamiento del marco jurídico para la cibercriminalidad, identificar, analizar y la gestión de riesgos.

El mismo reporte toma como referencia el documento "Un Abordaje Integral de la ciberseguridad" (Almagro, 2019) para realizar el marco de trabajo para definir la postura de ciberseguridad y como se deberá estructurar el programa y para ello se siguieron los siguientes pasos:

1. Priorizar y determinar el alcance
2. Orientación
3. Crear un perfil actual
4. Realizar una evaluación de riesgo
5. Crear un perfil objetivo
6. Determinar, analizar y priorizar las brechas
7. Implementar el plan de acción

Este marco de trabajo será implementado al menos una vez al año por todas las instituciones del gobierno para reportar el resultado a la entidad coordinadora de ciberseguridad.

Como puede ver todo problema tiene solución, aun las que requieran que un país movilice sus recursos para que sea logrado. Esto se debe que la privacidad es un derecho de todo ciudadano y el gobierno debe velar por la seguridad de todos sus ciudadanos. Impulsando al congreso a tomar mejores medidas preventivas y correctivas para el bien de la población. De esta manera los usuarios de dispositivos inteligentes y propietarios de casas domóticas tendrán una capa más de protección sobre la información generada dentro de sus hogares.

6.5 Caso 5: Prevenciones para Usuarios

El 95% de los ataques humanos se deben a errores humanos. Esto es porque es muy difícil concientizar a las personas del riesgo tangible al que se están enfrentando. Proteger la información es muy importante y no es fácil porque muchos perciben la seguridad como algo que impide trabajar más rápido.

Debemos asumir una cultura de ciberseguridad en esta nueva era tecnológica, que más allá de tener cuidado en las calles, también debemos tener cuido al conectarnos al internet y la información que dejamos que transite por ella. Aún más si se tiene o se planea tener una casa inteligente. La información que fluye a través de sus dispositivos móviles dice mucho del usuario, sus gustos, sus preferencias, su horario, sus contactos y muchas otras cosas importantes. Pero en el momento que se involucra la información del hogar, se pone en riesgo no solo la privacidad, sino que la seguridad del usuario y su familia.

Porque la domótica es comodidad y seguridad, solo si se utiliza de manera adecuada. Los dispositivos inteligentes tienen acceso a historial médico, puertas, ventanas, WIFI, toda aquella información digital presente en la vida de un usuario y esta puede ser usada en su contra. Y muchos de los incidentes que ocurren pudieron ser evitadas si se hubieran tomado medidas preventivas al memento de adquirir los dispositivos inteligentes. Esto ya no debería considerarse una tarea separada de la programación básica, sino como parte de la instalación.

No siempre el usuario está al tanto de toda la configuración que se lleva a cabo durante la estación. Sin embargo, como parte de la seguridad prometida en estos dispositivos, un servicio que explique y simplifique estas conductas de precaución deberían ser un requerimiento de las empresas a cargo de estos servicios.

Muchos dispositivos IoT no incluyen funciones de seguridad, talvez por el costo de desarrollo o por mantener el producto al nivel del mercado actual, pero es una realidad que tenemos que enfrentar y los usuarios se deben proteger.

Ya antes mencionados en esta investigación, entre los causantes de brechas de seguridad tenemos no dedicarle suficiente tiempo para configurar las funciones de seguridad y mantenerlas

adecuadas. Dejándole la puerta abierta a los delincuentes.

Mas allá de las aplicaciones llamativas de realizar el café por la mañana, descongelar la cena, mantener la temperatura perfecta y que nos abran la puerta cuando llegamos, debemos también observar el lado oscuro de las casas inteligentes y el riesgo en que se ponen a sí mismos los usuarios. Toda esta generación de información, esta interconectada a servidores y otros dispositivos que pueden ser explotadas por personas maliciosas.

Un malware es todo lo que puede ser necesario para destruir todo lo que se ha creado. El IoT y los dispositivos inteligentes se han vuelto uno de los principales objetivos de los hackers donde malware pueden convertirse en redes de robots para la denegación de servicio o simplemente bloquear los dispositivos. Debido a la gran cantidad de información personal distribuida por los mismos, los hackers han empezado a desarrollar softwares diseñados para atacar los dispositivos de domótica.

Ilustración 6.6 Nest Ecosystem (CNET,2019)

Hay casos más extremos donde la vida de un usuario puede ponerse en riesgo. En varias ocasiones la cámara de seguridad Nest ha sido atacada y secuestrada efectivamente. Los atacantes no dudaron en mandar advertencia que había un misil nuclear en la zona por un ataque terrorista. En otra instancia, una pareja fue amenazada con secuestrar su bebe y fingir estar en la habitación del bebe. Y, por último, en otra instancia, un hacker entro a la red de la cámara Nest y se comunicó con una mujer, insultándola y elevando la temperatura a 30º grados Celsius. Una temperatura no mortal, pero definitivamente nada placentera.

Todos estos ataques tuvieron algo en común, ninguno de los usuarios tenía la autenticación de 2 pasos activada y en algunos casos habían reutilizado contraseñas de otras páginas poco seguras, dándole el pase gratis a su red a los atacantes. La autenticación de 2 pasos puede parecer tediosa cuando estamos de prisa, pero si se toma en cuenta que este contribuye a que cada día el usuario llegue a su hogar inteligente y pueda disfrutar su comodidad tecnológica en paz, puede no ser tan frustrante.

Ahora que se conoce el peligro que se corre, debemos ver las formas de mitigar el riesgo que se corre, para evitar entrar en el 95% de los ataques que son por errores humanos.

Hay mucho que se puede hacer para evitar estos ataques, algunos que solo son necesarios una vez durante su instalación, otras que se deben hacer periódicamente y otras que se deben realizar todos los días:

Dispositivos IoT necesarios: Mas no siempre es mejor y no todos los dispositivos inteligentes son necesarios en la casa. Así como no todos es necesario que estén encendidos las 24 horas del día los 7 días de la semana. No es necesario tener los altavoces inteligentes encendidos cuando está durmiendo ni es necesario que la impresora de la oficina esta encendida fuera de las horas de trabajo.

Red IoT independiente: Esto funciona similar como la autenticación de dos pasos. Aunque un hacker pueda conectarse a un dispositivo inteligente. El atacante no tendrá acceso a todo en el hogar y esto le dará tiempo para reaccionar y desactivar el dispositivo contaminado. Esta red debe tener una contraseña robusta única para mejorar la seguridad contra ataques de fuerza bruta.

No contraseñas de fabrica: Las contraseñas de fabrica son asignadas por modelo en muchos casos y no es difícil conseguir la contraseña adjuntada al buscar el modelo. Las contraseñas deben ser distintas y seguras. De preferencia no deben incluir fechas de nacimiento, nombres de familiares o pines fácilmente descifrables como 1234. Si el dispositivo cuenta con autenticación de varios factores, es imperativo activarlos. Esto aplica para los dispositivos, cuentas, y routers.

Actualizaciones automáticas: Ningún sistema de seguridad es perfecto, pero muchas

empresas trabajan para hacer que estén un paso delante de los ciberdelincuentes. Pero para que este esfuerzo llegue a los dispositivos, es necesario que se instalen rutinariamente en los aparatos. Así mismo, también se debe revisar si ha habido actualizaciones de software u otros beneficios como soporte para contraseñas u otras características.

Antivirus: Es normal que las computadoras y celulares móviles tengan un antivirus como una capa extra de seguridad. ¿Porque nuestros demás dispositivos IoT no? televisores inteligentes traen la función de buscar antivirus y en otros casos es posible buscar servicios antimalware como AVAST o ESET en caso que no se pueda instalar directamente.

Ajustes de privacidad y seguridad: uno de los requerimientos de un dispositivo es tener una sección de ajustes donde se pueden hacer cambios de configuración, incluyendo los de seguridad. Desactivar la recolección de información comercial, el guardado del historial de voz y revisar que todos los protocolos de seguridad estén activos es una prioridad.

Solo paginas oficiales: Una buena acción puede terminar como un daño si no se es cuidadoso. No todas las páginas disponibles en internet son reales y beneficiosas. Uno de los trucos de hackers es plantar copias de páginas oficiales para obtener información confidencial y acceder al sistema de manera sencilla. De preferencia es mejor usar un hipervínculo desde dentro de la aplicación o el panel de los dispositivos.

Protege el router: Cambia la contraseña de fábrica, actualiza el firmware y software con regularidad, y cierra los puertos que no estén en función. El router principal es el corazón de todo el sistema y debe estar protegido para evitar que le resto de nuestros dispositivos se vean afectados.

Algunos de los pasos anteriores pueden ser complicado para usuarios que no estén interesados en la tecnología más allá de su confort o no tengan el tiempo de realizar estas rutinas por distintas razones. Pero es por estas razones que se vuelven un blanco vulnerable. En casos donde no se sabe que realizar es apropiado contactar a especialistas que ayuden con la configuración y puedan explicar paso a paso lo que se va a realizar. Por supuesto, no hay que olvidar cambiar la contraseña al final, por precaución.

CAPITULO VII. CONCLUSIONES

Por medio de los descubrimientos de la investigación podemos acertar que Honduras se encuentra en una situación precaria de enfrentarse a un ataque cibernético de alto nivel a dispositivos de domótica. Sin embargo, el nivel de automatización y digitalización de Honduras aún no ha llegado a un nivel crítico donde las personas y su información están directamente amenazadas. Honduras actualmente solo cuenta con un distribuidor de esta tecnología que limita grandemente la expansión de la misma. Dándole al país tiempo que requiere para elevar su nivel de seguridad.

El mejoramiento de seguridad físico y lógico de dispositivos, uso de nuevos protocolos de transmisión y recepción de datos y la institución de leyes de protección de datos en los siguientes años dictaran la protección que contara los usuarios de dispositivos inteligentes en el país. Al establecer estas medidas y fortalecer las actuales, el país estaría previendo para el futuro cercano cuando los hogares se automaticen. De tal forma, que se podrá prevenir dejar los datos e información personal expuesto a la ciberdelincuencia.

Los casos de estudio vistos en la investigación nos permiten inferir que todo problema de seguridad y privacidad están ligados a los dominios de problemática expuestos y estos poseen una solución realizable por fabricantes, usuarios y el apoyo del gobierno para afianzar la respuesta a incidentes y formar un marco concreto de como procesar los ataques y los atacantes. Al resolver de manera proactiva y continua estos problemas, el país se podrá automatizar sin problemas. Esto le dará una ventaja sobre aquellos que han hecho este proceso a la inversa. Un proceso que es muy difícil de reversar debido a la expansión exponencial de la automatización una vez que comienza.

CAPITULO VIII. RECOMENDACIONES

1. Se recomienda al gobierno nacional de honduras acelerar la aprobación de “La ley de ciberseguridad y medidas de protección ante los actos de odio y discriminación en Internet y redes sociales” actual y proseguir con el desarrollo de una Estrategia Nacional de Seguridad. Partiendo de esta, se podrá realizar la formación del grupo de respuesta a ataques cibernéticos CSERT para

el apoyo de víctimas de ataques a la red y se encargue del análisis de situaciones y responda a las amenazas.

2. Así mismo, se recomienda basar las estrategias de ciberseguridad en marcos previamente establecidos acotados a la situación actual de Honduras. Preferencialmente, se recomienda firmar el convenio de Budapest seguido los estándares del primer tratado para hacerle frente a los delitos informáticos. De esta manera se podrá depender de naciones más avanzadas como base para generar nuevas leyes que apoyen la seguridad cibernética.

3. A los fabricantes se recomienda utilizar sistemas de actualización constante para mantener el servidor y los usuarios actualizados en cuestión de nuevas configuraciones de seguridad y actualizaciones de firmware. A la vez, se recomienda usar protocolos de autenticación de dos pasos como configuración de contraseña predeterminado para evitar robo de identidad de usuarios que repitan contraseñas con sitios web poco seguros o dejen sus contraseñas expuestas o de bajo nivel de seguridad.

4. A usuarios de dispositivos inteligentes, se les recomienda no reutilizar contraseñas de otros sitios web, darles preferencia a los protocolos de seguridad que, al acceso rápido, y no utilizar versiones “desbloqueadas” de productos pagados para evadir el costo ya que esto pone en riesgo al dispositivo y la red. Se exhorta la prevención antes de la corrección; hacer una revisión preliminar de las características del dispositivo, la reputación de una empresa y posibles problemas que podrían presentarse en su hogar reduce de gran manera los riesgos potenciales al sistema.

CAPITULO IX. BIBLIOGRAFIA

Almagro, L. (2019). *Un abordaje Integral de la Ciberseguridad.* OEA.

Anscombe, T. (2018). *Proteccion cmpleta para un hogar inteligente.* Bratislava: ESET.

Anscombe, T. (6 de agosto de 2020). *Welivesecurity*. Obtenido de https://www.welivesecurity.com/2020/08/06/blackbaud-data-breach-what-you-should-know/

Araico, N. (19 de noviembre de 2019). *ABB*. Obtenido de https://www.abb-conversations.com/es/2019/11/beneficios-de-la-domotica/

Arquitectura, A. (22 de diciembre de 2001). *Arqhys Arquitectura*. Obtenido de https://www.arqhys.com/arquitectura/domotica-historia.html

BID. (2020). *CIBERSEGURIDAD.* OEA.

Boros, B. (2020). Una casa más inteligente es más vulnerable. *The conversation*.

Constantino, I. (2011). Domotica e inmotica. *Universidad Veracruzana*, 24-25.

Doménech, F. (17 de abril de 2020). *OpenMind*. Obtenido de https://www.bbvaopenmind.com/tecnologia/mundo-digital/evitar-la-domotica-arruine-nuestra-ciberseguridad/

HDL. (2011). *Smart Home Solutions.* Guangzhou: Guangzhou Hedong Electronic CO.

Honduras, C. d. (2013). Decreto legislativo No. 10-2013. *La Caseta*.

LIFX. (30 de enero de 2019). *LIFX*. Obtenido de https://www.lifx.com/pages/privacy-security-responsible-disclosure-of-security-vulnerabilities

Limitedresults. (23 de enero de 2019). *LimitedResults*. Obtenido de https://limitedresults.com/2019/01/pwn-the-lifx-mini-white/

MEGATK. (22 de agosto de 2021). *MEGATK*. Obtenido de https://megatk.net/soluciones-eficiencia-energetica.html

Moyr, J. M. (2010). *Manual de la Domotica.* España: Creaciones Copyright.

Muelaner, J. (27 de abril de 2021). *Digi-Key*. Obtenido de https://www.digikey.com/es/articles/application-layer-protocol-options-for-m2m-and-iot-functionality

Paz, M. A. (2020). Analizar el uso de la domótica y su influencia en la comodidad de los hogares arequipeños. *Universidad COntinental*, 28.

Profis, S. (3 de julio de 2019). *CNET*. Obtenido de https://www.cnet.com/home/smart-home/you-can-finally-delete-most-of-your-amazon-echo-transcripts-heres-how/

RAE. (15 de agosto de 2021). *Definicion.de*. Obtenido de https://definicion.de/software/

RAE. (22 de agosto de 2021). *DLE RAE*. Obtenido de https://dle.rae.es/inteligente

RAE. (15 de agosto de 2021). *RAE*. Obtenido de https://dle.rae.es/precauci%C3%B3n

Ronen, E. (21 de noviembre de 2018). *Eyalro*. Obtenido de https://eyalro.net/project/iotworm.html

Rose, K. (2015). *La internet de las cosas - una breve reseña.* Geneva: Internet society.

Salazar, J. (2016). *INTERNET DE LAS COSAS.* Praha: České vysoké učení technické v Praze.

Sistemas, D. (22 de agosto de 2021). *DOmotica Sistemas*. Obtenido de https://domoticasistemas.com/tienda/tutoriales/1_sistemas-existentes-tipos-y-estandares.html

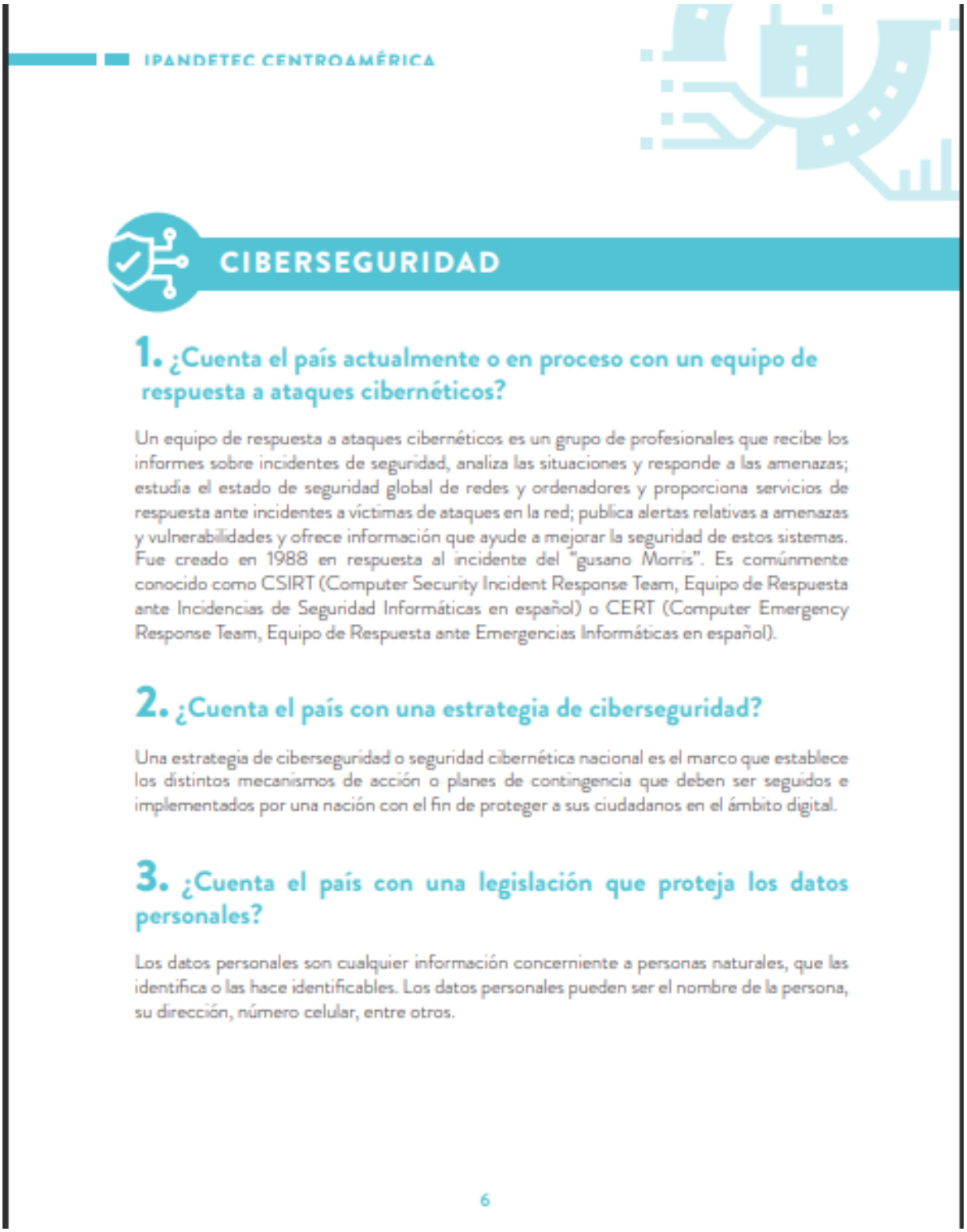
Tejero, A. (2017). Metodologia de analisis de riesgo para la mejora del Internet de las cosas. *Universidad Politecnica de Madrid*.

Tomé, E. (2019). Estudio Centroamericano dep proteccion de datos. *IPANDEC*, 7.

CAPITULO X. ANEXOS

ETAPA	DESCRIPCIÓN
ETAPA 1 IDENTIFICACIÓN DEL PROBLEMA	Elección del problema Histórico del problema
	Mostrar pérdidas actuales y ganancias viables
	Hacer el análisis de Pareto (demuestra la frecuencia de las ocurrencias (de mayor a menor)) a través del grafico
	Nombrar responsables
ETAPA 2 OBSERVACIÓN	Descubra las características del problema a través de la recolección de datos y observación del sitio
	Cronograma, presupuesto y meta Definición de las causas influyentes
ETAPA 3 ANALISIS	Elección de las causas más probables (hipótesis)
	Análisis de las causas más probables (verificación de las hipótesis)
ETAPA 4 PLAN DE ACCIÓN	Elaboración de estrategia de acción Elaboración de plan de acción para el bloqueo y revisión del cronograma y presupuesto final
ETAPA 5 ACCIÓN	Entrenamiento
	Ejecución de acción
ETAPA 6 VERIFICACIÓN	Comparación de resultados Listado de los efectos secundarios
	Verificación de la continuidad o no del problema
ETAPA 7 ESTANDARIZAR	Elaboración o alteración de un patrón
	Comunicación
	Educación y entrenamiento Acompañamiento en la utilización de un patrón
ETAPA 8 CONCLUSIÓN	Relación de los problemas remanentes
	Planificación del ataque a los problemas remanentes
	Reflexión

Tabla 10.1 Ejemplo Aplicación MASP (Jeison,2018



IPANDETEC CENTROAMÉRICA

CIBERSEGURIDAD

1. ¿Cuenta el país actualmente o en proceso con un equipo de respuesta a ataques cibernéticos?

Un equipo de respuesta a ataques cibernéticos es un grupo de profesionales que recibe los informes sobre incidentes de seguridad, analiza las situaciones y responde a las amenazas; estudia el estado de seguridad global de redes y ordenadores y proporciona servicios de respuesta ante incidentes a víctimas de ataques en la red; publica alertas relativas a amenazas y vulnerabilidades y ofrece información que ayude a mejorar la seguridad de estos sistemas. Fue creado en 1988 en respuesta al incidente del "gusano Morris". Es comúnmente conocido como CSIRT (Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad Informáticas en español) o CERT (Computer Emergency Response Team, Equipo de Respuesta ante Emergencias Informáticas en español).

2. ¿Cuenta el país con una estrategia de ciberseguridad?

Una estrategia de ciberseguridad o seguridad cibernética nacional es el marco que establece los distintos mecanismos de acción o planes de contingencia que deben ser seguidos e implementados por una nación con el fin de proteger a sus ciudadanos en el ámbito digital.

3. ¿Cuenta el país con una legislación que proteja los datos personales?

Los datos personales son cualquier información concerniente a personas naturales, que las identifica o las hace identificables. Los datos personales pueden ser el nombre de la persona, su dirección, número celular, entre otros.

6

Ilustración 10.1 Cuestionario Ejemplo de ciberseguridad parte 1 (IPANDEC,2020)

4. ¿Cuenta el país con una agencia o ministerio de gobierno especializado en tecnologías de la información?

La tecnología o tecnologías de la información y la comunicación (TIC) son un conjunto de servicios de redes y aparatos que tiene como objetivo mejorar la calidad de vida del ser humano dentro de un entorno. La tecnología de la información incluye aquellas herramientas computacionales e informáticas que procesan, almacenan y recuperan información, y pueden ser una herramienta muy útil para estudiantes por ejemplo, ya que podrían beneficiarse con el flujo de información que permiten[1] acceder más allá del uso común de las redes sociales. Gracias a su creciente uso, los países han desarrollado diferentes entes gubernamentales para poder proteger a sus ciudadanos, educar a la población y sacar provecho de ella.

5. ¿Participa el país en foros o encuentros regionales multisectoriales en materia de ciberseguridad?

La retroalimentación y el poder intercambiar información entre organismos de cada país siempre es importante para el avance de las diversas materias en las que un estado muestre interés. Esta pregunta califica la participación de agentes del Estado en reuniones o foros regionales multisectoriales sobre ciberseguridad.

6. ¿Cuenta el país con una legislación conexa que regule la materia?

Muchas veces los países y sus legisladores crean leyes que tratan la ciberseguridad; sin embargo, estas no se encuentran dentro de un capítulo llamado "Seguridad cibernética" o algo parecido. También sucede que no existe una legislación centralizada, sino diferentes leyes que regulan.

7. ¿Cuenta el país con grupos de trabajo multisectoriales que trabajen en ciberseguridad?

Para poder participar en encuentros en el exterior y exportar experiencias y/o conocimientos debe existir un robusto intercambio entre los diferentes sectores del país. Esta pregunta califica si entes estatales, sociedad civil, academia, entre otros actores mantienen constante comunicación mediante grupos de trabajo o coaliciones.

Ilustración 10.2 Cuestionario Ejemplo de ciberseguridad parte 2 (IPANDEC,2020)

CIBERDELINCUENCIA

8. ¿Es el país signatario de convenios o tratados contra la ciberdelincuencia?

El Convenio de Budapest, o Convenio sobre Cibercriminalidad, es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes entre naciones, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones firmantes[2].

9. ¿Están los delitos cibernéticos debidamente tipificados en la legislación penal?

El Convenio sobre Cibercriminalidad enmarca los diferentes tipos penales que deben ser adheridos por cada país firmante. Sin embargo, muchos países sin firmar el convenio y por iniciativa propia, o buscando regular los ciberdelitos antes de su formal entrada a los países signatarios del Convenio proponen y sancionan iniciativas de ley que buscan incluir los delitos cibernéticos a la legislación penal.

10. ¿Cuenta el país con tribunales o agencias de investigación especializadas en informática?

Investigar o juzgar delitos cibernéticos requiere personal altamente calificado, con las herramientas necesarias y todos los recursos posibles para una adecuada investigación.

Ilustración 10.3 Cuestionario Ejemplo de ciberseguridad parte 3 (IPANDEC,2020)

HONDURAS

1. ¿Cuenta el país actualmente o en proceso con un equipo de respuesta a ataques cibernéticos?

Honduras no cuenta con un equipo nacional de ciberseguridad que defienda a la población de la ciberdelincuencia.

2. ¿Cuenta el país con una estrategia de ciberseguridad?

Honduras no cuenta con una política nacional cibernética que les permita asegurar el espacio cibernético de su país.

3. ¿Cuenta el país con una legislación que proteja los datos personales?

En Honduras actualmente no existe una ley vigente que regule la protección de datos personales,

no obstante, se han hecho esfuerzos en este sentido. En el año 2015, un proyecto de Ley de Protección de Datos Personales fue impulsado por el entonces vicepresidente del Congreso Nacional, el diputado Antonio Rivera Callejas. Este proyecto se basó en el anteproyecto que fue presentado por el Instituto Nacional de Acceso a la Información Pública en el año 2013 con el apoyo de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID). Actualmente, el proyecto sigue en proceso de debate en el hemiciclo legislativo. El último debate se llevó a cabo en el mes de abril del año 2018. Sin embargo, este proceso se ha retrasado más de lo esperado, considerando que solo se han aprobado 19 de los 97 artículos que contiene el proyecto.

20

Ilustración 10.4 Cuestionario Honduras de ciberseguridad parte 1(IPANDEC,2020)

A falta de una legislación especial, los datos personales en Honduras cuentan con al menos una protección que se reconoce en la Ley del Instituto de Acceso a la Información Pública, Decreto Legislativo No. 170 – 2006. En los artículos 24 al 26 de esta ley se reconoce el Hábeas Data, la protección de los datos personales y presenta la figura del Comisionado Nacional de Derechos Humanos como una oficina facultada para incoar acciones para la protección de datos personales; además establece una prohibición en la cual ninguna persona puede solicitar a otros datos personales que puedan generar algún tipo de discriminación o poner en riesgo los derechos morales y patrimoniales de ese individuo[28].

4. ¿Cuenta el país con una agencia o ministerio de gobierno especializado en tecnologías de la información?

Honduras, dentro de su organigrama estatal, mantiene el Instituto Hondureño de Ciencia, Tecnología y la Innovación (IHCIETI)[29], el cual forma parte del Sistema Nacional de Ciencia, Tecnología e Innovación. El IHCIETI organiza actividades que promueven la armonización de la relación gobierno-academia-sector privado, la mejora de políticas y programas, el desarrollo de las capacidades y competencias del capital humano, el establecimiento de la infraestructura necesaria para el avance de la ciencia y la tecnología, la mejora de la competitividad del sector productivo y el acceso a mercados regionales y globales.

5. ¿Participa el país en foros o encuentros regionales multisectoriales en materia de ciberseguridad?

Honduras, por medio de su gobierno, academia, sociedad civil, entre otros sectores, acude y es representado anualmente en el Foro de Gobernanza de Internet (IGF) que la Organización de Naciones Unidas (ONU) realiza anualmente. Este evento es un espacio neutral donde los actores preocupados por Internet y su futuro pueden compartir sus ideas sobre los asuntos relacionados con la política y el desarrollo de Internet, sin importar su procedencia. Este Foro a su vez tiene iniciativas regionales y nacionales, siendo celebrado cada año el Foro de Gobernanza de Internet de Honduras y el Latin American and the Caribbean Internet Governance Forum (Foro de Gobernanza de Internet de Latinoamérica y el Caribe LAC IGF, por sus siglas en inglés).

Recientemente, participaron de una reunión de alto nivel entre el FOPREL y el GLACY+, referente al estado de ciberseguridad en el país y la posible adhesión al Convenio de Budapest.

Ilustración 10.5 Cuestionario Honduras de ciberseguridad parte 2(IPANDEC,2020)

6. ¿Cuenta el país con una legislación conexa que regule la materia?

Honduras tiene diferentes disposiciones conexas relativas a la ciberseguridad[30]:

Disposiciones especificas:

- Interferencia en los Datos: Artículos 214, Código Penal.
- Abuso de Dispositivos: Artículo 254, Código Penal.

Derecho Procesal

Procedimientos para la investigación de Delitos Informáticos:

- Código Procesal Penal

Disposiciones especificas:

- Interceptación de Datos sobre el Contenido: Artículo 223, Código Procesal Penal.

7. ¿Cuenta el país con grupos de trabajo multisectoriales que trabajen en ciberseguridad?

Honduras tiene un capítulo de la Sociedad de Internet donde tanto la academia, miembros de la empresa privada, servidores públicos, entre otros ciudadanos pueden generar intercambios y sinergia de opiniones en favor de la ciberseguridad de la nación. Esta organización se dedica al desarrollo de internet y dentro de sus grupos de trabajo se encuentra el Observatorio sobre Ciberseguridad Global (GCO), un Grupo de Interés Especial (SIG) de la Internet Society (ISOC). La GCO-SIG fue fundada para desarrollar los mecanismos adecuados de participación, la colaboración y el diálogo para proponer cómo construir la confianza, la prosperidad y la seguridad en Internet, equilibrar las cuestiones de seguridad nacional con los derechos humanos y fundamentales (tales como, la privacidad, la libertad de expresión, etc.) y permitir la innovación para fomentar el despliegue de tecnologías emergentes bajo las más estrictas normas de privacidad, protección de datos y seguridad.

8. ¿Es el país signatario de convenios o tratados contra la ciberdelincuencia?

Honduras no es signataria del Convenio de Budapest. Sin embargo, recientemente congresistas de la comisión especial multipartidaria del Congreso Nacional para la aprobación de una ley de ciberseguridad recomendaron la adhesión al Convenio[31]. Esta recomendación es efectuada

Ilustración 10.6 Cuestionario Honduras de ciberseguridad parte 3 (IPANDEC,2020)

después de una reunión entre congresistas con miembros del GLACY+ en reunión de FOPREL en San Salvador[32].

La American Chamber of Commerce in Honduras es signataria del Llamamiento de París para la confianza y la seguridad en el ciberespacio, consistente en impulsar iniciativas acerca de nuevas cuestiones cuya regulación es por ahora insuficiente, trabajando desde distintos sectores[33].

9. ¿Están los delitos cibernéticos debidamente tipificados en la legislación penal?

Actualmente, el Congreso hondureño se apresta a aprobar en Tercer Debate una Ley de Ciberseguridad y Medidas de Protección ante los actos de Odio y Discriminación en Internet. La iniciativa ha sido objeto de rechazo por parte de diversos sectores porque establece censura previa y pretende imponer obligaciones a los administradores de sitios web [34].
Inclusive el Relator para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH), instancia de la Organización de Estados Americanos, lamentó y criticó los matices del proyecto, los cuales podrían ser claros violadores de la libertad de expresión, expresó[35].

La iniciativa legisla sobre delitos ya legislados y su regulación del odio en las redes sociales es muy general, lo que podría conllevar a interpretaciones ambiguas por parte del juzgador. La Ley continúa siendo ambigua, imprecisa y desproporcionada para determinar qué contenido digital debe entenderse como "amenaza, calumnia e injuria", debido a que en el contexto actual de Honduras esto puede ser utilizado para retirar y bloquear contenido.

Se regula la creación de un Comité Interinstitucional de Ciberseguridad, el cual será el encargado de desarrollar e implementar la Estrategia Nacional de Ciberseguridad. Sin embargo, únicamente se integrará con entidades de Gobierno. La ausencia del enfoque de múltiples partes interesadas es una debilidad, la falta de coordinación y colaboración con otros sectores como sociedad civil, sector privado, comunidad técnica y académica es un peligro, porque la Estrategia será la base para la creación de futuras políticas públicas relacionadas a ciberseguridad[36].

10. ¿Cuenta el país con tribunales o agencias de investigación especializadas en informática?

Honduras tiene una Fiscalía Especial de Protección a la Propiedad Industrial y Seguridad Informática (FEPROSI, por sus siglas en español), encargada de realizar investigaciones y formular cargos a quienes se presuman hayan quebrantado la ley penal.

Ilustración 10.7 Cuestionario Honduras de ciberseguridad parte 4 (IPANDEC,2020)

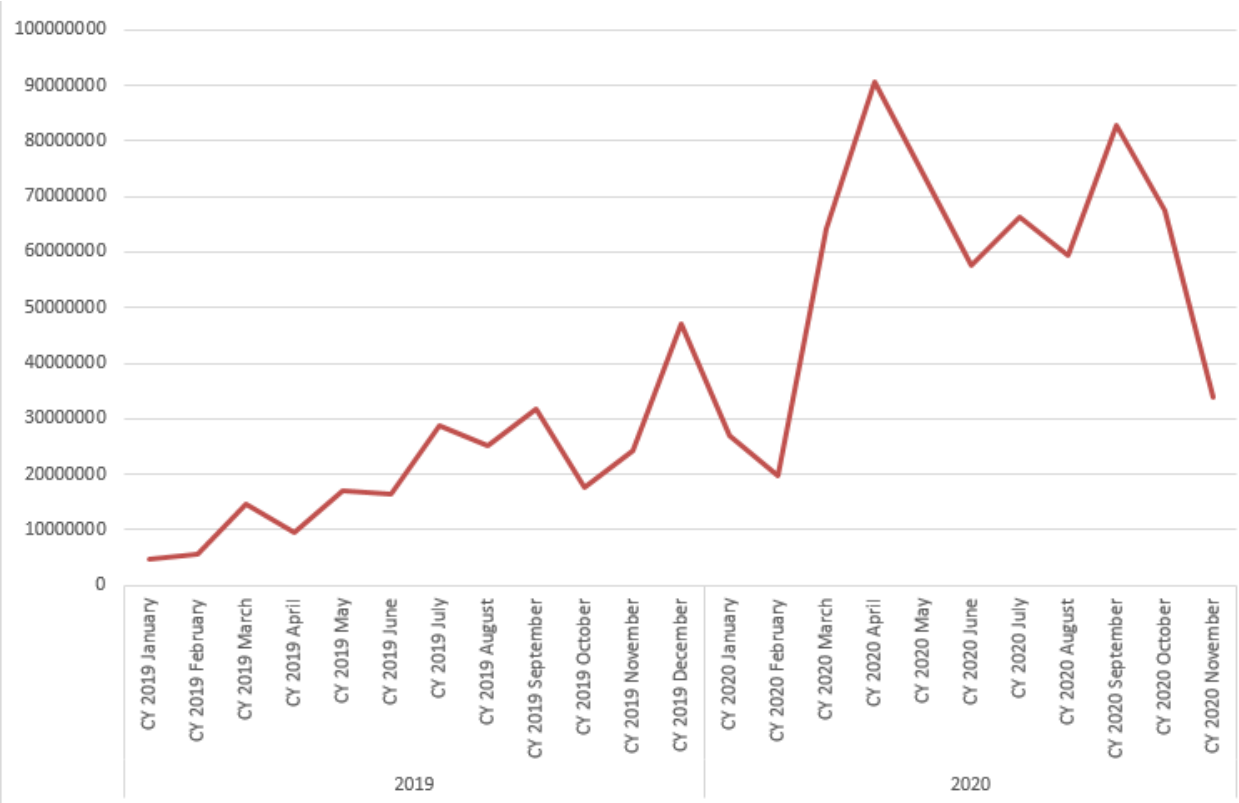


Ilustración 10.8 Grafica de ataques cibernéticos Remotos Latinoamérica (Kapersky,2020)

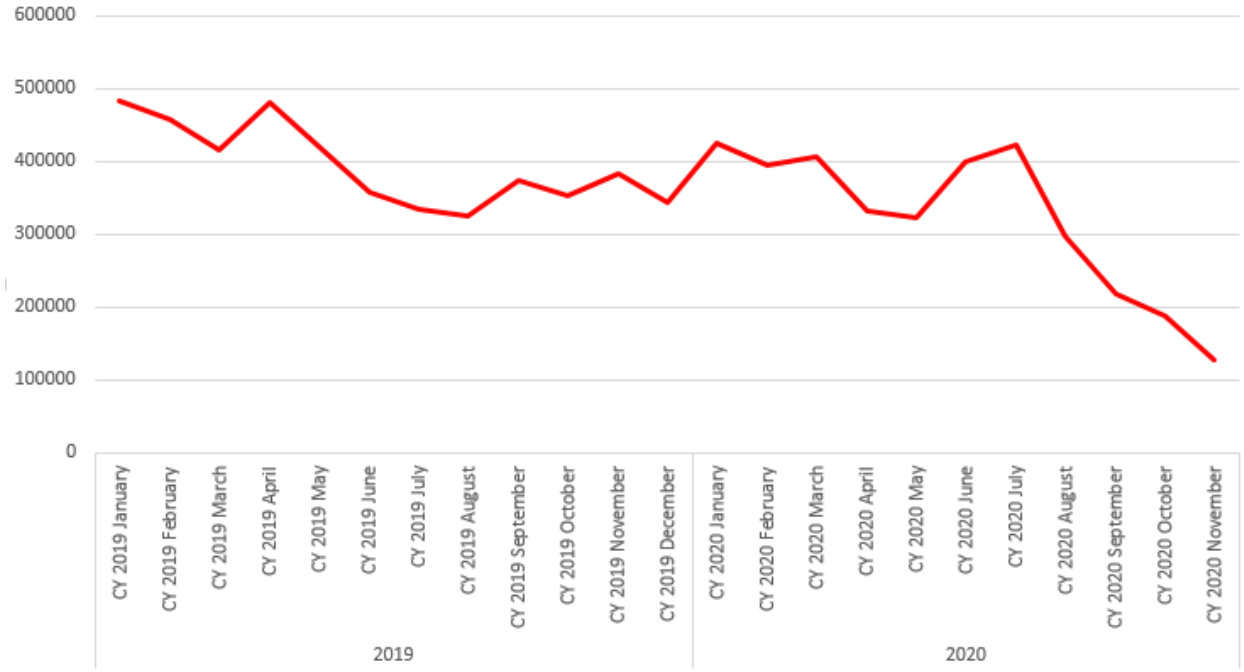


Ilustración 10.9 Grafica de ataques cibernéticos Ransomware Latinoamérica (Kapersky,2020)