TRABAJO DE GRADO

IDENTIFICACION DE RIESGOS EN LA SEGURIDAD DE LA INFORMACION DE CAMARAS DE VIGILANCIA DOMESTICAS EN ENTORNOS IOT

SYLVIA MARGARITA RIBERO CORZO

YEISON ANDRES PRIETO GUERRERO

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

2021

TRABAJO DE GRADO

IDENTIFICACION DE RIESGOS EN LA SEGURIDAD DE LA INFORMACION DE CAMARAS DE VIGILANCIA DOMESTICAS EN ENTORNOS IOT

SYLVIA MARGARITA RIBERO CORZO

YEISON ANDRES PRIETO GUERRERO

Trabajo de grado presentado para optar al título de Especialista en Seguridad de la Información

Docente

MSc. Carlos Mauricio Blanco Muñoz.
Profesor Especialización en Seguridad de la Información

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

2021

Atribución-NoComercial 4.0 Internacional (CC BY-NC 4.0)

This is a human-readable summary of (and not a substitute for) the license. Advertencia.

Usted es libre de:

Compartir — copiar y redistribuir el material en cualquier medio o formato

Adaptar — remezclar, transformar y construir a partir del material

La licenciante no puede revocar estas libertades en tanto usted siga los términos de la licencia

Bajo los siguientes términos:

Atribución — Usted debe dar crédito de manera adecuada, brindar un enlace a la licencia, e indicar si se han realizado cambios. Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que usted o su uso tienen el apoyo de la licenciante.

NoComercial — Usted no puede hacer uso del material con propósitos comerciales.

No hay restricciones adicionales — No puede aplicar términos legales ni medidas tecnológicas que restrinjan legalmente a otras a hacer cualquier uso permitido por la licencia.

TABLA DE CONTENIDO

LISTA DE FIGURAS

Pág.

.

.

LISTA DE TABLAS

Pág.

1. INTRODUCCIÓN

Internet de las cosas (En inglés Internet of Tingas, IOT) se refiere a la interconexión digital de objetos cotidianos con internet, este concepto lo propuso Kevin Aston en el MIT AUTO-ID LABORATORY[1] en 1999 donde se realizaban investigaciones en el campo de radiofrecuencia en red (RFID) y tecnologías de sensores. La conectividad digital de estos dispositivos permite enviar y recibir información para realizar tareas que hasta no hace mucho podrían parecer imposibles, otorgando a los usuarios la facilidad de manejar todos sus dispositivos conectados con tan solo un clic. Las cámaras IP son un claro ejemplo de la tecnología IOT, disponen de su propia dirección IP que está directamente conectada a la red y se pueden instalar en cualquier ubicación en la que exista una conexión de red, su principal función es vigilar y monitorear infraestructuras ya sean ciudades, empresas o viviendas.

Un aspecto clave en la tecnología es su rápido cambio y su impacto en el mundo, por lo que la adaptación también debe ser rápida, en este punto es donde se cuestiona si la sociedad está lista para este cambio, o aún más importante ¿si está protegida durante estos cambios? Al mismo tiempo que avanza la tecnología también debe avanzar la seguridad para proteger sobre los posibles ataques. Como estudiante en seguridad de la información se es consciente de las amenazas que enfrentan los datos y las consecuencias a las que se exponen los usuarios cuando no cuentan con las medidas de seguridad y protección adecuadas. En este sentido se debe tener una visión general de los riesgos de seguridad en la tecnología IOT que pueden afectar la privacidad de la información.

En esta investigación se analizaron los riesgos de las cámaras IP en el sector hogar con el fin de generar una guía de buenas prácticas para los usuarios que quieran tener un dispositivo de estos en su casa o apartamento, el riesgo varía según la criticidad del equipo, sus funciones o la dependencia que se tenga del mismo. Según las amenazas que enfrentan los dispositivos puede afectar la accesibilidad del equipo, la integridad de la información contenida en el mismo y la identidad del usuario propietario del equipo, ya que esto puede conducir al robo de información privada. Otro factor a considerar y directamente relacionado con la seguridad es la confidencialidad de los datos que se debe garantizar tanto a la información almacenada en el dispositivo como a la transmitida en las comunicaciones que éste realice.

[1] Centro de Identificación Automática del Instituto de Tecnología de Massachusetts

2. GENERALIDADES

2.1 LÍNEA DE INVESTIGACIÓN

El programa se trabaja sobre Software Inteligente y Convergencia Tecnológica

2.2 PLANTEAMIENTO DEL PROBLEMA

Una estadística realizada por STATISTA[2] muestra un exponencial incremento en el número de dispositivos conectados a internet, con una proyección indicada en la figura 1.

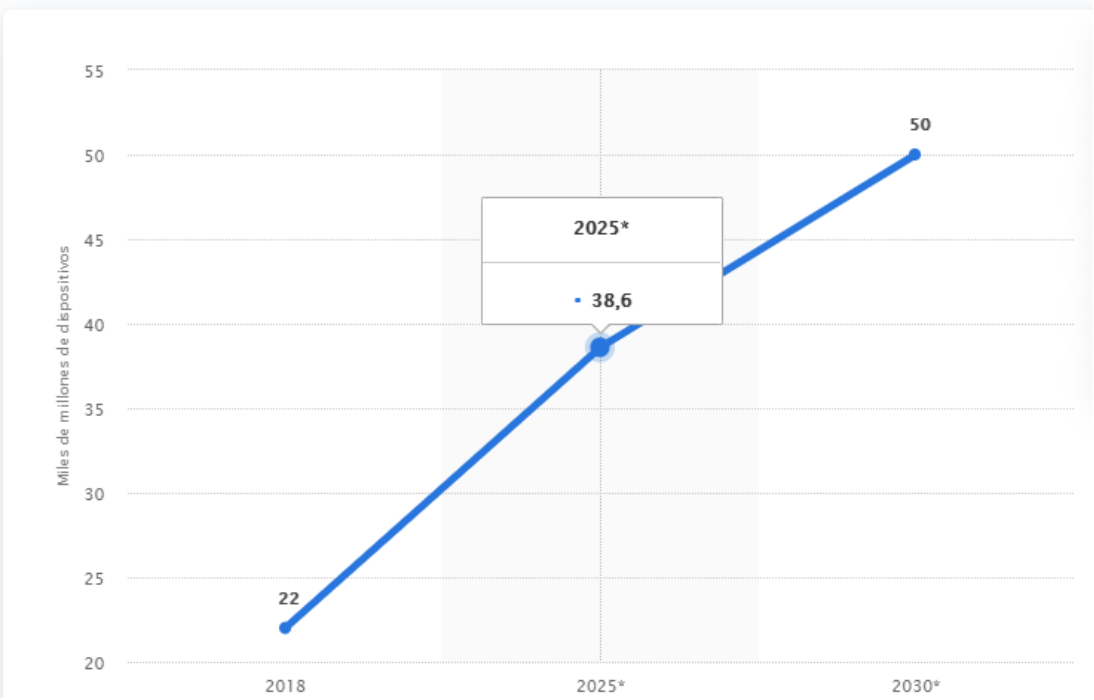


Figura 1. Esta estadística muestra la evolución a nivel mundial de los dispositivos conectados a Internet en 2018, así como una serie de previsiones para 2025 y 2030. De cumplirse las previsiones, el número de dispositivos conectados podría superar la barrera de los 50.000 millones en el año 2030. Recuperado de https://es.statista.com/estadisticas/517654/prevision-de-la-evolucion-de-los-dispositivos-conectados-para-el-internet-de-las-cosas-en-el-mundo/#statisticContainer

Se supone un aumento en la exposición de datos en la red, por lo tanto, la seguridad de la información es un aspecto que se debe considerar todos los días. La interconexión de estos dispositivos es a su vez su talón de Aquiles, puesto que los Ciberdelicuentes podrían utilizarlos a su propio beneficio. Aunque en general los dispositivos de IOT no parecen críticos, lo pueden llegar a hacer si no son utilizados de forma adecuada. En términos de seguridad, un problema es garantizar que los

[2] Plataforma Global de datos empresariales, España.

comandos emitidos hacia los dispositivos provengan de usuarios autorizados, otra de las preocupaciones es la privacidad de las personas. Por ejemplo, si alguien tiene una cámara de video en línea para vigilar que pasa en casa en su ausencia, y la conexión no está protegida, cualquiera podría saber lo que sucede allí. Las cámaras conectadas a Internet de las Cosas son un arma de doble filo, es decir, su función de vigilar y grabar lo que ocurre en una vivienda particular, una oficina o lugar público, es de gran valor a la hora de dar sensación de seguridad, pero al estar conectadas a Internet, son herramientas realmente peligrosas si no cuentan con una capa de Ciberseguridad bien armada, actualizada y monitorizada. Los sistemas basados en IP tienen diversas topologías y tecnologías que los hacen más complejos y que dan como resultado una superficie de ataque mucho mayor, por ejemplo, VPN, puertas de enlace, múltiples servidores, WIFI, sistemas de control de acceso, etcétera. Además, estos sistemas al estar expuestos a Internet permiten a los delincuentes atacarlos continuamente mientras se descubren nuevas vulnerabilidades todos los días. Otro aspecto que puede ser preocupante es sobre los usuarios que no comprenden que cierta información no debe ser divulgada, que no deben instalar algunos programas y que existen recomendaciones básicas o más avanzadas para evitar la intromisión a su información. Por otro lado los desarrolladores pueden introducir errores inadvertidamente en el código de la aplicación o en su protocolo y aun no se cuenta con la tecnología adecuada para evaluar automáticamente esos procesos, a pesar de la existencia de las listas de verificación, algunas herramientas de evaluación y extensas pruebas de software, la operación es muy limitada.

Respecto a las cámaras de red o de Internet que proporcionan transmisiones de audio y video en vivo donde se puede acceder de forma remota mediante un navegador de Internet se conoce que son vulnerables al espionaje digital, lo que hace que las funciones de seguridad sean clave cuando se compran y se usan estos dispositivos; es en este punto donde se cuestiona la seguridad de la información en un entorno de IOT, ya sea por error humano o por error de los dispositivos interconectados.

2.2.1 ANTECEDENTES DEL PROBLEMA

En octubre de 2016 se presentó el caso de DYNDNS, uno de los servidores DNS más utilizados en internet, que sufrió un ataque dirigido el cual involucro a más de 10 millones de direcciones IP relacionados con la Botnet Mirai[3], tuvo como propósito la infección masiva de dispositivos para reclutarlos y organizarlos en una Botnet, que no es más que un ejército de dispositivos que se controlan remotamente, ejecutando ordenes que son enviadas a través de un servidor que comanda las operaciones, otro propósito es ampliar su ejército para a partir de allí lanzar ataques de denegación de servicio distribuida comprometiendo la mayor cantidad de servicios, aplicaciones y dispositivos; Mirai trabaja con una serie de listas que

[3] Tipo de red que tiene como fin el beneficio económico de Ciberdelicuentes.

contienen usuarios y contraseñas por defecto, algunas de las cuales se pueden observar en la figura 2, estas han sido identificadas en muchos de los dispositivos que están conectados a Internet, así que se genera un script que es lanzado a través de diversos medios como archivos maliciosos, vulnerabilidades en sistemas operativos, infección de páginas web y vulnerabilidades en los navegadores, que están a la espera para que al momento que se ejecute el script se logre encontrar las credenciales de acceso por defecto a cualquier dispositivo y así se pueda abrir una puerta trasera, para que este sea controlado remotamente y reclutado por el ejército de Botnet, de igual manera desde los dispositivos comprometidos se hace un escaneo de otros dispositivos escaneando las direcciones IP que están asociadas al puerto 48101TCP, indicando que son accesibles a través del protocolo Telnet el cual no ofrece seguridad, una vez la Botnet tenga fuerza, lanzara ataques con instrucciones dadas desde el punto central a través de inundación de mensajes HTTP, GRE IP, SYN, ACK (Di Monte, E., & Solís, D., 2017)

root	xc3511	admin	1111	root	zlxx.
root	vizxv	root	666666	root	7ujMko0vizxv
root	admin	root	password	root	7ujMko0admin
admin	admin	root	1234	root	system
root	888888	root	klv123	root	ikwb
root	xmhdipc	Administrator	admin	root	dreambox
root	default	service	service	root	user
root	juantech	supervisor	supervisor	root	realtek
root	123456	guest	guest	root	00000000
root	54321	guest	12345	admin	1111111
support	support	guest	12345	admin	1234
root	(none)	admin1	password	admin	12345
admin	password	administrator	1234	admin	54321
root	root	666666	666666	admin	123456
root	12345	888888	888888	admin	7ujMko0admin
user	user	ubnt	ubnt	admin	1234
admin	(none)	root	klv1234	admin	pass
root	pass	root	Zte521	admin	meinsm
admin	admin1234	root	hi3518	tech	tech
root	1111	root	jvbzd	mother	fucker
admin	smcadmin	root	anko		

Figura 2. Combinaciones de usuarios y contraseñas comunes. Recuperado de: https://www.cert.gov.py/index.php/noticias/botnet-mirai-y-otras-amenazas-dispositivos-conectados-internet-iot

DYN confirmo el ataque a las 11:10 am y tardo dos horas en ser resuelto, sin embargo, la normalización de los sitios web se demoró unas horas más.

Otro caso relacionado con cámaras de seguridad se presentó el 17 de octubre del 2018 a las cámaras de seguridad de la vivienda en Madrid del líder de Unidos Podemos[4], Pablo Iglesias, con el cual se emitieron imágenes en directo por internet a través de una web abierta. Podemos conoció a través de un mensaje anónimo

[4] Partido Político Español

que esa cámara que apuntaba a la entrada de la vivienda había sido intervenida, las autoridades policiales solucionaron el problema, aunque no se tiene constancia de que se abriera ninguna investigación. Los miembros del partido denunciaron en los medios que esto era un ataque de opositores. Este es un caso de cómo una cámara de seguridad instalada en una vivienda sirve como arma política para general shows mediáticos.

El 09 de marzo del presente año se registró un nuevo ataque donde un grupo de hackers dice haber obtenido una valiosa cantidad de datos de cámaras de seguridad recopilados por la Statu de Silicón Valley Verkada Inc[5]., logrando acceder a las transmisiones en vivo de 150.000 cámaras de vigilancia dentro de hospitales, compañías, departamentos de Policía, prisiones y escuelas. Entre las compañías cuyas imágenes fueron expuestas están incluidos el fabricante de automóviles Tesla Inc. y el proveedor de software Cloudflare Inc. Además, los hackers pudieron ver videos desde el interior de clínicas de salud para mujeres, hospitales psiquiátricos y las oficinas de Verkada. La filtración de datos fue llevada a cabo por un colectivo internacional de hackers y tenía la intención de mostrar la omnipresencia de la video vigilancia y la facilidad con la que se puede ingresar a estos sistemas, dijo Tillie Kottmann, una de las hackers que se atribuyó el mérito de haber vulnerado el sistema de Verkada, con sede en San Mateo, California. (Bloomberg, 2021).
"Hemos desactivado todas las cuentas de administrador interno para evitar cualquier acceso no autorizado", dijo un representante de Verkada en un comunicado. "Nuestro equipo de seguridad interno y la firma de seguridad externa están investigando la escala y el alcance de este problema potencial". Una persona con conocimiento del asunto dijo que el director de seguridad de la información de Verkada, un equipo interno y una firma de seguridad externa están investigando el incidente. La compañía está trabajando para notificar a los clientes y establecer una línea de soporte para responder preguntas. (TURTON, 2021). En este caso los atacantes se delataron lo preocupante del tema es cuantos ataques pueden estar sucediendo en este momento sin ser detectados.

2.2.2 PREGUNTA DE INVESTIGACIÓN

¿Cómo se pueden mejorar los controles de seguridad en el manejo de la información de los sistemas de cámaras de vigilancia que se implementan en los hogares?

2.2.3 VARIABLES DEL PROBLEMA

La tabla 1 muestra las variables identificadas para el proyecto, se clasificaron como dependientes e independientes,

[5] Multinacional dedicada a soluciones de seguridad por video

TIPO DE VARIABLE	VARIABLE	DESCRIPCION	IMPACTO
Dependiente	Perdida de información	Posibilidad de perder la información personal registrada para el uso de la cámara	Fraude y suplantación de identidad por no contar con los controles adecuados que lo impidan
	Riesgos de ataques cibernéticos	Probabilidad de que se materialice una vulnerabilidad y la amenaza comprometa la seguridad de la información	Todos los eventos que se puedan desencadenar y comprometan la información
	Falta de actualización del firmware	Proceso que debe cumplir el fabricante del dispositivo para corregir y evitar que se exploten las vulnerabilidades encontradas	Aprovechamiento de una vulnerabilidad para realizar ataques periódicos a los dispositivos
	Eventos de intrusión para realizar espionaje	Posibilidad de presentar eventos no deseados que comprometan la confidencialidad e integridad de los datos, así como la privacidad	Situaciones que puedan alterar el normal funcionamiento del dispositivo
Independiente	Costos y beneficios de la inversión destinada a la seguridad perimetral	Relación directa de lo que se recibe cuando se realiza una inversión, que permita evitar ataques de Ciberseguridad	Distribución adecuada de los recursos económicos disponibles al momento de realizar la implementación del sistema de seguridad
	Vectores de ataque	Componentes que hacen parte de un ataque cibernético y permiten identificar las técnicas utilizadas para realizar el ataque	Presentar demasiadas vulnerabilidades provocan un mayor número de vectores de ataque
	Políticas del tratamiento de los datos, establecidas por el fabricante	Son de suma importancia para establecer los lineamientos y la forma en que se gestionan los datos recolectados	Normas que establecen los procesos y los responsables que intervienen en cada uno de ellos permitiendo dejar total claridad

Tabla 1. Variables del problema, Tabla propia.

2.3 JUSTIFICACIÓN

El uso de la tecnología para apoyar y optimizar la seguridad en los hogares y edificios es una tendencia que continúa en alza en el país ya que, según la Policía Nacional, en el año 2020 se reportaron 19.501 víctimas de robo a viviendas, una de las cifras más altas registradas en los últimos cinco años. De acuerdo con el último

estudio realizado por INVAMER[6] en agosto del 2020, el 88 % de los colombianos consultados consideró que la seguridad en el país había empeorado, un 8 % más en comparación al mes de junio del mismo año. En este panorama, los hogares colombianos han optado por adquirir sistemas de seguridad y herramientas tecnológicas que apoyen la vigilancia de sus viviendas, conjuntos residenciales y otros espacios que requieren de un adecuado control de acceso (Tecno Seguro , 2021). Las cámaras de seguridad también pueden ayudar a ver quién está en la puerta antes de abrirla, esta es una preocupación constante por las modalidades de robos que se conocen hoy en día. Si llegara a ocurrir un robo podrá proveer una valiosa evidencia para identificar al ladrón e incluso recuperar sus pertenencias. Otra preocupación de las personas es el cuidado de sus hijos, adultos mayores y mascotas; se observan a diario noticias de maltrato o abusos por parte de cuidadores o empleados domésticos, las cámaras de vigilancia pueden ayudar a los usuarios a monitorear estas situaciones.

La inseguridad en el país es la razón principal para que una persona decida instalar una cámara de vigilancia en su vivienda, aquí radica la importancia del buen uso de estos dispositivos. La investigación acerca de los riesgos en las cámaras de seguridad IP, permitirá determinar las principales causas por las cuales se pueden ver expuestos los usuarios con este tipo de dispositivos, esto debido a que la gran mayoría quedan instaladas con la configuración por defecto que traen de fábrica. Por esta razón, es necesario comprender que, al no contar con unos protocolos de configuración adecuados, se dejaran expuestos los dispositivos a un ataque informático, el cual permitirá la recopilación de información personal de los usuarios y que esta a su vez sea usada de manera inadecuada, así como también los dispositivos pueden verse inmersos en una Botnet. Cuando una persona decide comprar una cámara de seguridad IP por su propia cuenta sin tener los conocimientos de seguridad apropiados es posible que cometa errores que más adelante le pueden traer inconvenientes.
Para probar esto se utilizó Shodan que es un motor de búsqueda cuyo objetivo es ubicar todo tipo de dispositivos conectados a internet a través de una variedad de filtros. Se realizó la búsqueda por *ipcamera country:"CO",* como se muestra en la figura 3, indicando el tipo de cámara que se busca y el país que es Colombia, se encontraron 34 dispositivos, y el top de las ciudades se encuentra en la tabla 2.

TOP CIUDADES	
Bogotá	9
Medellín	8
Cartagena	3
Cali	3
Bello	2

Tabla 2. Top ciudades .Tabla propia.

[6] Portal de Investigación y asesoría del mercadeo

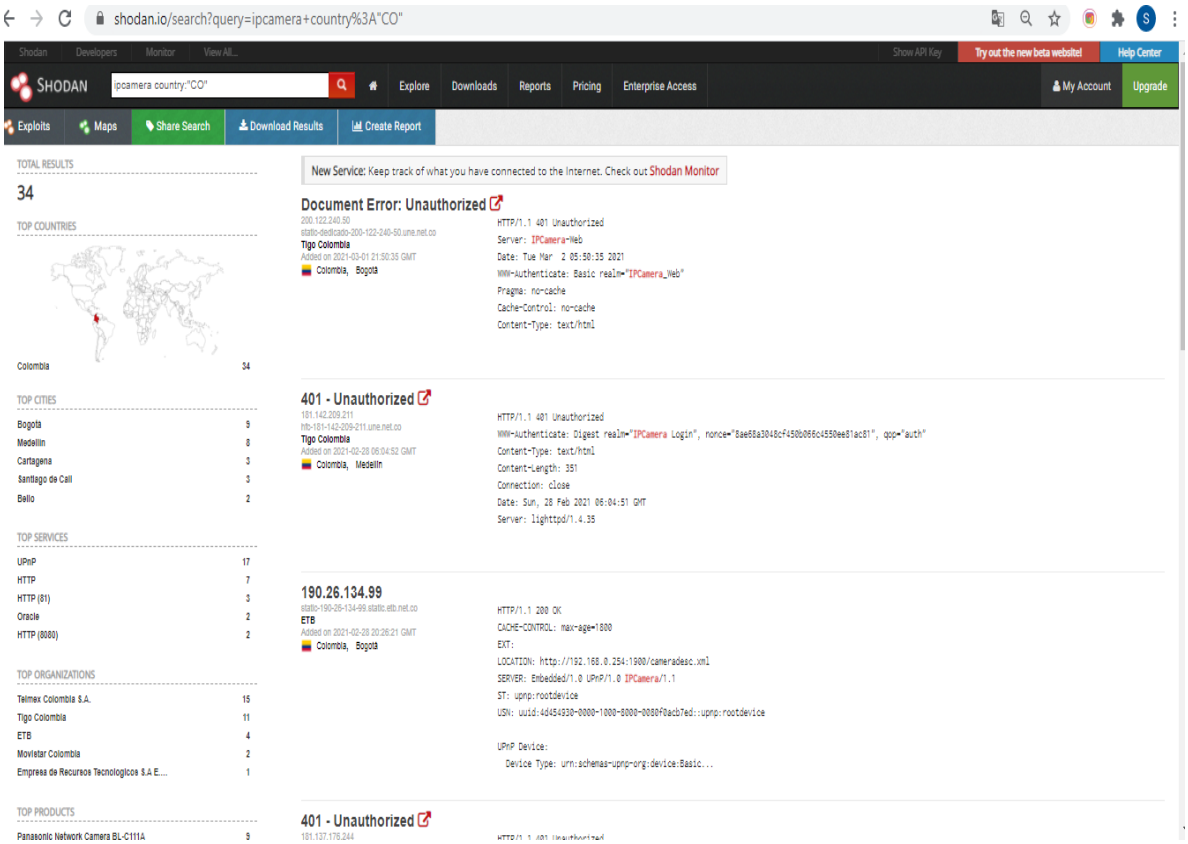


Figura 3. Búsqueda de Cámaras IP en Colombia. Recuperado de: https://www.shodan.io/

En la revisión de estas cámaras, se ubicó una en Medellín a la cual se logró acceder mediante las credenciales por defecto Admin, admin. En las figuras 4 y 5 se puede ver la configuración total de la cámara. Al ingresar a la cámara no solo se puede observar si no también realizar modificaciones en sus ajustes.

Como Shodan existen más tipos de búsquedas desde google hacking a herramientas más sofisticadas con las cuales cualquier usuario puede tener acceso a una cámara de seguridad IOT. De esta manera, la importancia del proyecto está dirigida a la identificación de riesgos para realizar las mínimas recomendaciones necesarias y que a su vez los usuarios puedan hacer uso de forma adecuada de las cámaras IP y sus servicios de manera segura.

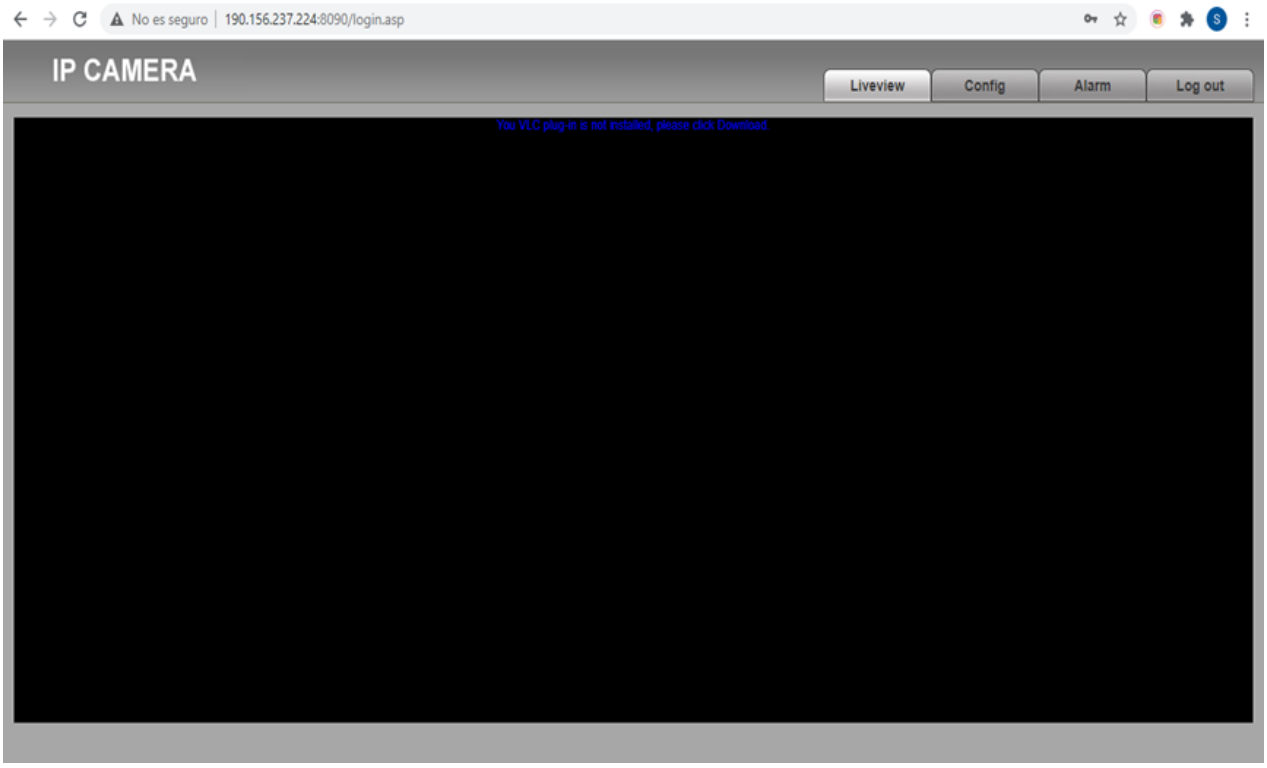


Figura 4. Cámara IP. Recuperado de: https://www.shodan.io/.

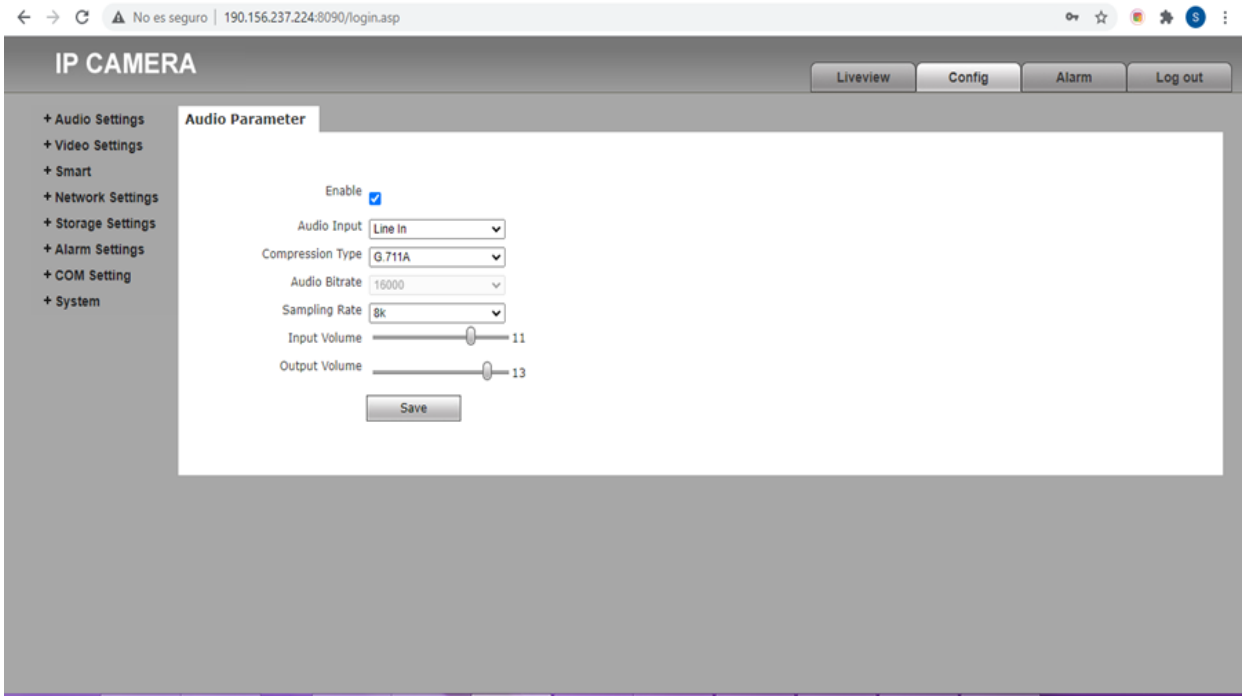


Figura 5. Configuración de la Cámara IP. Recuperado de: https://www.shodan.io/

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar una guía sobre los riesgos a los cuales se exponen las cámaras de seguridad IP en el sector hogar y dar las mínimas recomendaciones para prevenir dichos riesgos.

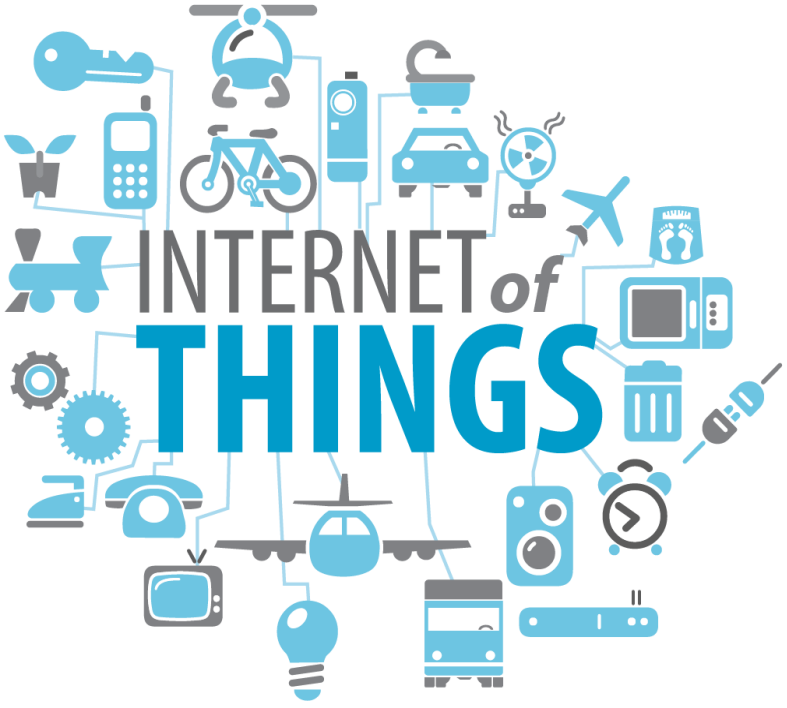
3.2 OBJETIVOS ESPECÍFICOS

- Comparar las características de los diferentes tipos de cámaras IP
- Identificar vectores de ataques que pueden comprometer las cámaras conectadas a una red.
- Evaluar los riesgos asociados al uso de cámaras IP
- Formular las recomendaciones mínimas de seguridad para garantizar el buen uso de cámaras un entorno IOT.

4 MARCOS DE REFERENCIA

4.1 MARCO CONCEPTUAL

Internet de las cosas (IOT), Son dispositivos que están conectados y controlados a través de Internet. El uso de dispositivos IOT ha aumentado exponencialmente con el tiempo y a sabiendas o sin saberlo nuestros datos son capturados a diario (Yogeesh Seralathan, 2018). En la figura 6 se muestra como el Internet de las cosas ha evolucionado debido a la unión de múltiples tecnologías, realizando análisis en tiempo real, aprendizaje autónomo, sensores y sistemas integrados, sistemas de control, automatización de viviendas y edificios, entre otros aspectos que aportan para su crecimiento y fortalecimiento.



. Figura 6. Unión de múltiples tecnologías con Internet de las cosas. Recuperado de: https://terminosaudiovisuales.es/iot/

En términos generales un dispositivo IOT se caracteriza por tener una IP propia, que le permite tener la capacidad de conectarse a una red, ya sea de forma alámbrica o inalámbrica y este a su vez debe ser compatible con otras plataformas. Esto permite integrar sensores, actuadores, receptores, controladores, etiquetas RFID, software, hardware, algoritmos para programar los dispositivos IOT, que permita otorgar la capacidad de comunicarse mediante internet, proporcionando información de todo lo esté a su alrededor, capaces de analizar, diagnosticar y ejecutar funciones tecnológicas avanzadas desde cualquier lugar y en cualquier momento.

En el sector hogar esta tecnología permite por ejemplo el ahorro de energía y uso razonable del agua, utilizando dispositivos de control remoto programados para que actúen en determinadas horas, así como también permite tener un sistema de seguridad que detecte el ingreso de intrusos y notifique inmediatamente según este configurado el sistema. En la siguiente figura se muestra el hogar inteligente como la aplicación del Internet de las Cosas más popular en ese momento, según un estudio del 2016 de IOT Analytics.

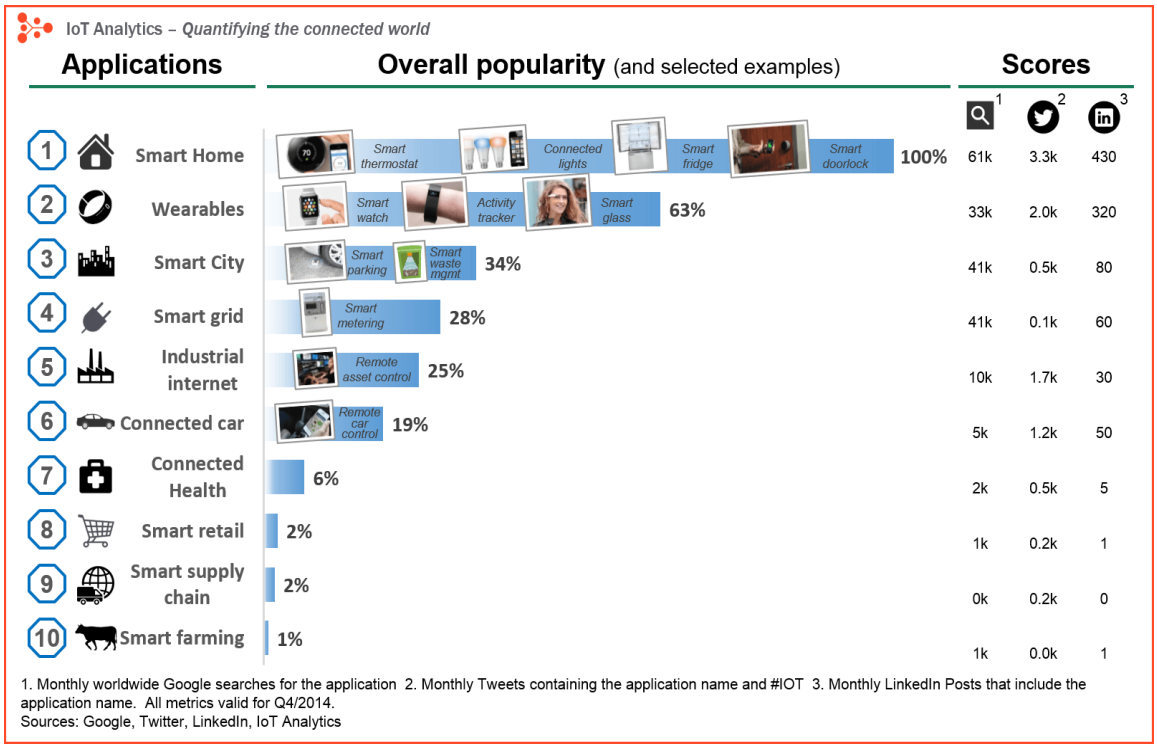


Figura 6. Estudio del 2016 de IOT Analytics Se midieron 3 aspectos: lo que la gente busca en Google, lo que la gente habla en Twitter y lo que la gente escribe en LinkedIn. La puntuación más alta recibió una calificación del 100%, las otras aplicaciones de Internet de las cosas se clasificaron con un porcentaje que representa la relación con la puntuación más alta (clasificación relativa). Recuperado de: https://iot-analytics.com/10-internet-of-things-applications/

Un dispositivo IOT común en las viviendas son las cámaras de red, también conocidas como cámara de internet o cámara IP, es un dispositivo que capta y transmite una señal de audio/video digital a través de una red IP estándar a otros dispositivos de red, tales como un computador, Smartphone y tablets. Mediante el uso de una dirección IP dedicada, un servidor web y protocolos de streaming de video, los usuarios pueden visualizar, almacenar y gestionar video de forma local o remota, en tiempo real. Una cámara IP pude además ser de diferente tipo de acuerdo con su uso:

- Las cámaras de red fijas como su nombre lo indica son las que permanecen fijas hacia un objetivo, ideales para exteriores en puntos considerados como importantes o críticos de un lugar determinado.

- Las cámaras de red domo fijas, las mismas que son cámaras fijas, pero dentro de una carcasa, a prueba de vandalismo que se instalan de forma predeterminada en techos, su característica principal es su discreción y resistente a las manipulaciones que puedan ser objeto. Su limitado espacio no permite en ciertos casos cubrir varios objetivos, por lo que resulta útil para objetivos fijos.

- Las cámaras de red PTZ, Pan Tilt Zoom, que permiten moverse de forma horizontal y verticalmente, además de poseer un zoom ajustable dentro de una determinada área, su utilización es ideal para espacios amplios para cubrir varios objetivos. (Mata, 2010)

Este tipo de cámaras pueden venir acompañadas de sistemas de vigilancia, estos se han vuelto asequibles debido a la tendencia IOT, como resultado el mercado de dispositivos de seguridad en hogares conectados ha incrementado, convirtiendo los sistemas en blanco de numerosos ciberataques; Para comprender mejor estos sistemas se identificaron 4 conceptos:

1. Propósito: El propósito de un sistema de video vigilancia depende de las necesidades del usuario.

2. Implementación: Hay varias formas en que el hardware / software del sistema se puede configurar para recopilar e interpretar las imágenes de video.

3. Topología: Puede describirse por su distribución, contención e infraestructura. La distribución se refiere a si las cámaras están ubicadas en algún lugar en el mundo o ubicados físicamente en un área. La contención se refiere a si el sistema es de circuito cerrado (no está conectado a Internet) o de circuito abierto, y se basa en el control de acceso para denegar a los usuarios sin las credenciales adecuadas. Finalmente, la infraestructura se refiere a cómo los elementos del sistema están conectados entre sí: inalámbrico (por ejemplo, Wi-Fi), cableado (por ejemplo, Ethernet a través de cables CAT6) o ambos.

4. Protección: La protección del sistema de vigilancia se refiere a cómo el usuario asegura el acceso físico y virtual a los activos y servicios del sistema. Sin protección física, un atacante puede manipular o dañar las cámaras o instalar su propio equipo en la red. La protección virtual se puede emplear en los hosts de la red o en la propia red

Los sistemas de vigilancia pueden tener infracciones de seguridad en la disponibilidad, integridad y confidencialidad de la información. Existe un mayor

riesgo de que una cámara se vea comprometida por sus capacidades (observar el metraje de video) o para actuar como un trampolín en un ataque mayor.

4.2 MARCO TEÓRICO

El proceso de trasformación digital es imparable. Las tecnologías emergentes como el internet de las cosas marcan la pauta en cuando a innovación digital. A continuación, se mostrarán algunos ejemplos de cómo Colombia se ha ido adaptando y evolucionando en esta tecnología:

El 30 de octubre de 2019 se anunció el primer laboratorio de Internet de las cosas en Colombia, el objetivo del laboratorio es brindar a los diferentes actores del ecosistema emprendedor colombiano un ambiente propicio para desarrollar aplicaciones y herramientas con base en tecnología internet de las cosas y que las puedan probar sobre una red exclusiva. Según explicó Johana Harker, impulsora de la iniciativa, "lo que hicimos fue coger el espacio que ya teníamos e instalar aquí las redes en las que los objetos se comunican y con esto lo que pasa es que los objetos no van a tener que pelear por espacio" (Hernandez, 2020). Adicionalmente, se crearán espacios de capacitación para los emprendedores donde podrán avanzar en temas de desarrollo de soluciones IOT, contarán con material de formación para las interacciones con los dispositivos dispuestos allí y el apoyo de personal capacitado. Este espacio es una caja de herramientas para que los emprendedores se apropien de la tecnología IOT y pueda innovar y experimentar con ella

En Colombia también se encuentra una gran variedad de empresas que trabajan con soluciones IOT. Una de ellas es E-Security la cual lleva en el mercado más de 20 años siendo pionero en el país, mediante un artículo el Gerente de E-Security explica las ventajas de IOT que no solo tienen que ver con comodidad, pues en el hogar también permite racionalizar el uso de servicios como el agua y la energía. Pero incluso en estas casas llamadas inteligentes la seguridad sigue siendo importante, Por eso, al plantearse tener un hogar inteligente, es fundamental que las personas se asesoren previamente con empresas de reconocido prestigio en el mercado, este tipo de asesoría es fundamental porque permite minimizar y dar un tratamiento adecuado a los diferentes riesgos asociados al IOT. “Hogar inteligente no es sinónimo de hogar seguro, ya que se pueden presentar al menos dos situaciones altamente críticas: por una parte, un ciberataque y, por la otra, la saturación con diversos equipos interconectados puede hacer colapsar la infraestructura domótica de su hogar”, explica Hugo Bejarano, gerente de E-Security Ltda. (Patrocinado, 2019)
A raíz de estas vulnerabilidades nace E-Security protección y tecnología, que es una compañía dedicada a la prestación de servicios de vigilancia y seguridad privada, debidamente autorizada por la SUPERVIGILANCIA, en las modalidades de: Vigilancia fija – móvil, escolta personal, escolta vehicular, escolta de carga, protección electrónica, asesoría, consultoría e investigación.

Los dispositivos IOT pueden ser una presa fácil para los Ciberdelicuentes que buscan este tipo de dispositivos como punto de entrada a la red. El ciberataque y compromiso de estos dispositivos puede dar lugar a consecuencias graves para la seguridad como:

- Infectarlos para formar parte de una red zombi que los utilicen para realizar ciberataques, por ejemplo, de denegación de servicio distribuida o DDoS[5];

- Utilizarlos como puente o punto de entrada para atacar otros equipos de la misma red, para robar información o para realizar otras acciones delictivas;

- Reconfigurarlos para inhabilitarlos o cambiar sus condiciones de utilización.

4.3 MARCO JURÍDICO

Para el desarrollo de esta investigación se tendrá en cuenta únicamente el nivel jurídico colombiano y sus diferentes organismos de regulación y control que han establecido leyes que amparan la privacidad de todo colombiano, como la Superintendencia de Industria y Comercio, la Ley Estatutaria 1581 de 2012 que aplica al tratamiento de datos personales ; La ley 1273 de 2009 que estipula diez (10) delitos informáticos y las sanciones aplicables a los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Ley 1581 de 2012 por la cual se “aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales”. Así pues, se analiza con mayor énfasis el principio de seguridad en el cual se plantea que el encargado del manejo de la información debe brindar las garantías de seguridad de la información, así como en el principio de confidencialidad, se plantea la obligatoriedad a garantizar la reserva de la información.

Igualmente se analiza la Ley 1273 de 2009, la “cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.” De ella se resalta el Artículo 269F: Violación de datos personales, que tipifica la pena a la que se enfrenta el tercero por la violación de los datos.

Se tiene en cuenta el reglamento (UE) 2018/1725, el cual establece las normas aplicables al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión Europea. Sus disposiciones se ajustan al Reglamento General de Protección de Datos y a la Directiva sobre protección de datos en el ámbito penal.

4.4 ESTADO DEL ARTE

IOT es un nuevo paradigma que combina aspectos y tecnologías provenientes de diferentes enfoques. Al colocar inteligencia en los objetos cotidianos, se convierten en objetos inteligentes capaces no solo de recopilar información del entorno e interactuar/controlar el mundo físico, sino también de estar interconectados entre sí a través de Internet para intercambiar datos e información. La evolución integrada desde el pre internet, después se crea el internet de contenidos como plataformas, siguiendo se ve el internet de los servicios con la integración aplicaciones, más adelante encontramos el internet de las personas con la integración de las redes sociales, dispositivos y objetos conectados, y por último se evidencia el internet de las cosas que integra las maquinas interactuando, identificando, monitoreando todo lo que podemos tener conectado en línea transmitiéndolo para poder controlar desde la comodidad de cualquier lugar. (MOLINA, 2019).

En la figura 8 se muestra una línea de tiempo con la evolución desde el pre internet hasta internet de las cosas.

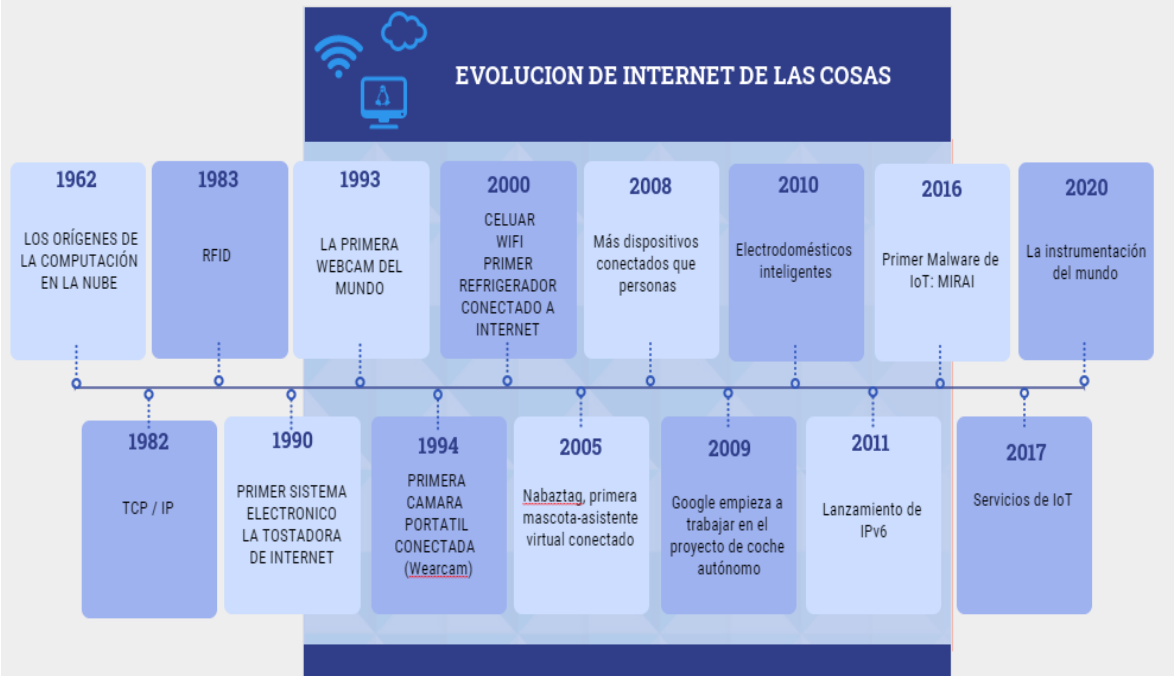


Figura 7. Evolución de IOT. Figura propia.

1962: El psicólogo estadounidense y científico informático Dr. Joseph Carl Robnett Licklider escribió una serie de memorandos que exploran su idea de una "red informática intergaláctica". Imaginó un sistema de computadoras conectadas entre sí, y un espacio donde todos los datos están disponibles para todos desde cualquier lugar. Esta idea preparó el camino para la creación de interfaces bancarias en línea, bibliotecas digitales y computación en la nube. (MOLINA, 2019).

1982: El Departamento de Defensa de EE. UU. Declaró TCP / IP como el estándar para todas las redes informáticas militares. TCP / IP es un conjunto de protocolos de comunicación utilizados en redes de computadoras, que proporcionan conectividad de extremo a extremo para computadoras. (MOLINA, 2019)

1983 Tecnología de identificación de frecuencia, el inventor Charles Walton patentó por primera vez el dispositivo de identificación por radiofrecuencia (RFID). El dispositivo, que consiste en un pequeño chip y una antena, se utiliza para transferir datos de forma inalámbrica entre los objetos conectados, la tecnología se desarrolló por primera vez para espionaje en 1945. (MOLINA, 2019)

1990: El primer sistema electrónico para rastrear el movimiento del personal Olivetti inventó un sistema de identificación electrónica para rastrear el movimiento del personal. La insignia transmite señales de infrarrojos, que son captadas por sensores en todo el edificio. Por otro lado, el 08 de octubre los informáticos John Romkey y Simon Hackett conectaron una tostadora a Internet, convirtiéndolo en el primer dispositivo controlado a través de Internet. Usando una conexión TCP / IP, la tostadora podría encenderse y apagarse. Un ser humano todavía tenía que insertar el pan. Un año después, se agregó un brazo robótico para recoger e insertar la rebanada de pan, el brazo también podría controlarse desde Internet. (MOLINA, 2019)

1993: La primera cámara web, transmitiendo el nivel de café de una olla en la Sala de Troya del Laboratorio de Computación de la Universidad de Cambridge, se conectó en línea. La cámara se instaló en 1991 para mostrarles a las personas en una red local que trabajaban en el edificio si había café en la olla individual del laboratorio o no. La transmisión se movió a la World Wide Web una vez que los navegadores lo lograron. (MOLINA, 2019)

1994: Steve Mann, (Universidad de Stanford), conocido como “El padre de la computación vestible” (*The Father of Wearable Computing*), conectó la primera cámara portátil a la web. (Santos, 2020)

2000: A comienzos del siglo XXI, gracias a la popularización de la conectividad inalámbrica (celular o WiFi), se produjo la primera explosión en el crecimiento de los objetos conectados. Este crecimiento se ha consolidado especialmente en los últimos años, según han ido surgiendo nuevos conceptos como el WSN (*Wireless Sensor Networks*) o las nuevas tecnologías de acceso radio como LPWA (NB-IoT, LTE-M), para finalmente dar paso al IoT que todos conocemos. También LG lanza el primer refigerador conectado a Internet. No tuvo gran acogida ya que su precio era muy elevado. (Santos, 2020)

2005: La empresa francesa Violet lanzó al mercado Nabaztag. Se trataba de un dispositivo con forma de conejo que se conecta a Internet por ondas WIFI, se

comunica con el usuario mediante mensajes de voz, y cambios de color o movimiento. Como buena mascota virtual, Nabaztag reproduce, habla, escucha y responde a la voz de los usuarios. También mostraba las noticias de actualidad de diarios digitales, la música de su emisora favorita o la información del tiempo. (Santos, 2020)

2008: Fue un hito importante en la historia del IOT, ya que fue el primer año en el que los dispositivos conectados a Internet superaron al número de personas conectadas. (Santos, 2020)

2009: Aunque ya era usado el termino en círculos especializados desde 1999, no fue hasta este año cuando el profesor del MIT Kevin Ashton lo introdujo para el gran público en su artículo "That Internet of Things Thing", del que vale la pena traducir una pequeña frase.

"*El Internet de las Cosas tiene el potencial de cambiar el mundo, tal como lo hizo el Internet. Tal vez incluso más".*

Google arranca su proyecto de coches autónomos, Google self-driving car project, que posteriormente pasaría a ser conocido como Waymo**.** La tecnología desarrollada por Waymo permite a un automóvil conducirse de forma autónoma por ciudad y por carretera, detectando otros vehículos, señales de tráfico, peatones, etcétera. (Santos, 2020)

2010: La compañía NEST empieza a fabricar electrodomésticos inteligentes. El primero fue un termostato que optimizaba el horario de la calefacción a partir de los patrones de uso de los usuarios. (Santos, 2020)

2011: Los primeros pasos en IOT se dieron con la versión IPV4. Esto suponía una importante limitación, ya que el número de direcciones que se podían generar era muy reducido, a partir de este año se diseña el protocolo de direccionamiento de INTERNET IPV6 posibilitando la identificación de una infinidad de direcciones. Poco después Samsung, Google, Nokia y otros fabricantes anuncian sus proyectos NFC. (Santos, 2020)

2016: Surgió Mirai, un Botnet cuyo objetivo son dispositivos IOT, principalmente Routers, grabadoras digitales de vídeo y cámaras IP de vigilancia. Este malware recopila las contraseñas por defecto que establecen los fabricantes de los dispositivos y que los usuarios muchas veces se olvidan de cambiar, luego utiliza los dispositivos para realizar ataques de denegación de servicio a terceros, normalmente, páginas web muy populares. (Santos, 2020)

2017: Los grandes fabricantes de servicios en la nube ofrecen soluciones IOT: Azure IoT Edge*,* AWS IoT *y* Google Cloud IoT core*.* (Santos, 2020).

2020: Según Gartner, una gran variedad de unos 21.000 millones de "cosas" conectadas están en este momento recogiendo datos y realizando todo tipo de tareas. La mayoría son dispositivos de consumo, desde altavoces inteligentes hasta relojes y cerraduras de puertas. El resto sirve a los negocios: dispositivos médicos, sensores de motor, robots industriales, etcétera. Casi todas las empresas dependen ahora de los dispositivos de IOT de una forma u otra**.** Por el momento, no existe un ejemplo más dramático del valor del IOT que el dispositivo médico Kinsa[7], del se agregan datos sobre posibles brotes de COVID-19. (NOTICIAS, 2020)

El artículo publicado por OVACEN[8] "Cámaras de seguridad: Tipos, consejos y cuál comprar para casa", muestra qué cámaras de seguridad para hogares se pueden encontrar en el mercado, sus diferentes tipos, y como elegirlas. El artículo primero muestra cuales son las medidas de protección y seguridad más utilizadas mediante la siguiente figura:

Figura 8. ¿Cuáles son las medidas de protección más utilizadas? Recuperado de https://ovance.com/camaras-de-seguridad/

Como se puede ver en la figura, la cámara de seguridad es la última opción por los usuarios, sin embargo, es una de las opciones más eficaces tanto para dentro como para fuera de la vivienda. Alguna de las ventajas que aportan las cámaras son las siguientes:

[7] Termómetro inteligente que se conecta a un Smartphone

[8] Medio de comunicación online referente en noticias y artículos de opinión para profesionales del sector de la eficiencia energética en edificaciones y la arquitectura sostenible.

- Aunque pueda parecer mentira, el aspecto psicológico es importante, dado que este sistema antirrobo proporciona “tranquilidad mental” a los usuarios de la vivienda reconociendo que pueden ser advertidos mientras intenta entrar en la vivienda.
- Desalentar el posible robo dado que son realmente visibles.
- Son relativamente económicas y el rango de precios en venta en el mercado es amplio.
- Las cámaras de vigilancia son extremadamente útiles ya que permiten monitorear las actividades de las personas que visitan su hogar y oficina, así como los eventos. Tenemos un registro de lo que sucede.
- Recopila pruebas de los posibles delitos – robos que se practican en la vivienda.
- Puede ayudarle a tomar decisiones correctas y justas a la hora de resolver disputas, tanto en el ámbito doméstico como en el profesional. tenemos imágenes para resolver disputas.

El articulo también describe algunas desventajas cómo: problemas de privacidad, las instalaciones complejas no son baratas, no se puede detener el robo “in situ” sino que es una medida de aviso y registro, y al ser un sistema electrónico, en el peor de los casos, pues existen los hackers.
Un apartado relevante del artículo es sobre las cámaras IP donde dan su definición tipos de cámara y resalta que la principal ventaja de la cámara IP reside en que es un dispositivo de vigilancia a través de vídeo permitiendo ver las imágenes en tiempo real a distancia, a través de la conexión con una dirección IP de Internet. Se pueden encontrar a la venta con especificaciones técnicas de consumo normal, para casa, o más desarrolladas para profesionales.

Finalmente, el artículo describe los siguientes consejos a la hora de comprar una cámara de seguridad:

- ¿Qué funciones necesitas?… Decide si quieres evitar sólo intrusiones o también utilizar el sistema en caso de atraco, de urgencias médicas o para el control de entradas de personas (familiares, hijos, empleados, etcétera.)
- Tenemos que determinar el tipo de control que necesitamos. Sí únicamente queremos que se graben las imágenes o queremos ver lo que está ocurriendo por medio del móvilo otro aparato.
- Para montar un sistema de seguridad es importante señalar las debilidades de la casa sobre un pequeño esquema – croquis, es decir, los principales accesos; puertas, ventanas, garaje, balcones…
- Mira las posibles ubicaciones de las cámaras. Por ejemplo, si existen lugares que pueden acceder, pero no hay nada de valor (Una caseta en el jardín de trastos o un garaje independiente)… Debes pensar si en estos espacios necesitas realmente seguridad.
- Debes de considerar el número de usuarios de la vivienda. La instalación debe ser práctica y su activación o desactivación también; sea con un mando

a distancia, por voz, teclado y por el móvil.

- Mira la calidad de la imagen, mejor si es de HD 1080P.
- Por último, debes de determinar el grado de actuación, es decir, sí ocurre un robo cómo seré avisado. Sea por un SMS al móvil, se por medio de una alarma sonora o un sistema conectado a un CRA (Centro de recepción de alertas) que conecta la policía.

En la actualidad se encuentran trabajos de grado en la relacionados con la seguridad de la información en dispositivos específicos es el caso de “Seguridad de la Información en Dispositivos Smartwatch”, es un proyecto realizado por estudiantes de postgrado de la Universidad Católica donde se analizan los riesgos para llegar a la definición de recomendaciones sobre el uso de Smartwatch, dispositivos IOT. También se encuentran investigaciones en instituciones y portales, un ejemplo llamado “Seguridad en la instalación y uso de dispositivos IOT”, que es una guía realizada por INCIBE[9] sobre la seguridad de entornos IOT en empresas. Contiene conceptos sobre IOT, amenazas hacia los dispositivos y finalmente medidas de seguridad que deben aplicar los usuarios y que se deben aplicar a los dispositivos.

[9] Instituto Nacional de Ciberseguridad, España.

5. METODOLOGÍA

Para el desarrollo de este trabajo se establecieron cuatro fases, en donde ninguna es requisito de la otra, por lo cual se pueden ir ejecutando al mismo tiempo.

5.1 FASES DEL TRABAJO DE GRADO

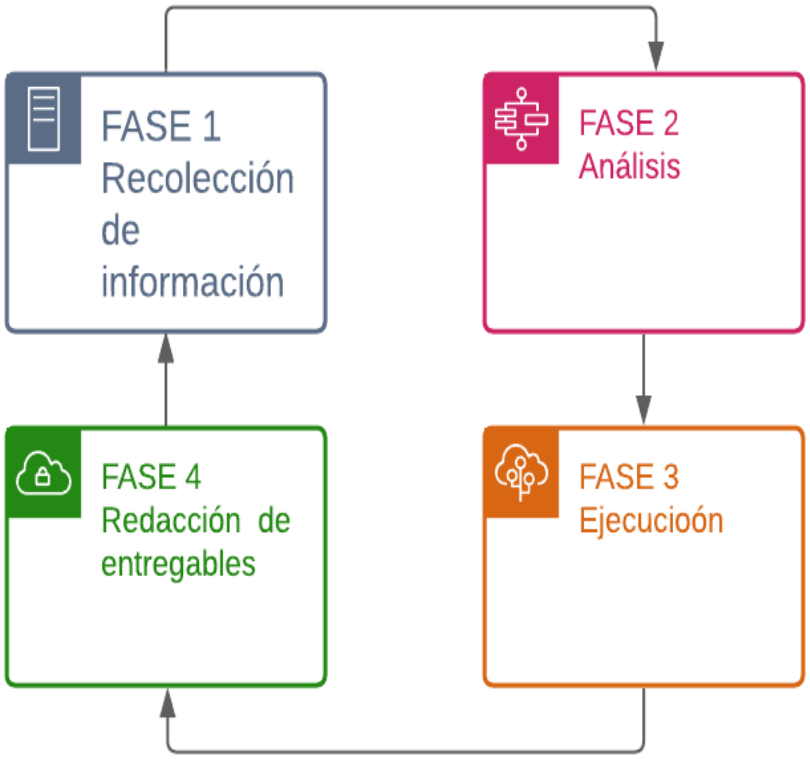


Figura 10. Fases del proyecto. Figura propia

Fase 1: Recolección de la información
Se realiza mediante bases de datos, libros, revistas, estudios de gremios nacionales e internacionales, seminarios y material digital. Se establecieron los siguientes tipos de búsqueda

1.1 Información general sobre las cámaras de vigilancia en viviendas.
1.2 Proceso de compra, instalación y funcionamiento de las cámaras IOT
1.3 Seguridad de la información en cámaras IP

Fase 2: Análisis de la información
Se realizará el análisis de la información recopilada para la identificación de riesgos y controles de seguridad necesarios en las cámaras IP, se realizan dos pasos:

2.1 Revisar el material de la fase 1 e identificar la información relevante para el alcance del proyecto

2.2 Focalizar la investigación en la identificación de riesgos y controles de seguridad necesarios, específicamente en cámaras de vigilancia IP que existen actualmente.

Fase 3: Ejecución

3.1 Durante el desarrollo de la investigación se listarán los riesgos y controles de seguridad necesarios

3.2 Elaboración de las recomendaciones mínimas de seguridad para garantizar el buen uso de cámaras un entorno IOT.

Fase 4: Desarrollo de entregables

Una vez se haya culminado cada una de las fases de la investigación y se haya logrado el cumplimiento del objetivo general, se realizará la entrega de:

4.1 Redacción de este documento

4.2 Redacción de la guía

4.3 Redacción del artículo IEEE

5.2 INSTRUMENTOS O HERRAMIENTAS UTILIZADAS

- Tabla de Excel comparativa de las cámaras IP
- Motor de búsqueda de seguridad Shodan.
- Tipos de búsqueda en google de cámaras IP, para medir seguridad.
- Matriz de riesgos en Excel

5.3 ALCANCES Y LIMITACIONES

El alcance de este proyecto de investigación es analizar las condiciones de seguridad de la información que están presentes en las cámaras de seguridad IP, con el fin de identificar los riesgos para este tipo de cámaras y generar recomendaciones para las personas del común que quieran adquirir estos dispositivos y no cuentan con un conocimiento técnico sobre seguridad. La investigación se realizará para y en pro de viviendas colombianas, incluyendo propiedad horizontal.

La limitación del proyecto está enfocada en el tipo de cámaras, que solo incluye cámaras IP, que son utilizadas para la vigilancia en los hogares. Tampoco se tendrá en cuenta los sistemas de vigilancia que incluyen otros dispositivos como sensores, alarmas, detectores de movimiento, entre otros. A su vez a las cámaras seleccionadas no se les realizaran pruebas de funcionamiento que permitan determinar sus vulnerabilidades y riesgos potenciales.

6. PRODUCTOS A ENTREGAR

- Documento de trabajo de grado: Formato establecido por la universidad con todo el desarrollo del trabajo
- Matriz de riesgos con la identificación de las características de seguridad de las cámaras IP que están enfocadas al sector hogar.
- Guía de recomendaciones: Con el análisis de riesgos de las cámaras IP se realizará un documento con recomendaciones de seguridad.

7. ENTREGA DE RESULTADOS E IMPACTOS

En la actualidad tener un sistema de vigilancia o una cámara de seguridad es una solución óptima para mantener alejados a los ladrones y proteger las viviendas. Para iniciar la investigación se escogieron cuatro (4) cámaras IP teniendo en cuenta a las de consumo masivo que se encuentran en las páginas web comerciales que venden productos en Colombia. Se identificaron en la tabla 3 las características generales compartidas por los dispositivos.

7.1 CARACTERISTICAS GENERALES DE LAS CAMARAS IP

La tabla 3 se realizó teniendo en cuanta los manuales de cada cámara IP.

MARCA	**TP-LINK TAPO C200**	**HUSKY AIR 720P C3W**	**YOOSEE V380 WIFI**	**D-LINK DSC 6010L**
				
RED				
Seguridad	Cifrado AES de 128 bits con SSL / TLS	64/128-bit WEP	64/128-bit WEP	64/128-bit WEP
Tarifa inalámbrica	11 Mbps (802.11b) 54 Mbps	IEEE802.11 b/g/n	IEEE 802.11b / g / n	IEEE 802.11 n
Frecuencia	2.4 GHz	2.4GHz ~ 2.4835 GHz	2.4GHz ~ 2.4835 GHz	2.4GHz
Seguridad inalámbrica	WPA / WPA2-PSK	WPA/WPA2, WPA-PSK/WPA2-PSK, WPS	Cifrado WPS	WPA/WPA2, WPS
NOTIFICACIONES DE ACTIVIDAD				
Disparador de entrada	Detección de movimiento	Detección de movimiento inteligente	Detección de movimiento inteligente	Detección de movimiento inteligente
Notificación de salida	Notificación de inserción	Notificación de inserción	Notificación de inserción	Notificación de inserción
VIDEO				
Compresión de Video	H.264	H.264	H.264	H.264/MPEG-4 Multicast streaming
Cuadros por Segundo	15 FPS	25 FPS		15 FPS

Vídeo transmitido en vivo	1080p	1080p	720p HD	1600p HD
SISTEMA				
Certificación Regulatoria	FCC, IC, CE, NCC	No disponible	No disponible	CE, CELVD,FCC, C-Tick
Requisitos del sistema teléfono	iOS 9+, Android 4.4+	iOS 7+, Android 4.4+	iOS 2,3+, Android 2.3+	iOS 6+, Android 4.3+
AMBIENTE				
Temperatura en Funcionamiento	0 ° C ~ 40 ° C (32 ° F ~ 104 ° F)	-22 ° F ~ 140 ° F (-30 ° C ~ 60 ° C)	-22 ° F ~ 140 ° F (-10 ° C ~ 50 ° C)	-20 ° F ~ 158 ° F (-20 ° C ~ 70 ° C)
Humedad en Funcionamiento	10% ~ 90% RH sin condensación	95% o menos (sin condensación)	90% o menos (sin condensación)	95% o menos (sin condensación)
HARDWARE				
LED Indicador	LED del sistema	LED del sistema	LED del sistema	LED del sistema
Entrada del Adaptador	100-240 VCA, 50/60 Hz, 0,3 A	DC 12V±10%	Dc5±0. 3 V	100 a 240 V AC, 50/60 Hz
Salida del Adaptador	9.0V / 0.6A	6 W	3,5 W	3,9 W
Dimensiones (An x Pr x Al)	86,6 x 85 x 117,7 mm (3,4 x 3,3 x 4,6 pulg.)	2.82*3.78*5.92”	14x13x11cm	14x13x11cm
CAMARA				
Sensor de Imagen	1/2.9“	1 / 2.7 “Escaneó progresivo CMOS	1/4 720 p sensor CMOS progresivo	1/3.2” 2 megapíxeles progresivo
Resolución	1080p Full HD	1920 × 1080, soporte de doble flujo	720 p (1280*720), VGA (640*480)	FULL HD p (1600*1200)
Lente	F / NO: 2,4; Longitud focal: 4 mm	2.8MM@F2.2	3.6mm/F1.4/56.14 °	1.25 mm F2.0
Rango de vista	360° horizontal, 114° vertical	103° horizontal, 118° diagonal	355° horizontal, 90° vertical	180° horizontal, 180° vertical
Visión nocturna	LED IR de 850 nm hasta 30 pies	Filtro de corte IR conmutación automática	11 IR Led 5mm. Gama IR: 10m	No disponible
AUDIO				
Comunicación de audio	Audio bidireccional	Audio bidireccional	Audio bidireccional	Audio bidireccional
Entrada y salida de audio:	Micrófono y altavoz integrados	Micrófono y altavoz integrados	Micrófono y altavoz integrados	Micrófono y altavoz integrados

Tabla 3. Características de cámaras IP, Tabla propia.

7.2 CARACTERISTICAS DE SEGURIAD CAMARAS IP

Con base en la tabla anterior e información de los manuales de cada cámara se registran las siguientes características de seguridad en la tabla 4.

CAMARA	TP-LINK TAPO C200	HUSKY AIR 720P C3W	YOOSEE V380 WIFI	D-LINK DSC 6010L
CARACTERISTICAS DE SEGURIDAD	Comunicación WIFI	Comunicación WIFI	Comunicación WIFI	Comunicación WIFI
	Vigilancia en tiempo real 24/7	Vigilancia en tiempo real 24/7	Vigilancia en tiempo real 24/7	Vigilancia en tiempo real 24/7
	Estándar H.264	Estándar H.264	Estándar H.264	Estándar H.264
	Método WPA / WPA2-PSK	WPA/WPA2, WPA-PSK/WPA2-PSK, WPS	Autenticación WPS	WPA/WPA2, WPS
	Visualización nocturna	Visualización nocturna	Visualización nocturna	Almacenamiento tarjeta MicroSD
	Almacenamiento tarjeta MicroSD	Almacenamiento tarjeta MicroSD	Almacenamiento tarjeta MicroSD	Función "Configuración Zero"
	Audio doble vía	Almacenamiento en la nube	Audio doble vía	
		Uso en exteriores		
		Protección contra agua y polvo Antenas WIFI dobles		
Información recolectada para acceder a la vista de la cámara se relaciona a continuación	Ingreso a las funciones de la cámara a través de la APP de la marca TP-Link. Solicitud de ubicación. Aceptar términos de servicio, políticas de privacidad. Solicitud de dirección de correo electrónico	Ingreso a las funciones de la cámara a través de la APP de la marca EZVIZ. Solicitud de ubicación. Aceptar términos de servicio, políticas de privacidad y uso de cookies. Solicitud de dirección de correo electrónico. Solicitud de número de teléfono	Ingreso a las funciones de la cámara a través de la APP de la marca Yoosee Gwell. Solicitud de ubicación. Aceptar términos de servicio, políticas de privacidad. Solicitud de dirección de correo electrónico. Solicitud de número de teléfono	Ingreso a las funciones de la cámara a través de la APP de la marca Mydlink. Solicitud de ubicación. Aceptar términos de uso, política de privacidad. Solicitud de dirección de correo electrónico

Tabla 4. Características de Seguridad. Tabla propia.

7.3 AMENAZAS

Las cámaras IP son susceptibles a ser atacadas. Esto implica que es posible acceder al contenido que graba una cámara, ya sea para obtener imágenes o información sensible, también pueden ser hackeadas para que muestren un contenido falso y ser vulnerables a malware especializado convirtiéndose en un medio para atacar, Si el sistema está abierto a internet, las cámaras IP, no están seguras de sufrir un ataque informático**,** pudiendo ocasionar peligros en la seguridad. El problema principal de las cámaras IP es que no están correctamente aseguradas mediante barreras y defensas informáticas, ya que no disponen de capacidad suficiente para cifrar de manera efectiva la comunicación inalámbrica, o muestran problemas de seguridad al conectarse con servidores externos. En la tabla 5 se ilustraron algunas amenazas a las que se ven expuestas las cámaras IP dependiendo de su tipo, fuente y origen que puede ser deliberado, accidental o de ambiente.

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego, Agua , polvo	Accidental, Ambiente, Deliberado
	Destrucción del equipo	Ambiente
Pérdida de los servicios esenciales	Perdida en el suministro de energía	Accidental, Deliberado
	Falla en las telecomunicaciones del equipo	Accidental, Deliberado
Compromiso de la información	Interceptación de señales de interferencia comprometedoras	Deliberado
	Espionaje remoto extorsivo	Deliberado
	Escucha encubierta	Deliberado
	Hurto de dispositivo	Deliberado
	Datos provenientes de fuentes no confiables	Deliberado
	Denegación distribuida de servicio (DDoS)	Deliberado
	Manipulación con Software	Deliberado
Fallas técnicas	Fallas de la cámara	Accidental
Acciones no autorizadas	Uso no autorizado de la cámara	Deliberado
	Uso de software falso o copiado	Deliberado
Compromiso de las funciones	Errores de los usuarios	Accidental

Tabla 5. Norma Técnica Colombiana NTC-ISO/IEC 27005, ANEXO C, Ejemplos de amenazas comunes.

7.4 VULNERABILIDADES

Todas las cámaras de seguridad son vulnerables. La desafortunada realidad es que en el entorno de Ciberseguridad actual, la pregunta no es si un sistema será hackeado, sino cuándo, lo que hace que las medidas de seguridad continuas y proactivas sean una necesidad. Los delincuentes informáticos pueden entrar en un

sistema de video vigilancia de diversas formas. Además de hackear las cámaras, pueden ingresar a la red a través de:

- El sistema operativo de la computadora que utiliza (por ejemplo, Microsoft Windows, Linux, etc.)
- El software que utiliza su sistema, incluida la grabación de video digital (DVR), la grabación de video en red (NVR) o el software del sistema de gestión de video (VMS)
- Cualquier puerto de firewall que pueda estar usando para acceder a los controles del sistema.

Dados estos puntos de entrada adicionales, la seguridad de las cámaras IP depende no solo de las cámaras que se utilicen, sino también de la tecnología de red y la configuración del sistema. En general, la seguridad relativa que proporciona el sistema depende de cómo esté configurado el acceso.

Los piratas informáticos buscan vulnerabilidades para explotar, generalmente con fines maliciosos. Hay muchas razones por las que los piratas informáticos pueden querer ingresar a su sistema de vigilancia de cámaras de seguridad IP, incluidas algunas que prometen recompensas potencialmente enormes:

- Pueden estar planeando un robo o un ataque físico contra el edificio o sus ocupantes.
- Si pueden entrar en cámaras de red, pueden observar la seguridad física del lugar, incluso cuando los guardias van y vienen y donde hay oportunidades para ingresar al edificio. Una vez que sepan dónde y cuándo ingresar, toda su instalación y todos sus ocupantes están en riesgo.
- Robar información personal con el fin de realizar ataques de Phishing para obtener información bancaria y de tarjetas de crédito de personas.
- Para instalar malware, como Keyloggers, para capturar contraseñas a medida que se ingresan o Ransomware que toma su sistema como rehén hasta que le pague al hacker para que lo libere. (security, 2018)

La importancia de la información obtenida por las cámaras y sus múltiples usos ha llevado a la explotación de vulnerabilidades y posibles ataques, en la tabla 6 se especifican las vulnerabilidades generales de cámaras IP y posibles ataques frecuentes.

VULNERABILIDADES	ATAQUES FRECUENTES
Comunicación con casa matriz en texto plano y sin autenticación Firmware actualizable sin firmas digitales	1. MITM Hombre en el medio, que permiten verificar la comunicación entre dos dispositivos y así re direccionar tráfico.
Inyección código	

Inyección SQL	2. Ataques de fuerza bruta: buscan encontrar contraseñas a través de combinación de caracteres básicos. 3. Sniffing: olfatea y visualiza el tráfico en la búsqueda de vulnerabilidades
Asignación incorrecta de permisos para control de recursos	
Acceso por Telnet	
Funciones ocultas	
Controles de acceso inadecuado	
Credenciales inseguras	
Autenticación por defecto	
Bloqueo a través de solicitudes POST Autenticación HTTP básica	
Corrupción de memoria	

Tabla 6. Vulnerabilidades y ataques frecuentes de cámaras IP. Recuperado de: https://repository.unad.edu.co/bitstream/handle/10596/33326/naariass.pdf?sequence=1&isAllowed=y

Por otro lado se registran las vulnerabilidades de El Common Vulnerabilities and Exposures (CVE) que es una lista de identificadores comunes para vulnerabilidades de seguridad cibernética conocidas públicamente. CVE proporciona información sobre una vulnerabilidad de software única. Cada CVE único tiene un ID de CVE y una breve descripción de la vulnerabilidad o exposición de seguridad. Se puede buscar por palabras clave específicas o directamente en un ID de CVE específico para obtener información sobre la vulnerabilidad y la exposición.
Por ejemplo, con la palabra clave "IP CAMERAS" se pueden observar las vulnerabilidades registradas hasta la fecha, se identificaron 91 vulnerabilidades conocidas de diferentes marcas, tipos y versiones. En la tabla 7 se registraron el nombre, descripción y análisis de algunas relevantes al proyecto relacionadas con las marca TP-Link y D-Link.

NOMBRE	DESCRIPCION	ANALISIS
CVE-2019-10711	El control de acceso incorrecto en la transmisión RTSP y el portal web en todas las cámaras IP basadas en el firmware Hisilicon Hi3510 (hasta la versión de Webware V1.0.1) permite a los atacantes ver una transmisión RTSP al conectarse a la transmisión con credenciales ocultas (invitado o usuario) que no son ni visualizados ni configurables en la aplicación de gestión móvil CamHi o keye de la cámara. Esto afecta a ciertos dispositivos etiquetados como HI3510, HI3518, LOOSAFE, LEVCOECAM, Sywstoda, BESDER, WUSONGLUSAN, GADINAN, Unitoptek, ESCAM, etc.	Gracias a la vulnerabilidad presentada en el firmware Hisilicon Hi3510, permite acceso a la transmisión en tiempo real de las cámaras, con usuarios de forma oculta al registro de la aplicación, esto a su vez genera una exposición de la intimidad familiar donde se encuentra instalada, así como la afectación de vario modelos de cámaras en las cuales se instaló la versión del firmware mencionado.
CVE-2019-10710	Los permisos inseguros en el portal de	El acceso a los portales de

NOMBRE	DESCRIPCION	ANALISIS
	administración web en todas las cámaras IP basadas en el firmware Hisilicon Hi3510 permiten a los atacantes autenticados recibir credenciales WiFi de texto sin cifrar de la red a través de una solicitud HTTP específica. Esto afecta a ciertos dispositivos etiquetados como HI3510, HI3518, LOOSAFE, LEVCOECAM, Sywstoda, BESDER, WUSONGLUSAN, GADINAN, Unitoptek, ESCAM, etc.	administración a través de la vulnerabilidad del firmware Hisilicon Hi3510, genera que el atacante pueda extraer información que debe ser segura para los miembros del grupo donde se encuentra instalada la cámara, esto permite que se pueda tener acceso a información adicional utilizando otro tipo de ataque hacia los diferentes dispositivos en la red.
CVE-2018-18441	Las cámaras Wi-Fi de la serie D-Link DCS exponen información confidencial sobre la configuración del dispositivo. Los dispositivos afectados incluyen muchos de las series DCS, como: DCS-936L, DCS-942L, DCS-8000LH, DCS-942LB1, DCS-5222L, DCS-825L, DCS-2630L, DCS-820L, DCS-855L, DCS-2121, DCS-5222LB1, DCS-5020L y muchos más. Hay muchas versiones de firmware afectadas a partir de la 1.00 y superiores. Se puede acceder al archivo de configuración de forma remota a través de: <Camera-IP> /common/info.cgi, sin autenticación. El archivo de configuración incluye los siguientes campos: modelo, producto, marca, versión, compilación, hw_version, versión nipca, nombre del dispositivo, ubicación, dirección MAC, dirección IP, dirección IP de la puerta de enlace, estado inalámbrico, configuración de entrada / salida, altavoz y sensor ajustes.	Al explotar la vulnerabilidad presentada en las cámaras, un atacante puede llegar a tener información valiosa del dispositivo ubicándose en el archivo de configuración de forma remota a través de: <Camera-IP> /common/info.cgi, sin autenticación, lo que le puede permitir conocer información confidencial como: modelo, producto, marca, versión, compilación, versión del hardware, nombre del dispositivo, ubicación, dirección MAC, dirección IP, dirección IP de la puerta de enlace, estado inalámbrico, configuración de entrada / salida, altavoz y sensor de ajustes, implicando poder llegar a extraer datos de otro tipo de dispositivo que se encuentre conectado en la misma red que esta la cámara.
CVE-2013-3688	Las cámaras IP TP-Link TL-SC3171, TL-SC3130, TL-SC3130G, TL-SC3171G, y posiblemente otros modelos antes del firmware beta LM.1.6.18P12_sign6, no restringen adecuadamente el acceso a ciertas funciones administrativas, lo que permite a los atacantes remotos (1) provocar una denegación de servicio (reinicio del dispositivo) a través de una solicitud a cgi-bin / reboot (2) causar una denegación de servicio (reiniciar y restablecer los valores predeterminados de fábrica) mediante una solicitud a cgi-bin / hardfactorydefault.	Con el firmware antes de la versión LM.1.6.18P12_sign6, del que disponen las cámaras, permite que un atacante pueda generar gran afectación en el dispositivo, ocasionando una denegación de servicio) a través de una solicitud a cgi-bin / reboot o en su defecto restableciendo la configuración de fábrica de la cámara mediante una solicitud a cgi-bin / hardfactorydefault. Esto implica que el usuario no pueda acceder a la transmisión en tiempo real del dispositivo cuando lo requiera o no poder tener la grabación del sitio en el cual fue instalada si se pierde la

NOMBRE	DESCRIPCION	ANALISIS
		configuración realizada.
CVE-2013-2581	cgi-bin / firmwareupgrade en cámaras IP TP-Link TL-SC3130, TL-SC3130G, TL-SC3171, TL-SC3171G y posiblemente otros modelos antes del firmware beta LM.1.6.18P12_sign6 permite a atacantes remotos modificar la revisión del firmware a través de un " acción "preestablecida".	La vulnerabilidad presente en los diferentes modelos de cámaras de la marca TP-Link, permite que un atacante pueda modificar información esencial para el funcionamiento del dispositivo, la cual solo debería ser modificada por el fabricante cuando sea necesario.
CVE-2013-2580	Vulnerabilidad de carga de archivos sin restricciones en cgi-bin / uploadfile en cámaras IP TP-Link TL-SC3130, TL-SC3130G, TL-SC3171, TL-SC3171G y posiblemente otros modelos antes del firmware beta LM.1.6.18P12_sign6, permite que los atacantes remotos carguen archivos arbitrarios, luego acceda a él a través de una solicitud directa al archivo en el directorio mnt / mtd.	Con el firmware antes de la versión LM.1.6.18P12_sign6, del que disponen las cámaras, permite que un atacante pueda realizar la carga de archivos sin tener restricciones a este tipo de acciones y que en el momento que lo desee genere una solicitud para acceder de forma directa a estos archivos.
CVE-2013-2579	Las cámaras IP TP-Link TL-SC3130, TL-SC3130G, TL-SC3171, TL-SC3171G y posiblemente otros modelos antes del firmware beta LM.1.6.18P12_sign6 tienen una contraseña vacía para la cuenta "qmik" codificada, que permite a los atacantes remotos obtener acceso administrativo a través de una sesión TELNET.	La vulnerabilidad le permite a un atacante tener acceso de forma remota a la cámara con una sesión TELNET, utilizando una cuenta predeterminada para la administración del dispositivo. Esto implica que se pueda conocer la información ingresada para la configuración, así como poder acceder a la transmisión en tiempo real.
CVE-2013-2578	cgi-bin / admin / servetest en cámaras IP TP-Link TL-SC3130, TL-SC3130G, TL-SC3171, TL-SC3171G y posiblemente otros modelos antes del firmware beta LM.1.6.18P12_sign6 permite a atacantes remotos ejecutar comandos arbitrarios a través de shell meta caracteres en (1) el parámetro ServerName y (2) otros parámetros no especificados.	La vulnerabilidad le permite al atacante poder ejecutar comandos arbitrarios de forma remota, lo cual implica modificaciones que afectan la configuración y disponibilidad del dispositivo.
CVE-2013-2573	Existe una vulnerabilidad de Command Injection en el parámetro ap del archivo /cgi-bin/mft/wireless_mft.cgi en las cámaras IP TP-Link TL-SC 3130, TL-SC 3130G, 3171G. y 4171G 1.6.18P12s, que podría permitir que un usuario malintencionado ejecute código arbitrario.	La vulnerabilidad presente en el parámetro ap del archivo /cgi-bin/mft/wireless_mft.cgi, puede ocasionar que un atacante ejecute código con el fin de alterar el funcionamiento normal del dispositivo. Esto ocasiona que se afecte la disponibilidad de la cámara.
CVE-2013-2572	Existe una vulnerabilidad de omisión de	Por implementación de fábrica se

NOMBRE	DESCRIPCION	ANALISIS
	seguridad en las cámaras IP TP-LINK TL-SC 3130, TL-SC 3130G, 3171G, 4171G y 3130 1.6.18P12 debido a las credenciales codificadas de forma predeterminada para la interfaz web administrativa, que podría permitir que un usuario malintencionado obtenga acceso no autorizado a archivos CGI.	dejan credenciales guardadas de forma predeterminada para el acceso a la interfaz web que permite administrar la cámara, esto implica que un atacante pueda acceder a esta información al identificar los scripts que la almacenan, de llegar a explotar esta vulnerabilidad, ocasiona que se pueda modificar información esencial para el funcionamiento de la cámara.
CVE-2013-1599	Existe una vulnerabilidad de Command Injection en el script /var/www/cgi-bin/rtpd.cgi en las cámaras IP D-Link DCS-3411/3430 firmware 1.02, DCS-5605/5635 1.01, DCS-1100L / 1130L 1.04, DCS- 1100/1130 1.03, DCS-1100/1130 1.04_US, DCS-2102/2121 1.05_RU, DCS-3410 1.02, DCS-5230 1.02, DCS-5230L 1.02, DCS-6410 1.00, DCS-7410 1.00, DCS-7510 1.00 y WCS-1100 1.02, que podría permitir que un usuario malintencionado remoto ejecute comandos arbitrarios a través de la interfaz web de la cámara.	La vulnerabilidad presente en el script /var/www/cgi-bin/rtpd.cgi en las cámaras IP D-Link, puede ocasionar que un atacante ejecute código a través de la interfaz web con el fin de alterar el funcionamiento normal del dispositivo. Esto ocasiona que se afecte la disponibilidad y normal funcionamiento de la cámara.
CVE-2012-4046	La cámara D-Link DCS-932L con firmware 1.02 permite a atacantes remotos descubrir la contraseña a través de un paquete de transmisión UDP, como se demuestra al ejecutar el Asistente de configuración de D-Link y leer el valor _paramR ["P"].	La vulnerabilidad presente en el firmware 1.02, permite que un atacante pueda capturar la contraseña de acceso a través de la transmisión de UDP, lo que implica que sea accedida sin tener limitaciones y pase desapercibido el acceso.

Tabla 7. Vulnerabilidades CVE "IPCAMERAS". Recuperado de: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=IP+CAMERA

En el proceso de instalación de una cámara IP también se pueden identificar vulnerabilidades. A continuación en la tabla 8 se registraron los pasos para instalar los 4 dispositivos mencionados.

PROCESO DE INSTALACION CAMARAS IP	1. Descargar la aplicación de la marca en el teléfono celular	7. Se debe otorgar permiso a la aplicación para que acceda a la ubicación del dispositivo

	2. Permitir a la aplicación enviar notificaciones al teléfono	8. Desde el teléfono se debe realizar la conexión a la red inalámbrica que trae por defecto la cámara, esto permitirá que se pueda sincronizar con la aplicación
	3. Realizar el registro de un correo electrónico	9. Ingresar a la aplicación en el teléfono celular, validar la conexión a la cámara y seleccionar la red WIFI a la cual se conectará
	4. Revisar la bandeja del correo electrónico registrado para verificar la cuenta y poder acceder a la aplicación	10. Luego de tener la cámara sincronizada, se debe asignar un nombre para identificarla en la red
	5. Conectar la cámara al adaptador de energía y proceder a encenderla	11. Seleccionar el lugar físico en el cual se encuentra instalada la cámara (sala, habitación, patio, entre otros)
	6. Desde la aplicación en el teléfono ir a la opción añadir cámara, seleccionar el modelo y esperar que la cámara se sincronice con el teléfono	12. Finalmente al completar el proceso de sincronización, se podrá ingresar a la visualización de vídeo de la cámara

Tabla 8. Proceso de instalación cámaras IP. Tabla propia.

Con la información recopilada sobre amenazas y vulnerabilidades se generó la tabla 9 donde se asocian las vulnerabilidades a las amenazas ya establecidas para las cámaras IP seleccionadas.

AMENAZA	VULNERABILIDAD
Fuego, Agua y Polvo	Susceptibilidad a la humedad, polvo y fuego.
Destrucción de la cámara	Ubicación vulnerable del dispositivo
Perdida en el suministro de energía	Funcionamiento inadecuado del suministro eléctrico
Falla en las telecomunicaciones de la cámara	Conexión deficiente en la comunicación
	Conexiones de red sin protección
Interceptación de señales de interferencia comprometedoras	Falta de cifrado en datos enviados a través de la red (contraseñas e imágenes de la grabación en tiempo real)
Espionaje remoto extorsivo	Contraseñas de cámara IOT por defecto
	Contraseñas de sitio web de acceso a la cámara por defecto o igual al de la cámara IOT con contraseña por defecto

Escucha encubierta	Trafico sensible sin protección
Hurto de dispositivo	Ausencia de protección física
Datos provenientes de fuentes no confiables	Inyección de código
Denegación distribuida de servicio (DDoS)	Contraseñas de cámaras IOT por defecto
Manipulación con Software	Descarga y uso no controlado de software
Fallas de la cámara	Falta de mantenimiento preventivo
	Firmware desactualizado
	Acceso de forma remota sin autenticación
	Errores de fabricación
	Autenticación y registró de dispositivos por compatibilidad de fábrica sin intervención del usuario
Uso no autorizado de la cámara	Falta de autenticación robusta
	Acceso de forma remota sin autenticación
Uso de software falso o copiado	No verificar la autenticidad del sitio web al que se accede para ingresar a las funciones de la cámara
Errores de los usuarios	Falta de conciencia acerca de la seguridad
	Autenticación débiles

Tabla 9. Vulnerabilidades. Tabla propia.

7.5 RIESGO

7.5.1 CRITERIOS DE RIESGO

Para la identificación de riesgos se realizó una matriz (Ver tabla 12) donde se relacionan las amenazas con vulnerabilidades y se identifica el riesgo que es la probabilidad por el impacto. En la tabla se especifica la descripción y consecuencia de cada riesgo, en otra columna para cual cámara aplica siendo cámara: 1 TP-LINK TAPO C200, cámara 2: HUSKY AIR 720P C3W, cámara 3: YOOSEE V380 WIFI, y cámara 4: D-LINK DSC 6010L. La columna final representa el número del riesgo. El orden de los riesgos se estableció por la relevancia respecto a seguridad IOT.

En la tabla 10 se generó un mapa de calor para el nivel de riesgo, teniendo en cuenta que tanto la probabilidad como el impacto se clasifican en Bajo=1, Moderado=2 y Alto=3.

PROBABILIDAD				
	ALTO	**3**	**6**	**9**
	MODERADO	**2**	**4**	**6**
	BAJO	**1**	**2**	**3**
		BAJO	**MODERADO**	**ALTO**
			IMPACTO	

Tabla 10. Mapa de calor. Tabla propia.

En la tabla 11, Teniendo en cuenta el nivel de riesgo se generó una escala de cantidades y colores.

RIESGO			
MIN	**MAXI**	**COLOR**	**ESTATUS**
1	3		**BAJO**
4	6		**MODERADO**
7	9		**ALTO**

Tabla 11. Nivel de riesgo. Tabla propia.

7.5.2 MATRIZ DE RIESGOS

AMENAZA	VULNERABILIDAD	DESCRIPCION DEL RIESGO	CONSECUENCIAS	PROBABILIDAD	IMPACTO	RIESGO	CAMARA	#RIESGO
Espionaje remoto extorsivo	Contraseñas de cámara IOT por defecto	Criminales realizan espionaje remoto de la información intima de las personas registrada por cámaras IOT domésticas, con fines extorsivos, aprovechando que mantienen su contraseña de fabrica	Pérdidas económicas por exigencias de naturaleza extorsiva de los criminales para no revelar información intima de las personas	3	3	9	1,2,3,4	R1
	Contraseñas de sitio web de acceso a la cámara por defecto o igual al de la cámara IOT con contraseña por defecto	Criminales realizan espionaje remoto de la información intima de las personas registrada por cámaras IOT domésticas, con fines extorsivos, aprovechando que mantienen su contraseña de fabrica	Pérdidas económicas por exigencias de naturaleza extorsiva de los criminales para no revelar información intima de las personas	3	3	9	12,3,4	R2
Escucha encubierta	Trafico sensible sin protección	Falta de cifrado en los datos enviados que impida que se extraiga información sensible del usuario (contraseñas, cuentas de correo). Un atacante puede acceder al dispositivo sin tener limitaciones pasando desapercibido	Afectaciones de la reputación del (los) dueño(s) de las cámaras IOT, por invasión de su intimidad	2	2	4	1,2,3,4	R3

AMENAZA	VULNERABILIDAD	DESCRIPCION DEL RIESGO	CONSECUENCIAS	PROBABILIDAD	IMPACTO	RIESGO	CAMARA	#RIESGO
		Permite a atacantes remotos descubrir las contraseñas a través de un paquete de transmisión UDP	Manipulación indebida de las credenciales de la cámara IOT por parte de un atacante	2	2	4	4	R4
			Perdida reputacional del fabricante (D-LINK)	1	2	2	4	
Denegación distribuida de servicio (DDoS)	Contraseñas de cámaras IOT por defecto	Denegación distribuida del servicio de páginas de terceros a través del uso de cámaras IOT como parte de una BotNet aprovechando que mantienen su contraseña de fábrica	Ingresos no percibidos por ventas de bienes y servicios no realizadas.	2	3	6	1,2,3,4	R5
		Incriminación de los dueños de cámaras IOT en un ataque de Denegación distribuida del servicio de páginas de terceros a través del uso de sus cámaras aprovechando que mantienen su contraseña de fábrica	Posibles problemas legales y afectación de la reputación del (los) dueño(s) de las cámaras IOT reclutadas para la BotNet	2	3	6	1,2,3,4	R6
		Incriminación de los dueños de cámaras IOT en un ataque de Denegación distribuida	Posibles pérdidas económicas por la exigencia de indemnizaciones	2	3	6	1,2,3,4	R7

AMENAZA	VULNERABILIDAD	DESCRIPCION DEL RIESGO	CONSECUENCIAS	PROBABILIDAD	IMPACTO	RIESGO	CAMARA	#RIESGO
		del servicio de páginas de terceros a través del uso de sus cámaras aprovechando que mantienen su contraseña de fábrica	por parte de los terceros propietarios de los sitios afectados.					
Errores de los usuarios	Falta de conciencia acerca de la seguridad	Exposición a ciberataques al no leer los manuales de uso de las cámaras IP y no seguir buenas prácticas de seguridad.	Sustracción y/o perdida de la información resguardada en la cámara IP	3	3	9	1,2,3,4	R8
	Autenticación débiles	Exposición a ataques de fuerza bruta y diccionario permitiendo que un atacante descifre las claves de acceso	Pérdidas económicas por exigencias de naturaleza de criminales para no revelar información intima de las personas.	3	3	9	1,2,3,4	R9
Interceptación de señales de interferencia comprometedoras	Falta de cifrado en datos enviados a través de la red (contraseñas e imágenes de la grabación en tiempo real)	Exposición a Sniffing ocasionando que un atacante pueda tener conocimiento de información susceptible para el usuario	Posibles afectaciones de la reputación del (los) dueño(s) de las cámaras IOT, al compartir la información intima de las personas a terceros	2	2	4	1,2,3,4	R10
Datos provenientes de fuentes no confiables	Inyección de código	Permite que un atacante pueda realizar la carga de archivos que intenta modificar ficheros y	Posible pérdida económica por exigencias de naturaleza	1	3	3	1	R11

AMENAZA	VULNERABILIDAD	DESCRIPCION DEL RIESGO	CONSECUENCIAS	PROBABILIDAD	IMPACTO	RIESGO	CAMARA	#RIESGO
		valores de la estructura funcional del dispositivo para llevar a cabo ataques y comprometer la seguridad y privacidad de los usuarios	extorsiva de los criminales para no revelar información intima de las personas					
			Perdida reputacional del fabricante (TP-LINK)	1	2	2	1	
Manipulación con Software	Descarga y uso no controlado de software	Realizar el acceso a las funciones de la cámara a través de software no autorizado por el fabricante que permita que la información y configuración de la cámara queden expuestos a terceros	Afectaciones de la reputación del (los) dueño(s) de las cámaras IOT, por la exposición de la información almacenada	2	3	6	1,2,3,4	R12
Uso de software falso o copiado	No verificar la autenticidad del sitio web al que se accede para ingresar a las funciones de la cámara	Exposición a Phishing permitiendo la captura de información sensible del usuario (cuentas de correo, contraseñas, ubicación del dispositivo)	Afectaciones de la reputación del (los) dueño(s) de las cámaras IOT, por la exposición de la información del usuario	2	3	6	1,2,3,4	R13
Uso no autorizado de la cámara	Falta de autenticación robusta	Afectación en la confidencialidad de la información por acceso de terceros para realizar manipulación del dispositivo	Posibles pérdidas económicas debido a la manipulación de la cámara por parte de terceros	2	3	6	1,2,3,4	R14

AMENAZA	VULNERABILIDAD	DESCRIPCION DEL RIESGO	CONSECUENCIAS	PROBABILIDAD	IMPACTO	RIESGO	CAMARA	#RIESGO
	Acceso de forma remota sin autenticación	Permite a los atacantes remotos obtener acceso administrativo a través de una sesión TELNET que les permite conocer la información ingresada requerida para la configuración inicial (cuentas de correo, ubicación del dispositivo, números de contacto, contraseñas), así como poder acceder a la transmisión en tiempo real	Afectaciones de la reputación del (los) dueño(s) de las cámaras IOT, por invasión de la intimidad sin el consentimiento del usuario	1	2	2	1	R15
			Perdida reputacional del fabricante(TP-LINK)	1	2	2		
Fallas de la cámara	Falta de mantenimiento preventivo	Compromiso de disponibilidad de las grabaciones	Pérdida parcial o total de las grabaciones	3	3	9	1,2,3,4	R16
	Firmware desactualizado	Daño de hardware provocado por virus informático	Posible daño funcional de la cámara IP	3	3	9	1,2,3,4	R17
		Vulnerabilidades propias de fabricantes	Perdida reputacional del fabricante	1	2	2	1,2,3,4	R18
	Acceso de forma remota sin autenticación	Al explotar la vulnerabilidad presentada en las cámaras, un atacante puede llegar a tener información valiosa propia del dispositivo al ubicarse en el archivo de configuración de forma remota a través de la	Afectación reputacional del fabricante (D-LINK) al tener acceso de la información propia de la cámara (modelo, producto, marca, versión,	1	2	2	4	R19

AMENAZA	VULNERABILIDAD	DESCRIPCION DEL RIESGO	CONSECUENCIAS	PROBABILIDAD	IMPACTO	RIESGO	CAMARA	#RIESGO
		ruta: <Camera-IP> /common/info.cgi, esto sin requerir autenticación previa	compilación, nombre del dispositivo, ubicación, dirección MAC, dirección IP, dirección IP de la puerta de enlace, estado inalámbrico)					
	Errores de fabricación	Credenciales débiles para el acceso a la interfaz web administrativa del fabricante, permite que un usuario malintencionado obtenga acceso no autorizado a archivos CGI y pueda modificar información esencial para el funcionamiento de la cámara	Posibles pérdidas económicas que genere el daño del dispositivo por modificación en los parámetros de funcionamiento establecidos por el fabricante	1	2	2	1,4	R20
			Perdida reputacional del fabricante (D-LINK, TP-LINK)	1	2	2	1,4	
	Autenticación y registró de dispositivos por compatibilidad de fábrica sin intervención del usuario	Compromiso de confidencialidad a través de la función "zero configuration" si se dispone de un Router de D-Link, simplemente se enciende la Cámara y se conecta al Router mediante un cable Ethernet y la cámara se añade automáticamente	Afectación reputacional al presentarse la conexión de la cámara IP sin intervención del usuario queda expuesta la información del usuario	1	1	1	4	R21

AMENAZA	VULNERABILIDAD	DESCRIPCION DEL RIESGO	CONSECUENCIAS	PROBABILIDAD	IMPACTO	RIESGO	CAMARA	#RIESGO
		a la cuenta mydlink del usuario						
			Perdida reputacional del fabricante(D-LINK)	1	2	2		
Hurto de dispositivo	Ausencia de protección física	Compromiso de la disponibilidad de la información por robo del dispositivo	Perdida de las grabaciones	2	3	6	1,2,3,4	R22
			Pérdidas económicas al presentarse el hurto de la cámara	2	2	4	1,2,3,4	R23
		Compromiso de la confidencialidad de la información por la pérdida de las grabaciones almacenadas en la memoria SD del dispositivo	Pérdidas económicas por exigencias de naturaleza extorsiva de los criminales para no revelar información intima de las personas	2	3	6	1,2,3,4	R24
Falla en las telecomunicaciones de la cámara	Conexión deficiente en la comunicación	Compromiso de la disponibilidad sobre las grabaciones del dispositivo en un tiempo especifico	Perdida de grabaciones en un tiempo especifico	2	1	2	1,2,3,4	R25

AMENAZA	VULNERABILIDAD	DESCRIPCION DEL RIESGO	CONSECUENCIAS	PROBABILIDAD	IMPACTO	RIESGO	CAMARA	#RIESGO
	Conexiones de red sin protección	Impedimento del acceso remoto autorizado a la transmisión en tiempo real	El usuario no podrá monitorear sus grabaciones durante el tiempo que dure la falla	2	1	2	1,2,3,4	R26
		Impedimento del acceso remoto autorizado a la configuración de la cámara	El usuario no podrá modificar ninguna función de la cámara durante el tiempo que dure la falla	2	1	2	1,2,3,4	R27
		Exposición a ataques "Man in the Middle" , interceptando información transmitida en la red (direcciones IP, credenciales, imágenes en tiempo real, cuentas de correo)	Pérdidas económicas por exigencias de naturaleza extorsiva de los criminales para no revelar información intima de las personas.	2	2	4	1,2,3,4	R28
Destrucción de la cámara	Ubicación vulnerable del dispositivo	Pérdida total o parcial de la información por acceso a la propiedad de un intruso	Pérdidas económicas para el usuario por la destrucción de la cámara por parte de criminales	1	3	3	1,3,4	R29

AMENAZA	VULNERABILIDAD	DESCRIPCION DEL RIESGO	CONSECUENCIAS	PROBABILIDAD	IMPACTO	RIESGO	CAMARA	#RIESGO
Perdida en el suministro de energía	Funcionamiento inadecuado del suministro eléctrico	Pérdida parcial de la grabación en tiempo real al no tener continuidad en el servicio de energía	Posibles pérdidas económicas por variaciones en el voltaje de energía que impacten el funcionamiento de la cámara de acuerdo a lo recomendado por el fabricante	1	2	2	1,2,3,4	R30
Fuego, Agua y Polvo	Susceptibilidad a la humedad, polvo y fuego.	Indisponibilidad de la información por fallas en la grabación generando pérdida parcial o total de la información	Pérdidas económicas por afectación en el funcionamiento de la cámara derivadas de condiciones ambientales	2	1	2	1,3,4	R31

Tabla 12. Matriz de riesgos. Tabla propia

7.5.3 ANALISIS DE LA MATRIZ DE RIESGOS

Con la valoración del nivel de riesgos identificados y descritos en la tabla 11, se registraron 6 riesgos de nivel alto relacionados con amenazas de espionaje remoto por parte de criminales, errores comunes de los usuarios y fallas de la cámara, estos riesgos traen afectaciones económicas de carácter extorsivo en contra de los usuarios, pérdida total de las grabaciones e incluso perdida funcional de la cámara. También se registraron 13 riesgos de nivel medio relacionados con amenazas de escucha encubierta, Denegación distribuida de servicio (DDoS), interceptación de señales de interferencia comprometedoras, software, uso no autorizado de la cámara y hurto del dispositivo, los cuales pueden provocar afectaciones económicas, reputacionales y legales Finalmente se registraron 12 riesgos de nivel bajo relacionados con amenazas en las telecomunicaciones de la cámara, fallas de la cámara, datos provenientes de fuentes no confiables y daños físicos; Estos riesgos son considerados en este nivel debido a que su impacto no ocasiona afectaciones graves para el usuario y no están relacionados directamente con la seguridad en entorno IOT, sin embargo son considerados para evitar o cualquier pérdida. Dando continuidad a la metodología establecida se generó una guía de buenas prácticas donde se les explica a los usuarios de estos dispositivos los riesgos de los cuales pueden ser víctimas y sus respectivas recomendaciones, la cual tiene como alcance evitar o mitigar dichos riesgos.

Durante el proceso de la investigación se tuvo en cuenta 4 modelos de cámaras IP, sin embargo se concluyó que los riesgos encontrados pueden aplicar para todos los modelos de cámara IP. A continuación un resumen de la guía en la tabla 13.

NUMERO	RIESGO	RECOMENDACIONES
R1	Mantener las contraseñas por defecto de la cámara IP permite a criminales realizar espionaje remoto de la información íntima de las personas para después realizar exigencias de naturaleza extorsiva con el fin de no revelar la información robada.	En el momento de instalación de la cámara IP cambiar las credenciales que vienen por defecto.
R2	Mantener las contraseñas de sitio web de acceso a la cámara por defecto o igual al de la cámara IOT con contraseña por defecto permiten a criminales realizar espionaje remoto de la información íntima de las personas para después realizar exigencias de naturaleza extorsiva con el fin de no revelar la información robada.	Las credenciales para ingresar al sitio web de acceso a la cámara IP, deben ser cambiadas y no deben ser iguales a las de la cámara IP.
R3	Un atacante puede acceder al dispositivo sin tener limitaciones, pasando desapercibido por la falta de cifrado en los datos enviados que impida que se extraiga información sensible del usuario (contraseñas, cuentas de correo)	Utilizar una conexión por VPN al momento de ingresar a la cámara IP

R4	Manipulación indebida de las credenciales de acceso de la cámara por parte de un delincuente	Seguir al pie de la letra los controles de seguridad adecuados recomendados por el fabricante que garanticen la seguridad en él envió de información de la cámara.
R5	Mantener las contraseñas por defecto de la cámara IP la exponen a un ataque por Denegación distribuida del servicio de páginas de terceros a través del uso de cámaras IOT como parte de una Botnet, donde el criminal usa la cámara como vector de ataque para cometer delitos que afectan páginas de terceros impidiendo que realicen su actividad comercial, eso impide que generen ingresos.	En el momento de instalación de la cámara IP cambiar las credenciales y para ingresar al sitio web de la cámara las credenciales deben ser diferentes.
R6	Mantener las contraseñas por defecto de la cámara IP la exponen a un ataque por Denegación distribuida del servicio de páginas de terceros a través del uso de cámaras IOT como parte de una Botnet, donde el criminal usa la cámara como vector de ataque para cometer delitos, incriminando al (los) dueño(s) de la cámara lo cual puede generar problemas legales.	
R7	Mantener las contraseñas por defecto de la cámara IP la exponen a un ataque por Denegación distribuida del servicio de páginas de terceros a través del uso de cámaras IOT como parte de una Botnet, donde el criminal usa la cámara como vector de ataque para cometer delitos, incriminando al (los) dueño(s) de la cámara lo cual puede generar posibles pérdidas económicas por la exigencia de indemnizaciones por parte de los terceros propietarios de los sitios afectado.	
R8	La falta de conciencia acerca de la seguridad, expone al dispositivo a Ciberataques donde se arriesga a la sustracción o pérdida de la información resguardada en la cámara.	La formación y concienciación es la principal medida de seguridad que se puede llevar a cabo para prevenir ciberataques. Leer el manual de uso de la cámara IP antes de instalarla y seguir paso a paso las instrucciones ; el usuario también debe leer los manuales que se encuentran en las páginas web de los fabricantes.
R9	Exposición del dispositivo a ataques de fuerza bruta y diccionario permitiendo que un atacante descifre las claves de acceso para después realizar exigencias de naturaleza extorsiva con el fin de no revelar la información robada.	Eliminar el usuario por defecto existente y crear uno nuevo con credenciales robustas. En el nombre de usuario no utilizar los que vienen por defecto como “admin”, “administrador”, “root”, etc, tampoco nombres fácilmente adivinables como el propio o de algún miembro que viva

		en la casa/apartamento. Para la contraseña se recomienda que sea robusta, utilizando mayúsculas, minúsculas, números y símbolos , con una longitud mínimo de 8 caracteres teniendo en cuenta que cuantos más caracteres tenga y variados la contraseña se hace más robusta
R10	La falta de cifrado en datos enviados a través de la red (contraseñas e imágenes de la grabación en tiempo real) expone al dispositivo a ataques de Sniffing ocasionando que un atacante pueda tener conocimiento de información susceptible para el usuario generando afectaciones económicas por el robo de la información del usuario con fines extorsivos	Utilizar una conexión por VPN a la cámara al momento de ingresar a la transmisión de video en tiempo real
R11	Inyección de código. Permite que un atacante pueda realizar la carga de archivos que intenta modificar ficheros y valores de la estructura funcional del dispositivo para llevar a cabo ataques y comprometer la seguridad y privacidad de los usuarios. Esto ocasiona posible pérdida económica por exigencias de naturaleza extorsiva de los criminales para no revelar información intima de las personas	No entrar a enlaces o descargas que envíen por correo electrónico o por mensaje de texto, que no provienen del fabricante. No se deben instalar actualizaciones de seguridad que provengan de otro sitio que no sea el oficial
R12	Manipulación con Software de la cámara permite que la información y configuración de la cámara IP queden expuestos a terceros.	No descargar Software que no está autorizado por el fabricante
R13	No verificar la autenticidad del sitio web al que se accede para ingresar a las funciones de la cámara , la expone a un ataque de Phishing permitiendo la captura por parte de terceros de la información sensible del usuario (cuentas de correo, contraseñas, ubicación del dispositivo)	Ingresar al sitio web de la cámara IP únicamente con la URL indicada por el fabricante.
R14	Si las credenciales establecidas no son robustas, un criminal puede hacer uso no autorizado de la cámara y manipular las configuraciones del dispositivo hasta el punto de dejarla obsoleta	Al instalar la cámara IP establecer credenciales robustas. En el nombre de usuario no utilizar los que vienen por defecto como “admin”, “administrador”, “root”, etc, tampoco nombres fácilmente adivinables como el propio o de algún miembro que viva en la casa/apartamento. Para la contraseña se recomienda que sea robusta, utilizando mayúsculas, minúsculas, números y símbolos , con una longitud mínimo de 8 caracteres teniendo en cuenta que cuantos más caracteres tenga y variados la contraseña se hace más robusta

R15	Atacantes remotos pueden obtener acceso administrativo que les permite conocer la información ingresada requerida para la configuración inicial (cuentas de correo, ubicación del dispositivo, números de contacto, contraseñas), así como poder acceder a la transmisión en tiempo real.	Si en la configuración de la cámara IP, tiene la opción de autenticación de dos factores, activarla**.** No entrar a enlaces o descargas que envíen por correo electrónico o por mensaje de texto.
R16	La falta de mantenimiento preventivo compromete la disponibilidad de las grabaciones e incluso general una pérdida parcial o total de las mismas	Verificar que la cámara esté ajustada y posicionada de forma correcta. Verificar que el lente de enfoque y el iris automático estén ajustados correctamente. Limpiar el exterior de la cámara, verificando que estén libres de polvo por dentro y por fuera. Verificar que la cámara esté funcionando correctamente con el controlador o software.
R17	No actualizar el Firmware de la cámara IP puede provocar ingreso de virus informáticos que dañan y afectan las funciones de la misma	Aplicar las últimas actualizaciones y parches de seguridad será una prioridad y se contará con las últimas funcionalidades implementadas por el fabricante. La actualización del firmware debe hacerse de manera manual, entrando en la web oficial del fabricante, descargando el firmware para el modelo exacto de la cámara IP, y posteriormente, acceder al firmware de la cámara para cargar el nuevo firmware. Cuando se tenga que descargar la actualización de seguridad de forma manual siempre se debe hacer desde el sitio web oficial del fabricante, nunca se deben instalar actualizaciones de seguridad que provengan de otro sitio que no sea el oficial
R18	Las cámaras IP pueden presentar vulnerabilidades propias de fabricantes facilitando a criminales acceder a ellas.	
R19	Por medio de una vulnerabilidad propia del fabricante un atacante puede llegar a tener información valiosa propia de la cámara (modelo, producto, marca, versión, compilación, nombre del dispositivo, ubicación, dirección MAC, dirección IP, dirección IP de la puerta de enlace, estado inalámbrico).	Aplicar las últimas actualizaciones y parches de seguridad establecidas por el fabricante
R20	Por medio de una vulnerabilidad propi a del fabricante un atacante malintencionado puede obtener acceso no autorizado a archivos CGI y puede modificar información esencial para el funcionamiento de la	Aplicar las últimas actualizaciones y parches de seguridad establecidas por el fabricante y en el momento de instalación de la cámara IP cambiar las credenciales que vienen por

	cámara.	defecto.
R21	Algunas cámaras IP tienen funciones donde conectan automáticamente dispositivos del mismo fabricante	No usar estas funciones si no es necesario. En caso de usarla, no establecer las mismas credenciales para todos los dispositivos.
R22	Perdida de las grabaciones almacenadas en la tarjeta SD debido al hurto de la cámara IP	Realizar copias de seguridad de las grabaciones almacenadas en la tarjeta SD de la cámara.
R23	Afectaciones económicas al requerir la compra de una nueva cámara debido al hurto de la misma	Realizar la compra de un seguro que permita la reposición del dispositivo sin generar mayores gastos al usuario
R24	Afectaciones económicas por el robo de las grabaciones de la cámara con fines extorsivos	Mantener el dispositivo con una cubierta protectora**.** Revisar los puertos que tenga y si son de fácil acceso, en caso de que si se debe protege el acceso a esos puertos. Si los puertos no son necesarios y la configuración de la cámara lo permite, deshabilitarlos.
R25	Una conexión deficiente de la cámara IP con la red WIFI puede comprometer la disponibilidad sobre las grabaciones del dispositivo en un tiempo específico, generando una pérdida parcial de las grabaciones.	Contratar un servicio de internet que se ajuste a las necesidades del usuario y permita tener una calidad adecuada del servicio
R26	La conexión deficiente de la cámara IP con la red WIFI dificulta el ingreso a ver la transmisión en tiempo real de la cámara IP	
R27	La conexión deficiente de la cámara IP con la red WIFI dificulta el ingreso a la configuración de la cámara IP impidiendo realizar cambios deseados en las funciones de la cámara en un momento específico.	
R28	Las conexiones de red sin protección exponen a la cámara IP a un ataque de "Man in the Middle", interceptando información transmitida en la red (direcciones IP, credenciales, imágenes en tiempo real, cuentas de correo). Con esta información los criminales pueden hacer exigencias extorsivas económicas para no revelar información intima de las personas.	Siempre que sea necesaria la comunicación con el dispositivo vía Internet, existe la opción de utilizar una red VPN. La implementación de esta red ofrece comunicaciones seguras con la cámara IP desde cualquier tipo de conexión, incluidas redes WIFI públicas
R29	Un intruso puede destruir la cámara IP por instalarla en una ubicación vulnerable acarreando perdidas económicas para el usuario.	Verificar previamente la mejor ubicación para instalar la cámara quedando fuera del alcance de cualquier persona.
R30	Las fallas en el servicio de energía pueden generar una avería de la cámara si se presentan variaciones de voltaje que no cumplan con lo establecido por el fabricante y también una perdida en la grabación en el tiempo donde no hay continuidad en el servicio.	Verificar previamente las recomendaciones del fabricante sobre el voltaje adecuado y la tolerancia permitida al presentar variaciones

R31	Perdida de las grabaciones de forma temporal o total por daños en la cámara ocasionados por fuego, agua o polvo. Estos elementos también pueden dañar las funciones de la cámara dejándola obsoleta.	Realizar mantenimientos de limpieza periódicos con el fin de detectar a tiempo alguna afectación que pueda provocar el daño de la cámara.

Tabla 13. Tabla de la Guía, Riesgos y Recomendaciones. Fuente propia.

8. NUEVAS AREAS DE ESTUDIO

Como continuación de este trabajo de investigación existen diversas líneas de indagación que quedan abiertas y en las que es posible continuar trabajando. Estas son el resultado de temas que han ido surgiendo durante la realización de la investigación, estas líneas pueden servir para retomarlas posteriormente como opción a trabajos futuros para otros investigadores. A continuación, se presentan algunos trabajos futuros que pueden desarrollarse como resultado de esta investigación o que, por exceder el alcance de esta tesis, no han podido ser tratados con la suficiente claridad:

- Realizar el estudio de seguridad informática en otro tipo de dispositivos IOT utilizados para la vigilancia de hogares y empresas.
- Indagar sobre los controles de seguridad y riesgos presentes en dispositivos IOT utilizados con frecuencia en los hogares como lo son neveras, lavadoras, barredoras entre otros.
- Investigar sobre las responsabilidades de las casas matrices de los dispositivos IOT frente a las vulnerabilidades presentadas en sus productos.

9. CONCLUSIONES

La información recopilada en la fase 1 permitió dar inicio al desarrollo de los objetivos específicos, en la fase 2 se logró focalizar la información para el análisis de los riesgos y así dar cumplimiento con los entregables. Acorde a esto se describen a continuación las colusiones al terminar el proyecto:

Los delitos informáticos están creciendo de forma desmesurada, en cualquier lugar donde estemos conectados estamos expuestos a ser atacados por Ciberdelicuentes, buscando un fin económico. Debido al auge de IOT, cada vez más dispositivos se conectan a la red, pero muchos de ellos no cuentan con medidas esenciales de seguridad, evidenciando una serie de vulnerabilidades relacionadas con los controles de acceso y el cifrado de la información, lo que conlleva a una serie de ataques relacionados con denegación de servicios o accesos no autorizados

En la actualidad se está prestando más atención a las cosas o dispositivos inteligentes IOT, y lo que pueden hacer, como parte de los nuevos servicios, aplicaciones y modelos comerciales que están implementado los fabricantes. Esta tecnología se encuentra en una etapa de evolución y su alcance comienza a ampliarse permitiendo más posibilidades de mejorar la calidad de vida de los usuarios, en las viviendas, cuidado del medio ambiente, entre otros.

Se deben tener aplicados los controles mínimos de seguridad recomendados por los fabricantes para el acceso a nuestros dispositivos IOT, para lograr la reducción del riesgo de materialización de ataques. La importancia de la información debe empezar desde los hogares, tomando conciencia sobre la protección de los datos personales expuestos en los dispositivos IOT, debido a que hay muchos datos que se registran de forma inconsciente, o que obligatoriamente se ingresan para poder acceder a un servicio en línea.

Con base en la información recopilada de las 4 cámaras IP que hacen parte de la investigación, se pudieron evidenciar vulnerabilidades frecuentes, relacionadas con la autenticación con contraseñas por defecto que las cámaras traen de fábrica, debilidad en la complejidad de las contraseñas, fallas en los controles de acceso a la interfaz de visualización de vídeo en tiempo real, inyección de código y desactualización de firmware para corregir vulnerabilidades. Por tal motivo se estableció una guía con recomendaciones mínimas que se deben tener en cuenta al momento de implementar este tipo de sistema de vigilancia para el hogar.

Por lo anteriormente expuesto se diseñó una guía sobre los riesgos a los cuales se exponen las cámaras de seguridad IP en el sector hogar y se realizaron las recomendaciones mínimas para prevenir dichos riesgos. Lo más importante de diseñar esta guía fue evidenciar como están expuestos los usuarios que usan la tecnología IOT, ya que en la actualidad existen demasiadas herramientas capaces

de realizar muchas tareas que en un momento se creían impensables, pero que acarrean miles de problemas relacionados con el robo de información, accesos no autorizados, entre otros.

10. BIBLIOGRAFÍA

Wikipedia, “Internet de las cosas”. Internet: https://es.wikipedia.org/wiki/Internet_de_las_cosas

Gartner, “Gartner Identifies Top 10 Strategic IoT Technologies and Trends”. Internet: https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends

CASTRO, Miguel, “Internet de las cosas, privacidad y seguridad. Trabajo de grado”. Internet: https://sinbad2.ujaen.es/sites/default/files/publications/Memoria_0.pdf

E-Security Proteccion y Tecnologia. Internet: https://www.es.company/

INCIBE, “Protege tu empresa – Blog - Medidas de prevención contra ataques de denegación de servicio”. Internet: https://www.incibe.es/protege-tu-empresa/blog/medidas-prevencion-ataques-denegacion-servicio

Flores, J., Guarda, T., & Molina, L. (2019). Seguridad Informática en el Uso de los Nuevos Equipos Tecnológicos. Revista Ibérica de Sistemas e Tecnologías de Información, (E17), 32-38.

Redes y Telecom, “Una cámara de seguridad conectada a la IOT también es vulnerable”. Internet: https://www.redestelecom.es/seguridad/noticias/1111355002503/camara-de-seguridad-conectada-iot-tambien-vulnerable.1.html

TREND Micro, “Internet of Things - IoT Attack Opportunities Seen in the Cybercrime Underground”. Internet: https://www.trendmicro.com/en_in/research/19/i/iot-attack-opportunities-seen-in-the-cybercrime-underground.html

MDP, “The Security of IP-Based Video Surveillance Systems”. Intenert: https://www.mdpi.com/1424-8220/20/17/4806/pdf.

OVANCE, “Las cámaras de seguridad y vigilancia en el hogar”. Internet: https://ovacen.com/camaras-de-seguridad/

ESCOBAR CORREDOR, Gina Julieth y HERNANDEZ VELASQUEZ, Laura Paola, “Seguridad de la Información en Dispositivos Smartwatch”. Internet: https://repository.ucatolica.edu.co/bitstream/10983/24872/3/resumen-analitico-en-educacion.pdf

INCIBE, “Seguridad en la instalación y uso de dispositivos IOT”. Internet: https://www.incibe.es/protege-tu-empresa/blog/medidas-prevencion-ataques-denegacion-servicio

BBC NOTICIAS, “¿Cómo un único ciberataque pudo dañar a varios sitios populares como Twitter, Spotify y Netflix al mismo tiempo?”. Internet: https://www.bbc.com/mundo/noticias-37735459

IOT Analytics, “THE 10 MOST POPULAR INTERNET OF THINGS APPLICATIONS RIGHT NOW”. Internet: https://iot-analytics.com/10-internet-of-things-applications/

Shodan, “The search engine for...”.Internet: https://www.shodan.io/

ITproportal, “Vulnerabilities in smart IP cameras expose users to privacy, security risks”. Internet: https://www.itproportal.com/features/vulnerabilities-in-smart-ip-cameras-expose-users-to-privacy-security-risks/

11. REFERENCIAS

Arias Silva, N. A. (04 de Octubre de 2019). *UNAD.* Obtenido de Análisis de seguridad de vulnerabilidades y ataques presentados en 4 dispositivos de Internet de las cosas: https://repository.unad.edu.co/handle/10596/33326

Bloomberg. (10 de Marzo de 2021). *EL TIEMPO.* Obtenido de Hackeo de cámaras de seguridad expuso a Tesla y a otras empresas: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/hackeo-de-camaras-de-seguridad-expuso-a-tesla-y-a-otras-empresas-572336

Felipe Clavijo Ramírez, D. O. (2017). *Banrep.* Obtenido de RIESGO CIBERNÉTICO: RELEVANCIA Y ENFOQUES PARA SU REGULACIÓN Y SUPERVISIÓN: https://www.banrep.gov.co/sites/default/files/publicaciones/archivos/rref_recuadro_7_2017.pdf

Hernandez, I. (26 de Febrero de 2020). *RCN RADIO .* Recuperado el 10 de Noviembre de 2020, de https://www.rcnradio.com/tecnologia/nace-primer-laboratorio-de-internet-de-las-cosas-en-colombia

Mata, F. J. (2010). *Videovigilancia: CCTV usando vídeos IP.* Malaga, España : VERTICE .

MOLINA, I. C. (2019). *Repositorio UNAD.* Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/28446/Monografia.pdf?sequence=1&isAllowed=y

NOTICIAS, T. |. (12 de Mayo de 2020). *Networkworld.* Obtenido de https://www.networkworld.es/telecomunicaciones/internet-de-las-cosas-en-2020-mas-vital-que-nunca

Patrocinado. (19 de Mayo de 2019). *EL TIEMPO.* Recuperado el 10 de Noviembre de 2020, de https://www.eltiempo.com/contenido-comercial/el-internet-de-las-cosas-tambien-es-seguridad-en-el-hogar-364758

Santos, P. R. (22 de Septiembre de 2020). *TELEFONICA.* Obtenido de Breve historia de Internet de las cosas (IoT): https://empresas.blogthinkbig.com/breve-historia-de-internet-de-las-cosas-iot/

security, K. f. (13 de 12 de 2018). *Koorsen fire y security.* Obtenido de TOP 10 WAYS TO MINIMIZE VULNERABILITIES IN IP SECURITY CAMERA SYSTEMS: https://blog.koorsen.com/10-ways-to-minimize-vulnerabilities-in-your-ip-security-camera-surveillance-system

SW Tho, Y. Y. (Marzo de 2015). *School Science Review.* Recuperado el 23 de Febrero de 2021, de https://www.researchgate.net/profile/Yau-yuen_Yeung/publication/294882199_Innovative_IP_camera_applications_for_scientific_investigation/links/59ef0f43a6fdcc0d0072744c/Innovative-IP-camera-applications-for-scientific-investigation.pdf

Tecno Seguro . (14 de Enero de 2021). Recuperado el 22 de Febrero de 2021, de https://www.tecnoseguro.com/noticias/cctv/video-porteros-ip-hikvision-seguridad-hogares

TURTON, B. /. (09 de Marzo de 2021). *EL FINANCIERO EN ALIANZA CON BLOOMBERG.* Obtenido de https://www.elfinanciero.com.mx/tech/hackers-

exponen-a-tesla-carceles-y-hospitales-tras-infiltrarse-en-150-000-camaras-de-seguridad

Wikipedia. (s.f.). Obtenido de Segurida Informatica : https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica#cite_note-:0-1

Yogeesh Seralathan, S. J. (26 de Marzo de 2018). *IEEE.* Recuperado el 23 de Febrero de 2021, de https://ieeexplore.ieee.org/abstract/document/8323686