CENTRO DE POSGRADOS

Tema:

MODELO DE GESTIÓN DE SEGURIDAD EN EL CICLO DE VIDA DE LOS DISPOSITIVOS IOT

Proyecto de investigación previo a la obtención del título de Magíster en Ciberseguridad

Línea de investigación:

PROTECCIÓN DE DATOS Y COMUNICACIONES

Autor:

Roberto Carlos Murillo Unda

Director:

Mg. José Marcelo Balseca Manzano

Ambato – Ecuador

Junio 2025

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **ROBERTO CARLOS MURILLO UNDA,** con cédula de ciudadanía **0503404386**, autor del trabajo de graduación intitulado: “MODELO DE GESTIÓN DE SEGURIDAD EN EL CICLO DE VIDA DE LOS DISPOSITIVOS IOT”, previo a la obtención del título profesional de **MAGÍSTER EN CIBERSEGURIDAD**, en el centro de **POSGRADOS**.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos del autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, junio 2025

Firmado electrónicamente por:
ROBERTO CARLOS MURILLO UNDA
Validar únicamente con FirmaEC

Roberto Carlos Murillo Unda
CC. 0503404386

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

APROBACIÓN DEL TRIBUNAL DE GRADO

Tema:

MODELO DE GESTIÓN DE SEGURIDAD EN EL CICLO DE VIDA DE LOS DISPOSITIVOS IOT

Línea de investigación:

PROTECCIÓN DE DATOS Y COMUNICACIONES

Autor:

Roberto Carlos Murillo Unda

José Marcelo Balseca Manzano, Ing. Mg. f._____

Firmado electrónicamente por: JOSE MARCELO BALSECA MANZANO. Validar únicamente con FirmaEC

CC. 1802572915

CALIFICADOR

Liliana del Rocío Mena Hernández, Ing. Mg. f._____

Firmado electrónicamente por: LILIANA DEL ROCIO MENA HERNANDEZ. Validar únicamente con FirmaEC

CALIFICADOR

Darío Javier Robayo Jácome, Ing. Mg. f._____

Firmado electrónicamente por: DARIO JAVIER ROBAYO JACOME. Validar únicamente con FirmaEC

CALIFICADOR

Dayamy Lima Rojas, Lic. Mg. f._____

DAYAMY LIMA ROJAS. Firmado digitalmente por DAYAMY LIMA ROJAS. Fecha: 2025.06.26 11:22:12 -05'00'

DIRECTORA CENTRO DE POSGRADOS

Diego Gonzalo Coca Chanalata, Dr. f._____

DIEGO GONZALO COCA CHANALATA. Firmado digitalmente por DIEGO GONZALO COCA CHANALATA. Fecha: 2025.06.26 12:02:57 -05'00'

SECRETARIO GENERAL PUCESA

Ambato – Ecuador

Junio 2025

DEDICATORIA

Con muestra de mi respeto, amor y cariño profundo, dedico la presente investigación a mi familia por acompañarme a lo lardo de mi proceso educativo, gracias a su apoyo constante durante mi vida profesional, a mi madre con todo el amor del mundo por siempre levantarme y nunca desampararme sin sus concejos no estaría en lugar que me encuentro, su apoyo incondicional durante su vida, para lograr cada uno de mis objetivos profesionales.

Para mi Anita mi amada esposa mediante su compañía y apoyo constante en nuestra nueva etapa, la cual es parte de mis logros, alegrías y tristezas, fuente de inspiración y lucha constante durante su vida, gracias por tu amor, paciencia y comprensión que me brinda cada día de su vida.

AGRADECIMIENTO

Agradezco a Dios por acompañarme y no desampararme durante toda mi vida, a mi querida familia por formar parte de este largo proceso de enseñanza profesional como personal.

Gracias al apoyo de mi tutor Mg. José Balseca por el conocimiento brindado, durante el proceso de titulación, eternamente agradecido

RESUMEN

La constante innovación tecnológica en dispositivos IoT presente en sectores domiciliarios y empresas ha permitido enfrentarse a retos tecnológicos debido a ser expuestos a una serie de vulnerabilidades exponiendo información relevante como datos personales, el auge en equipos, dispositivos conectados a internet y su despliegue masivo hace necesario contemplar medidas de seguridad sobre todo en aquellos dispositivos de gama baja que se encuentran conectados a internet o redes domiciliarias que normalmente no cuentan con la seguridad necesaria al momento de enviar, recopilar y procesar la información.

La gestión de seguridad en dispositivos IoT presentan su propio ciclo de vida que mantienen sus identidades desde su fabricación hasta su eliminación lo cual es el elemento más vulnerable antes de su desecho, dicho ambiente genera el espacio necesario para ataques cibernéticos, por esta razón el presente proyecto de desarrollo tiene como objetivo desarrollar un modelo de gestión de seguridad en el ciclo de vida de los dispositivos IoT.

El proyecto de desarrollo se basa en revisión bibliográfica de carácter descriptivo, no experimental, aplicando la metodología PRISMA, capaz de determinar un conjunto de procedimientos y medidas de prevención ante vulnerabilidades presente en cada una de las fases del ciclo de vida en dispositivos IoT, con la finalidad que se compile lógica y cronológicamente en un modelo de gestión de seguridad.

Palabras clave: modelo de gestión de seguridad, ciclo de vida, dispositivos IoT.

ABSTRACT

The continuous technological innovation in IoT devices present in both residential sectors and businesses has posed technological challenges due to their exposure to various vulnerabilities, which risk compromising sensitive information such as personal data. The rapid growth in the number of internet-connected devices and their widespread deployment necessitates the implementation of security measures, especially for low - end devices connected to the internet or home networks that often lack adequate security when transmitting, collecting, and processing information.

Security management in IoT devices involves a unique lifecycle that maintains device identities from manufacturing through to disposal, with the disposal phase representing the most vulnerable point before decommissioning. This environment creates opportunities for cyberattacks. Therefore, this development project aims to design a security management model for the lifecycle of IoT devices.

The project is based on a descriptive, non-experimental bibliographic review using the PRISMA methodology, which enables the identification of a set of procedures and preventive measures against vulnerabilities present at each phase of the IoT device lifecycle. The ultimate goal is to compile these logically and chronologically into a comprehensive security management model.

***Keywords**: security management model, lifecycle, IoT devices.*

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

INTRODUCCIÓN

La proliferación de dispositivos IoT y el auge de tener acceso a la información del producto desde el 2003 (Burhan et al., 2018a), son el producto de la fusión entre tecnología de la información y la tecnología operativa (Boeckl et al., 2021), por ello ha revolucionado el mundo digital desde los dispositivos domiciliarios hasta entornos industriales, lo cual abarca un amplio campo en la sociedad que están conectados a internet permitiendo su fácil implementación, lo que conlleva el aumento de vulnerabilidades que sé debe tomar en cuenta para la protección y detección ante ataques que puedan obtener datos privados de las empresas o los usuarios finales.

La importancia de recopilar datos de las fases del ciclo de vida en dispositivos conlleva una serie de desafíos durante su vida útil debido a la posibilidad de ser vulnerado en cada una de sus etapas, un estudio realizado por (Yousefnezhad et al., 2023a) basa su diseño en una arquitectura IoT para estándares de interfaz y formato de datos abiertos, que permite a controlar el acceso sin autenticación, restringir los datos o permisos de los usuarios (Yousefnezhad et al., 2023a)**,** como una solución a la seguridad tanto del usuario final al igual que en los equipos a emplear.

El crecimiento global de los dispositivos IoT ha planteado desafíos en términos de seguridad con el objeto de interactuar con cualquier otro dispositivo desde un teléfono móvil hasta ciudades completamente conectadas a la red, la evolución constante de la tecnología en los últimos años conlleva a sistemas de seguridad altamente vulnerables, por lo cual la implementación de políticas de control, modelos de gestión de seguridad es de vital importancia para proteger la información y satisfacer estándares de desempeño como el rendimiento, confiabilidad, resiliencia y seguridad(Boeckl et al., 2021), a lo largo de la vida útil de los equipos.

La relevancia de llevar a cabo una correcta administración de riesgos en dispositivos IoT, conlleva a que muchos elementos que se encuentran conectados

a la red permitan la recolección de información de datos importantes que en su mayoría en el área que se ejecuta es crítica para el entorno en que labora, lo cual resulta relevante la adopción de medidas de seguridad contra accesos no autorizados y protección de seguridad de los dispositivos durante las fases del ciclo de vida desde su fabricación, elaboración producción hasta su desecho.

Una de las conferencias relevantes de seguridad de la DEFCON en 2016 determinó alrededor de 47 afectaciones afectando a 23 equipos IoT de 21 distintos fabricantes, con un numero representativo de brechas de inseguridad en software, errores en la elaboración, contraseñas ineficientes, configuraciones falibles, protocolos de cifrado inseguro, entre otros.(Subramanian et al., 2017)

Ejemplos de incidencias de seguridad en dispositivos IOT incluye:

- En 2016, botnet Mirai aparece en el 2016 siendo un motor de ataque de denegación de servicios más relevante en la historia que ocurre regularmente por el puerto 23 , capaz de eliminar sitios web tales como Netflix o Twitter durante horas, dicho botnet se centra principalmente en infectar dispositivos con seguridad débil.(Kolias et al., 2017)
- En 2017, botnet Persirai basado en IoT, lleva a acceder a puertos abiertos para inyectar un comando que permite la instalación de un malware que se descarga, ejecuta y se elimina propiamente para evitar la detección, más de 1000 modelos de cámaras IP de diferentes fabricantes fueron utilizadas para llevar ataques de denegación de servicios sin consentimiento(Yeh et al., 2017)

De los botnets anteriores, mediante un análisis realizado en 2019 destaca que las vulnerabilidades en cámaras de seguridad, Alexa y Google Home conectados a redes domesticas equivalen al 47% de los dispositivos con mayor facilidad de robo de información debido a medidas de seguridad débiles, donde los principales países que ejecutan este tipo de ataques provienen de China y EE.UU (SAM, 2019), los ataques cibernéticos en Europa proviene del malware a través de correos

electrónicos, ingeniería social o phishing, mientras que en Estados Unidos ataques como *ramsonware* son más frecuentes (SAM, 2019)**.**

En América Latina, la adquisición de tecnología IoT de empresas o personas naturales adquiere mayor fuerza en su implementación y conlleva a tener dispositivos conectados a la red que permitan la facilidad para optimizar procesos, en Colombia el 56.3% de personas no conoce las ventajas de usar IoT, mientras que un 78.5% considera importante implementarlo en empresas(Molina, 2019).

De acuerdo a Telefónica Movistar existe alrededor de 700 nodos que permiten la conexión de 600 mil dispositivos con un 50% del país conectados a la red IoT (Molina, 2019),no obstante la conexión a internet sufre falencias en la prevención de vulnerabilidades, cifras estimadas del departamento de investigación de la Policía Nacional en Enero a Octubre del año 2022, se registra alrededor de 54.121 ataques cibernéticos entre los que destaca ataques en áreas de salud y comunicaciones. En Hispanoamérica, mediante un análisis existirá en 2023 alrededor de 996 millones de dispositivos y para el 2025 se prevé 1200 millones conectados a la red, donde el 64% será destinado para hogares inteligentes.(IoT en América Latina, s. f.)

En Ecuador un estudio realizado, determina que las vulnerabilidades en dispositivos IoT se presenta en las direcciones IPv4, hallando entre los dispositivos mayormente afectados como camaras de seguridad, acceso a routers, paginas web, entre otras, mediante puertos abiertos de comunicacion como http y https que son puertos para sitios web, donde se puede determinar accesos no autorizados a la informacion, siendo Quito y Guayaquil dos de las ciudades con 1137 y 879 direcciones ipv4 sin medidas de seguridad, tomando en cuenta que Ecuador se encuentra en uno de los paises con deficiencia en seguridad informatica en nivel bajo y no cuenta con un analisis sobre la fases presentes en el ciclo de vida de los equipos. (Jumbo et al., 2023)

El propósito del proyecto de desarrollo tiene como finalidad determinar procedimientos y medidas de prevención y vulnerabilidades presentes en el ciclo

de vida de los dispositivos IoT en un modelo para la administración de seguridad viable que permita gestionar y controlar una variedad de ataques cibernéticos que se presenta en cada etapa desde su fase de diseño hasta su eliminación, para el alcanzar el estudio de los objetivos específicos establecidos:

- Fundamentar teóricamente los modelos de gestión de seguridad aplicables al ciclo de vida de dispositivos IoT.
- Diagnosticar las vulnerabilidades presentes en el ciclo de vida de dispositivos IoT.
- Determinar mecanismos de seguridad para cada etapa del ciclo de vida la seguridad en dispositivos IoT.
- Seleccionar mecanismos o procedimientos de seguridad que sean factibles para integrar dentro de un modelo de gestión de ciclo de vida de dispositivos IoT.

La presente investigación es bibliográfica de alcance descriptivo, no experimental, mediante el método PRISMA que busca determinar un conjunto de procedimientos factibles en la administración, protección de los dispositivos IoT y las etapas que adquieren durante el ciclo de vida. El resultado a obtener es un conjunto de procedimientos determinados por la bibliografía, mediante una serie de pasos para identificar medidas de prevención ante vulnerabilidades que determina las fases del ciclo de vida de los dispositivos IoT, los mismos que se compilen lógica y cronológicamente, en un modelo que impulse la administración de seguridad de los equipos.

Analizar las vulnerabilidades presentes en un mundo cambiante va de la mano con la seguridad, es un reto para las empresas que disponen de métodos de protección de datos, países en desarrollo de nuevas tecnologías tienden a olvidar la parte más importante la protección de la información, en la que se busca perseverar la autenticidad de los datos, con medidas de seguridad viables se ha vuelto un reto para los ciber atacantes que encuentran con facilidad acceder a los datos de los usuarios de las redes domiciliares que son altamente vulnerables, donde los niveles de confidencialidad, integridad y disponibilidad se han visto expuestos.

Se ha considerado la situación actual de seguridad en los países en auge de nuevas tecnologías y las falencias que conlleva el uso de dispositivos IoT por la falta de implementación de metodologías, procedimientos, guías de seguridad o simplemente modelos de administración de riesgos con la finalidad de proteger los datos.

Dada la variedad de dispositivos IoT, los dispositivos mayormente vulnerables se presentan cámaras IP en hogares domésticos, con la facilidad del robo de información conectadas a través de la red, por lo que se requiere en lo posible personal técnico con conocimiento en instalación de cámaras que garantice en su mayoría la seguridad de la información, debido a que una persona natural no emplea medidas de seguridad antes de adquirir un cámara de seguridad y no comprenden la importancia de salvaguardar la información de manera adecuada o que conozca los procesos básicos para implementar cámaras, sin comprometer el robo de su propia información.

(Ribero-Corzo & Prieto-Guerrero, 2021), en su investigación determinan que las cámaras IP son propensas a ataques de seguridad al estar expuestos a la red como *gateways* (puertas de enlace), controles de acceso, redes wifi, etc.

El modelo de gestión de seguridad a desarrollar es determinado para personal técnico con conocimientos en cámaras de seguridad, una cantidad excesiva de personas se encuentran dedicadas a la instalación de cámaras de seguridad de diferentes modelos no poseen una visión técnica ya sea por la falta capacitación en el área de seguridad, dispositivos IoT o no obtengan una guía adecuada de instalación de cámaras IP y mucho menos poseen información sobre la facilidad de adquirir brechas de seguridad durante su implementación, el modelo de gestión de seguridad es empleado a diferentes marcas de cámaras IP de diferentes fabricantes, mediante un conjunto de métodos o guías preestablecidas que aseguren y autentifiquen la seguridad en dispositivos durante el ciclo de vida, dado que las de cámaras ip son expuestas a vulnerabilidades.

La presente investigación es viable para determinar aspectos y medidas de seguridad que puedan integrarse dentro de un modelo de administración de protección de datos adquiridos en dispositivos IoT como en modelos de cámaras Ip instaladas en hogares domésticos que son de uso común, donde el personal técnico adquiera conocimiento necesario de todas las fases del ciclo de vida del dispositivo antes y después de su instalación, desde su diseño, implementación, configuración, operación y eliminación (Molina, 2019) por medio de estándares, protocolos de seguridad, medidas de protección, etc, para prevenir vulnerabilidades que han sido detectadas en entornos sin supervisión directa por personal calificado.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

Se detallan las principales relaciones que permita comprender de una manera detallada la importancia del ciclo de vida de los dispositivos IoT en un modelo de gestión de seguridad, con el propósito de mitigar las amenazas presentes durante la vida útil para asegurar la información durante todo el proceso de durabilidad del dispositivo en el medio que este en uso.

1.1. Introducción a la seguridad del ciclo de vida en dispositivos IoT

A principios de los años 70 aparecen las primeras redes conocidas, Robert Kahn y Víctor Cerf inventores del protocolo de comunicación TCP-IP permite la conectividad entre dos equipos en una red, es la base fundamental para el conocido termino en la actualidad el Internet, en el año 1990 el primer objeto conectado a internet es una tostadora que basa su comunicación mediante el protocolo TCP/IP, el encendido y apagado se realiza mientras se encuentre conectada a la web siendo el primer dispositivo IOT. (Recuero, 2021b)

Kevin Ashton introduce el concepto sobre el internet de las cosas en el año 1999(Recuero, 2021a),con la idea basada en enlazar el mundo mediante sensores, un ejemplo de ellos en el Instituto de tecnología Massachusetts por su trabajo en radiofrecuencia (RFID) en red (Evans, 2011) que permitía enlazar las tarjetas de acceso a los procesos sin la necesidad de intervención humana.(Rose et al., 2015)

Básicamente un dispositivo IoT basa su comunicación con otro dispositivo capaz de intercambiar información específica la cual permita transportar, almacenar y procesar los datos adquiridos que son generados por el medio en que se propagan como el internet.

El termino ciclo de vida se introduce en el año 2003 para tener acceso a la información del producto durante su etapa de vida (Kärkkäinen et al., 2003),las empresas normalmente deben adquirir procesos de gestión del ciclo de vida del producto por los constantes cambios en los procesos y fabricación que realizan.

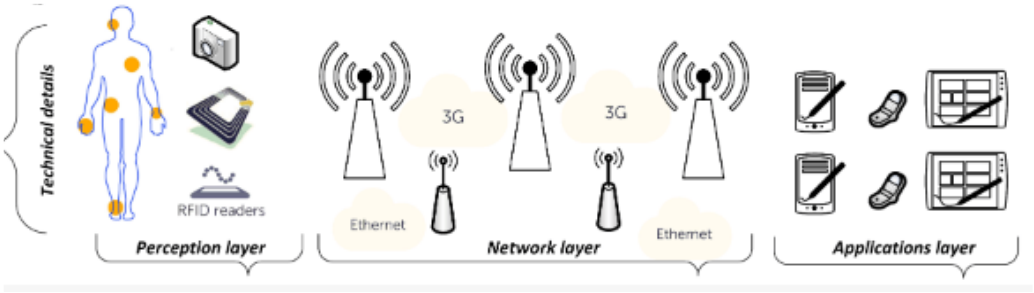
No obstante, debido a la falta de conocimiento o termino empleado del ciclo de vida en dispositivos IoT que se emplean hoy en día es de gran utilidad, debido al uso diario de las personas que utilizan dispositivos inteligentes y la mayor parte recae en la responsabilidad del personal técnico dedicado a la instalación de dispositivos IoT como cámaras de seguridad debido a la falta de información para detectar problemas dentro de los márgenes de fabricación o eliminación durante la vida del equipo en este caso cámaras ip.

El auge de los dispositivos IoT en sectores domiciliarios y la creciente demanda de tecnologías basado en internet de las cosas conlleva la falta de herramientas capaces de determinar vulnerabilidades debido al mantenimiento, rendimiento y aplicaciones futuras que favorezcan a la rentabilidad de implementar dispositivos, tomando en cuenta la falta de seguridad en la implementación de esta tecnología en gran escala (X. Li et al., 2025), sin obtener garantía de la información adquirida por las personas o inclusive de manera general especificar el proceso y desecho de un dispositivo IoT durante su vida útil.

La arquitectura y los protocolos de comunicación es parte esencial para la comprensión del ciclo de vida en cada una de sus etapas, las cuales no han sido estandarizados o diseñados como modelo de referencia para soportar tecnología IoT debido a la variedad de arquitecturas disponibles. Debido a la participación notable de los dispositivos inteligentes basan su tecnología en la estructura(B. Li, 2019), el tipo de arquitectura aplicado a IoT difiere de muchos autores pueden ser de tres hasta siete capas de acuerdo a la funcionalidad de cada uno de ellas.

Se ha identificado entre las principales tres tipos, la de cinco capas la cual cumple con las capacidades de seguridad aplicado hacia la industria 4.0 o IIRA , el modelo de tres capas es más simplificado y abastece el cumplimiento para el desarrollo de dispositivos IoT entendible de manera general para personal técnico y el modelo de cuatro capas siendo el modelo intermedio según UIT-T cumple con los requerimientos de seguridad y gestión (Darwish & Square, 2015)

Ilustración 1. Arquitectura de los sistemas IoT



Fuente: modificada a partir de (Ali & Awad, 2018)

De manera general se puede detallar en la capa de aplicación adquiere valores propios del usuario en sistemas IoT, los datos adquiridos durante la capa red por el medio físico en que se propaga a través del internet donde la presente capa es vulnerable a ataques de conectividad(Burhan et al., 2018b), y la capa de percepción o física que detecta objetos como sensores o actuadores para obtener información en esta etapa se colocan los dispositivos IoT.

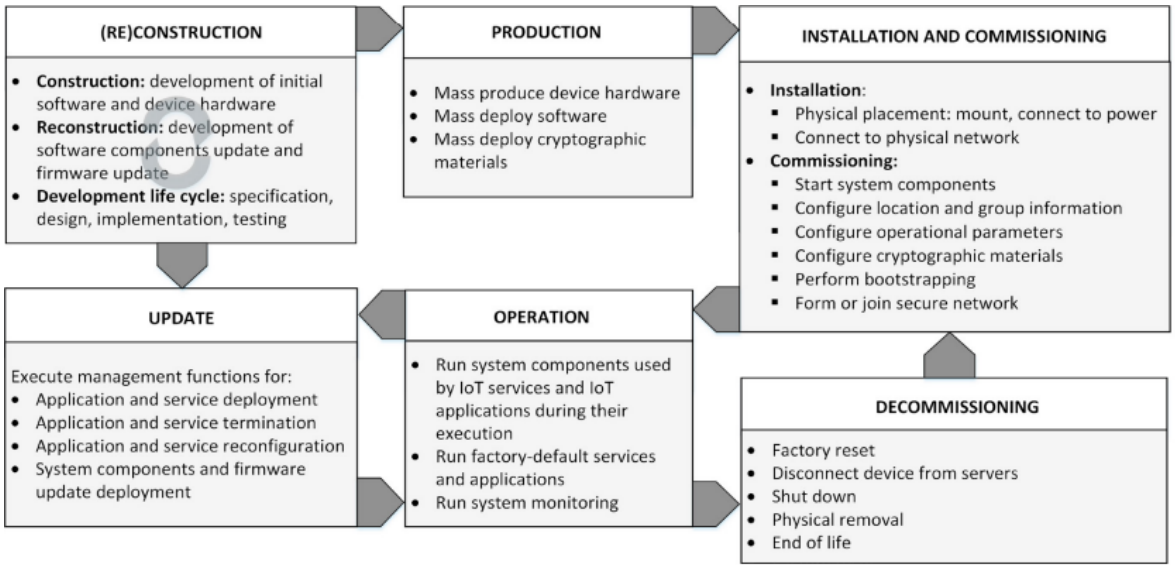
La arquitectura es parte determinante para conocer o analizar el termino ciclo de vida, deben cumplir requerimientos fundamentales como disponibilidad, integridad y confidencialidad del sistema y seguridad, el modelo de 3 capas es adquirido por la simplicidad y en lo posible garantice la gestión de seguridad orientada a servicios IoT e implica que las fábricas entreguen productos que cumplan con los requisitos de calidad debido a los desafíos de seguridad constantemente presentes.

El termino ciclo de vida en dispositivos IoT se puede interpretar como una serie de acciones que involucran netamente al dispositivo en si , por lo tanto se puede hallar diferentes áreas que incluyan el término ciclo de vida(Späthe, 2021), sin embargo algunas de ellas no tienen relación con el termino IoT como el ciclo de vida en desarrollo, proyecto, datos, industrial, comercial e inclusive en el ámbito empresarial(Soós et al., 2018)

El ciclo de vida de los dispositivos se pueden describir una serie de etapas desde su fabricación hasta su desecho, la etapa de instalación del dispositivo se prepara para funcionar en el entorno que será aplicado para su comunicación dentro de la red , en la ilustración 2 determina las actividades que conllevan en cada una debido

a requerir los parámetros necesarios para que el dispositivo funcione adecuadamente (Rahman et al., 2018)

Ilustración 2. Ciclo de vida para dispositivos IoT



Fuente: tomado a partir de (Rahman et al., 2018)

Los desafíos de seguridad ocurren en mayor parte en hogares inteligentes, cámaras de seguridad, asistencia sanitaria, dispositivos inteligentes, vehículos conectados a la red con el fin de mostrar los problemas de seguridad IoT (Karale, 2021), sin obtener información de cuál es el proceso que mantiene un dispositivo durante toda su vida útil.

Podemos incluir los hogares inteligentes y el uso de dispositivos Iot común en las viviendas son cámaras de seguridad conectadas a través de la red las cuales adquieren audio y video por medio de aplicaciones instaladas desde un Smartphone hasta un computador adquiriendo la facilidad de monitorear y visualizar de manera remota o local, sin tomar en cuenta que el dispositivo en la mayor parte de su tiempo este encendido y pueden llevar falencias de seguridad violando la privacidad de la información.

Un ejemplo básico que se puede incluir en las fases del ciclo de vida es basado en software mantiene seis procesos durante las fases que conlleva el ciclo de vida; análisis, diseño, implementación, prueba, actualización y mantenimiento(Carmona

& Antonio, 2019). Mediante el ciclo de vida se puede adquirir conocimiento de las acciones determinadas en detectar problemas de seguridad y vulnerabilidades existentes.

El presente documento basa su análisis en el sector domiciliario en cámaras ip que son instaladas en las viviendas, con el propósito de abastecer la información necesaria capaz de cubrir el robo de la integridad de la información de los dispositivos inteligentes y las brechas de seguridad que poseen los dispositivos durante su ciclo de vida que en el mayor de los casos está al alcance de las personas.

1.2. Modelos de gestión de seguridad en el ciclo de vida IoT

Para analizar el modelo gestión del ciclo de vida de los dispositivos IoT, debemos basarnos en primera instancia la relación con los productos en forma general, permite administrar de mejor manera cada una de las fases desde la elaboración hasta el desmantelamiento de los dispositivos.

Levitt una persona relevante en marketing empleo el termino desde su aparición en el siglo XX en 1965, introdujo el termino modelo del ciclo de vida del producto (Hernando, 2015), que es el tiempo de vida que se encuentra disponible un producto en el mercado , donde el producto debe ser considerado desde la producción antes del despacho del mismo, una consideración importante es que no todos los productos cumplen el mismo ciclo de vida, dependen netamente de la necesidad del usuario o empresa.

Algunos dispositivos IoT poseen un ciclo de vida mucho más largo y pueden durar años, mediante las nuevas tendencias que existen en la actualidad o la innovación permanente y la factibilidad del dispositivo dependerá de la rentabilidad del mismo.

Para el requerimiento del presente modelo del ciclo de vida de dispositivos se embarca en la idea generada por la concepción del producto(Hernando, 2015). El ejemplo más claro aplicado en el sector comercial es el VHS o conocido como

reproductor de video tuvo varias décadas en su ciclo de vida hasta el DVD (en fase de retiro del mercado) por la constante innovación del mismo(Hernando, 2015)

Los diferentes modelos de gestión del ciclo de vida, varía de acuerdo sus requerimientos entre los cuales podemos mencionar en la siguiente tabla 1:

Tabla 1. Servicios y limitaciones de analizar modelos de ciclos de vida

GESTION DEL CICLO DE VIDA	DEFINICIÓN	BENEFICIO	LIMITACIONES
ALM	Ciclo de vida de las aplicaciones	Integral para software productos y aplicaciones	No diseñado para complejos sistemas
ILM	Ciclo de vida de información	Bases del manejo de la información.	No responde cómo desarrollar aplicaciones o sistemas
PLM	Ciclo de vida del producto	Útil para la producción. y seguimiento de productos	El alcance está en el requisito específico del producto. Las características pueden ser diferente para los productos.
SDLC	Ciclo de vida del desarrollo de software	Conjunto bien definido de principios y metodologías para el desarrollo de software	No aplicable en todos los casos, para desarrollos pequeños o evolutivos. Es complicado de usar en entornos que cambian dinámicamente.
SLM	Ciclo de vida del servicio	Útil para la gestión de operaciones de servicio	El alcance se centra en los requisitos específicos del servicio. Las características pueden ser diferentes para los servicios. El objetivo es mejorar el rendimiento funcional

Fuente: modificado a partir de (Kozma et al., 2024)

Para basarnos en un determinado modelo de ciclo de vida de dispositivos IoT nos centramos en PLM o ciclo de vida del producto(Hernando, 2015), como uno de los modelos más completos desde el diseño hasta el desecho, el termino referencial PLM aparece a partir de los años 60. Obtener la información necesaria del producto

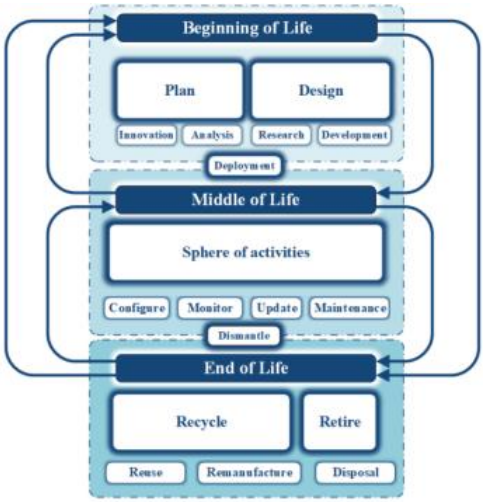
durante el ciclo de vida aparece en el año 2003 (Kiritsis et al., 2003) mucho antes del aumento de dispositivos IoT.

El PLM no difiere mucho a los procesos de un dispositivo IOT, el primero se basa en una perspectiva económica de un producto desde su inicio en el mercado hasta su retiro y el segundo se refiere al dispositivo que basa en el uso individual en cada una de sus etapas, por ellos nos basaremos en el estado actual de los dispositivos como una instancia individual(Späthe, 2021)

En la actualidad los procesos pueden variar mediante una serie de herramientas y obtener soluciones factibles en un mundo que se enfrenta a cambios constantes y los retos vinculados en cada uno de los productos, el PLM puede incorporar una serie de aplicaciones sistemas industriales o comerciales.

EL modelo gestión de ciclo de vida del producto (PLM)(Hernando, 2015) aplicado a dispositivos IoT describe tres fases fundamentales inicio (BOL), medio (MOL) y fin (EOL)(Borsato, 2014) garantizando que las etapas del ciclo de vida sean optimas y permita obtener una mejor decisión en cada etapa(Yoo et al., 2016)

Ilustración 3. Etapas y subetapas del ciclo de vida en dispositivos IoT



Fuente: tomada a partir de (Kozma et al., 2021)

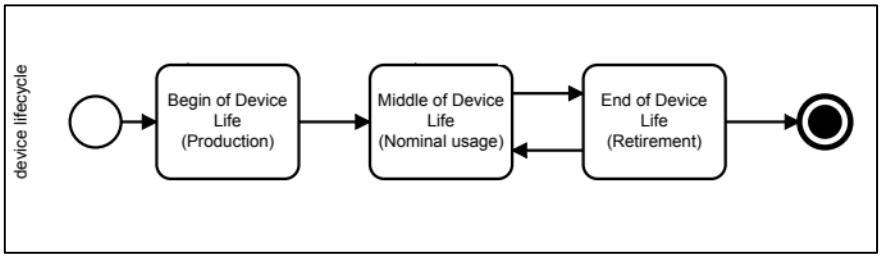
Mediante la gestión del ciclo de vida podemos determinar que es un proceso unidireccional (Kamalakkannan et al., 2020)debido a que pueden adquirir cambios

a lo largo de la eficiencia del dispositivo, por lo cual el modelo de seguridad durante la vida de los equipos se puede considerar completo si posee al menos una fase del ciclo de vida(Wellsandt et al., 2016)

ETAPAS DEL CICLO DE VIDA DE LOS DISPOSITIVOS IOT

En cada una de las etapas del modelo de gestión del ciclo de vida del dispositivo permite adquirir datos relevantes útiles, acerca del todo el ciclo de vida, como foco de desarrollo el dispositivo es el elemento principal(Kozma et al., 2024), por lo general PLM establece tres etapas fundamentales como se muestra en la ilustración 4 que están relacionados con el ciclo de vida de los dispositivos y se pueden describir de la siguiente manera:

Ilustración 4. Perspectiva del ciclo de vida en dispositivos IoT



Fuente: modificada a partir de (Späthe, 2021)

Por lo general PLM establece tres etapas fundamentales como se muestra en la ilustración 4 que están relacionados con el ciclo de vida de manera general en equipos inteligentes durante su ciclo de vida y se pueden describir como el punto de partida del dispositivo denominado BOL o producción abarca las ideas principales desde su diseño y arquitectura (Kozma et al., 2021), la fase intermedia conocida como la fase de uso nominal(Späthe, 2021), se utiliza para el uso, reparación y mantenimiento(Cavalcante & Gzara, 2018)

La fase dedicada al desmantelamiento o rehusó del dispositivo, se realiza modificaciones en la configuración del producto mucho de los dispositivos son removibles por cuestiones de versión o la calidad del producto, los problemas de seguridad en los dispositivos IoT se generan regularmente en el final, posee un gran efecto en la rentabilidad del dispositivo.

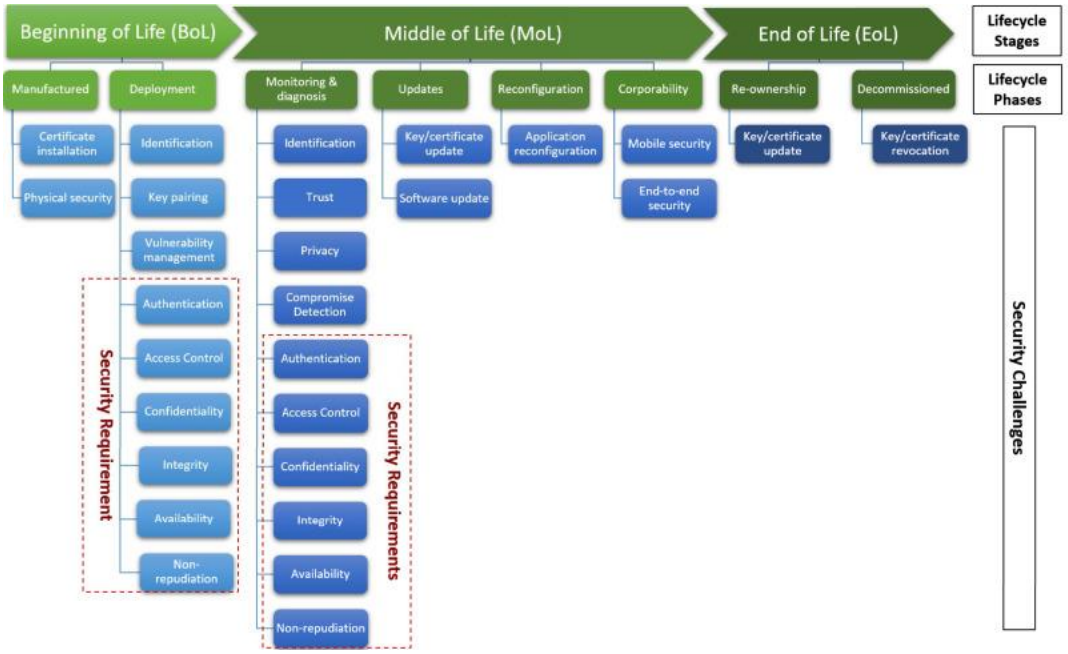
La fase final es la parte fundamental del ciclo de vida, debido a que los dispositivos desechados de manera errónea conllevan a una serie de vulnerabilidades al azar para los ciber atacantes.

1.3. Amenazas y vulnerabilidades en el ciclo de vida en dispositivos IoT

El aumento progresivo de dispositivos IoT ha permitido un conjunto de desafíos de seguridad donde los mecanismos de protección deben regirse a un conjunto de reglas basándose en los diferentes protocolos o estándares para la detección de vulnerabilidades en los dispositivos IoT. Los datos relevantes encontrados durante y mediante el ciclo de vida del dispositivo es de vital importancia durante sus inicios debido a los datos que manejan en tiempo real por parte de los usuarios.

Los datos del ciclo de vida demandan un seguimiento controlado desde el diseño hasta el desecho, mientras se pueda respaldar la información que en la mayoría son dispositivos inteligentes los mismos que contienen datos en tiempo real sin tomar en cuenta la exposición que presentan en cada una de sus fases.

Ilustración 5. Vulnerabilidades en cada fase del ciclo de vida en dispositivos IoT



Fuente: tomado a partir de (X. Li et al., 2025)

Los desafíos de seguridad que se presentan en la ilustración 5 es imprescindible detallar cada uno de las etapas principales con las fases Bol y Mol que contiene los principales pilares de la información como la confidencialidad que protege los datos para que no puedan acceder a la información no autorizada, la Integridad permite que la información sea viable y no sea alterada y por último la disponibilidad permite que los usuarios puedan obtener la información de los dispositivos (X. Li et al., 2025)

Además, requiere la supervisión constante durante el uso de los dispositivos inteligentes y asegurar los estándares de seguridad para los que fueron fabricados, en la sub etapa el ciclo EOL determina el entorno que será aplicado, en la etapa de uso nominal o MOL los dispositivos deben ser monitoreados constantemente para determinar con anticipación posibles amenazas de seguridad y permita ser diagnosticado a tiempo, y en la etapa final el declive del dispositivo es la eliminación de la información que contiene, para prever fallos de seguridad es primordial desecharlos de manera adecuada(X. Li et al., 2025)

En gran parte los dispositivos inteligentes son afectados por su uso en tiempo real, y con ello conlleva a desafíos de seguridad que van desde la autenticación, acceso, disponibilidad, confiabilidad e integridad, algunas de las soluciones de seguridad se basan en la arquitectura de IoT en la capa aplicación, red y percepción.

Estándares de Seguridad en dispositivos IoT

(Karale, 2021) menciona la importancia de implementar estándares para la seguridad de dispositivos IoT para reducir los riesgos de seguridad y permitan una comunicación eficiente entre dispositivos, entre las principales organizaciones se encuentran IEEE, ITU y ISO/IEC.

Los estándares ISO/IEC proporcionan un concepto de seguridad a nivel internacional para determinar la protección de información garantizando un ambiente seguro. En la tabla 2 establece alguno de los estándares necesario para sistemas IoT los cuales se detallan a continuación:

Tabla 2. Estándares de seguridad IoT ISO/IEC

Estándar ISO/IEC	Descripción
ISO/IEC 21823-1:2019	Ofrece un resumen de la interoperabilidad aplicable a los marcos de IoT, habilitando la interoperabilidad entre marcos independientes.
ISO/IEC 23093-1:2020	Describe la arquitectura de los marcos para IoT y determina las API y la representación de datos empaquetados.
ISO/IEC 21823-2:2020	Describe interfaces de interoperabilidad de transporte para el desarrollo de marcos de IoT con intercambio de datos.
ISO/IEC TR 30164:2020	Describe conceptos básicos, terminologías, casos de uso y avances de la computación de borde para IoT.
ISO/IEC TR 30166:2020	Trata marcos de la IIoT, análisis de riesgos y posibles estandarizaciones futuras.
ISO/IEC 27030	Se ocupa de la privacidad y la seguridad de IoT, proporcionando guías sobre principios, riesgos y controles.
ISO/IEC AWI 30147	Trata los procesos del ciclo de vida del sistema que se extienden a los marcos de IoT.
ISO/IEC AWI 30149	Aborda el marco de confianza de IoT, actualmente en desarrollo.

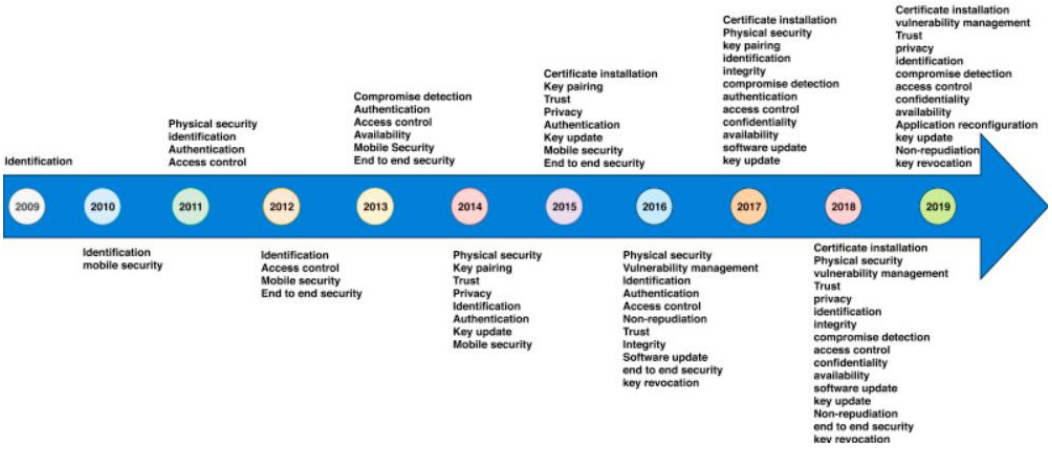
Fuente: tomado a partir de (Cisneros & Jacome, 2025)

ENISA (Agencia de la unión europea para la seguridad de redes y la información)(Enisa, 2018), establece una norma de referencia ISO/IEC 30141 para establecer medidas de seguridad en dispositivos IoT, detalla la aplicación de características como salvaguardar la información. La norma ISO/IEC AWI 30147 está vigente para procesos de ciclo de vida IoT para proteger la confiabilidad del sistema (ISO-IEC-30147-2021.pdf, s. f.), tomando en cuenta la protección de todo el sistema durante el periodo completo de vida en todos los niveles incorporando el proceso de progreso, producción e implementación(Enisa, 2018)

Sin embargo, esta norma no conlleva todos los aspectos de seguridad que requiere los dispositivos IoT, existe una norma basada en la ciberseguridad que expande su análisis de seguridad como controles o escenarios de riesgo pertinentes para dispositivos IoT que es la norma ISO/IEC 27400 con el fin de mitigar los riesgos de seguridad (Ameyed et al., 2023)

La seguridad en dispositivos IoT y su adaptación a las tareas de uso diario influyen en el aumento de vulnerabilidades exponiendo toda la información que es blanco fácil de los ciber-atacantes, la evolución de los desafíos de seguridad del ciclo de vida a través del tiempo se observa en la ilustración 6 con sus respectivas soluciones de seguridad:

Ilustración 6. Vulnerabilidades a lo largo de los años en dispositivos IoT



Fuente: tomada a partir de (Yousefnezhad et al., 2020)

Las vulnerabilidades que se pueden adquirir durante el ciclo de vida en dispositivos de uso domiciliario es extensa, desde su fabricación hasta el medio de uso en que se propaga, dichas vulnerabilidades se pueden crear reglas o medidas de mitigación para reducir los riesgos de seguridad, la tabla 3 determina un ejemplo de falencias de seguridad y medidas de mitigación en el sector domiciliario, en cada año se establece falencias de seguridad desde la identificación, control de acceso autenticación, actualización de claves, integridad hasta el final de la protección de los datos adquiridos:

Tabla 3. Medidas de prevención en vulnerabilidades de hogares domésticos

Vulnerabilidad	Medida de Mitigación
Contraseñas débiles	Uso de contraseñas fuertes y únicas
	Cambiar las contraseñas predeterminadas
Falta de actualizaciones	Implementar actualizaciones automáticas y regulares de software
	Garantizar que los dispositivos reciban parches de seguridad
Comunicación no cifrada	Usar protocolos de cifrado fuerte (como TLS) para todas las comunicaciones de datos
	Asegurar que los datos transmitidos y almacenados estén encriptados
Vulnerabilidades en firmware	Implementar mecanismos seguros de actualización de firmware
	Realizar auditorías de seguridad regulares del firmware
Falta de control de acceso	Implementar controles de acceso estrictos y autenticación de múltiples factores
	Asegurar que los dispositivos solo recopilen y envíen datos autorizados
Seguridad física deficiente	Fortalecer la seguridad física de los dispositivos IoT
	Proteger los dispositivos contra accesos físicos no autorizados
Violaciones de privacidad	Implementar fuertes medidas de protección de la privacidad
	Usar tecnologías como blockchain para mejorar la privacidad y seguridad
Ataques de inyección de código	Utilizar prácticas de programación seguras para prevenir la inyección de código malicioso
	Implementar validación y sanitización de datos de entrada

Fuente: tomado a partir de (Cisneros & Jacome, 2025)

La protección de la información durante las fases del ciclo de vida de los dispositivos en ambientes domiciliario ha generado gran impacto, identificar las amenazas existentes durante la vida útil es crítico lo que conlleva un desarrollo ineficiente de los dispositivos en el medio que se implementan.

El incremento de riesgos por los atacantes ya sea por protocolos de seguridad abiertos o simplemente malas prácticas por los usuarios que están expuestos al mundo, permite obtener información relevante al no poseer un modelo de seguridad administrable que en su mayoría permita reducir los ataques de seguridad.

Asegurar aspectos de privacidad entre dispositivos y fabricantes garantiza la escalabilidad y confiablidad frente ataques cibernéticos mediante un conjunto de controles de seguridad para dispositivos IoT (Ameyed et al., 2023)

Modelos de seguridad IoT en cámaras Ip mediante tecnología *blockchain*

Se ha mencionado que las cámaras ip son de uso común en hogares domésticos, con vulnerabilidades presentes dado que las cámaras IP utilizan un segmento de la red a través de la red en la que se encuentran empleadas, como se puede apreciar en la ilustración 7 de los dispositivos que pueden acceder a la conexión de internet.

Ilustración 7.- Dispositivos IoT conectados a través de internet

Fuente: tomada a partir de (Ospina Rodríguez, 2024a)

Las brechas de seguridad crecen conforme los dispositivos IoT aumentan en el mercado, las cámaras de seguridad han surgido de manera abundante y con ello sus fabricantes, existen de diferentes marcas Tplink, hikvision, dahua , dlink, Ezviz, hilook, etc, son las más conocidas en el mercado por su versatilidad y utilidad (Ospina Rodríguez, 2024), las cuales son puntos de ataques cibernéticos usando información confidencial desde la adquisición de video en tiempo real. Tomando en cuenta que las cámaras Tp-link, dahua y hikvision están en su mayoría disponibles en el mercado.

La necesidad de determinar procesos seguros y confiables ofrece un sin número de desafíos de seguridad, el modelo de autenticación mediante tecnología blockchain tiene como objetivo mejorar la seguridad de manera eficiente por medio de claves criptográficas o firmas digitales (Ospina Rodríguez, 2024)

El modelo de autenticación mediante *blockchain equirest*, emplea su análisis en tres cámaras ip diferentes (DH-IPC-HDW1239T1-LED-S5(dahua), DS-2CV2Q21FD-IW(hikvision) y Cámara wifi V380(gerrit))(Ospina Rodríguez, 2024b). Provistas por diferentes proveedores, los dispositivos elegidos poseen características y especificaciones similares, como medidas de seguridad se identifica especificaciones técnicas, medidas de seguridad y vulnerabilidades que se puede apreciar en la tabla 4.

Tabla 4.- Características similares basado en tres modelos de cámaras ip (dahua, hikvision, gerrit)

ESPECIFICACIONES	**MÉTODOS DE ACCESO** • Accesos web, acceso app (depende del fabricante) **PROTOCOLOS DE COMUNICACIÓN** • http,802.11b(CCK,QPSK,BPSK)802.11g/n(OFD) (DS-2CD2441G0-I(W), s. f.) CIFRADO • SSL/TLS, WPA2/WPA3
MEDIDAS DE SEGURIDAD	• Bloqueo de múltiples intentos de sesión • Utilizar algoritmos hash para proteger contraseñas • Configurar la cámara con ip fija • Encriptación de datos • Autenticación de nodos • Cambio de contraseña • Eliminación de contraseñas en archivos de configuración • Identificación segura de usuarios • Firmas digitales
VULNERABILIDADES	• Configuraciones por defecto • Usuarios, contraseñas, dirección ip, puertos no son cifrados • SSID predeterminado • Autenticación incorrecta • Puertos abiertos • Contraseñas predeterminadas • Acceso no autorizado • Ataques de fuerza bruta • Ataque de reenvió de contraseña

Fuente: tomada a partir de (Ospina Rodríguez, 2024b)

El modelo de seguridad empleado por (Ospina Rodríguez, 2024b), establece en lo mínimo cierto número de especificaciones técnicas, vulnerabilidades y medidas de prevención de seguridad, dicho proyecto de investigación no posee un modelo administrable para gestionar la seguridad durante el ciclo de vida de los dispositivos IoT aplicado a cámaras ip tomando en cuenta las medidas de seguridad en cada etapa del dispositivo y mucho menos realiza a detalle la falta de seguridad, guía de implementación y medidas de prevención.

Modelo de seguridad en cámaras ip en ambientes domésticos

Es esencial fomentar la identificación de vulnerabilidades en cámaras ip, para determinar las medidas de prevención y evitar el robo de información. (Ribero-Corzo & Prieto-Guerrero, 2021)establece un conjunto de riesgos en cámaras Ip en hogares domésticos con el propósito de procedimientos o guías prácticas de

seguridad para personas que desean adquirir e implementar este tipo de dispositivos, debido a la facilidad de monitorear de manera remota mediante cámaras ip a través del internet, permitiendo adquirir información sin consentimiento y propensos a ataques de seguridad**.**

(Ribero-Corzo & Prieto-Guerrero, 2021)realiza una comparación de diferentes tipos de cámara para evaluar cada una y determinar medidas de prevención para garantizar el uso y operación de las cámaras, desde la adquisición y la ubicación en un entorno doméstico, detalla algunos consejos de la forma de instalación de cámaras ip que sea de utilidad para personal técnico si de alguna forma obvio algún paso al momento de su implementación como guía de seguridad, en la siguiente tabla 5 se puede apreciar un conjunto de procedimientos para instalar cámaras de seguridad.

Tabla 5.- Procedimientos para implementar cámaras Ip

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

Fuente: tomada a partir de (Ribero-Corzo & Prieto-Guerrero, 2021)

Desde luego la guía realizada en la ilustración puede variar dependiendo la forma y el uso del personal técnico requiera emplear al momento de instalar una cámara de seguridad, no es una guía estandarizada, pero si la más viable identificada en su revisión y valoración en la investigación, para la identificación de vulnerabilidades y medidas de prevención.

Para determinar la seguridad de las cámaras ip basa su análisis en cuatro diferentes tipos de marcas, Tplink-Dlink, Ezviz, Dlink y Yoose, determinadas por los manuales técnicos de cada una(Ribero-Corzo & Prieto-Guerrero, 2021) especificadas en la tabla 6.

Tabla 6.- Características de seguridad en cuatro modelos distintos de camaras IP

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 Estándar H.264	Vigilancia en tiempo real 24/7 Estándar H.264	Vigilancia en tiempo real 24/7 Estándar H.264	Vigilancia en tiempo real 24/7 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

Fuente: tomada a partir de (Ribero-Corzo & Prieto-Guerrero, 2021)

El modelo de seguridad IoT determina que la mayoría de las cámaras ip son vulnerables accediendo a la red mediante los sistemas operativo a utilizar desde Linux o Windows, grabaciones disponibles en la red o cualquier cortafuegos disponible pueden ser afectados, las fallas de seguridad no dependen solo del dispositivo que se adquiere sino desde la configuración inicial, el uso y mantenimiento de los dispositivos instalados (Ribero-Corzo & Prieto-Guerrero, 2021)

En la siguiente tabla 7 se determina una serie de vulnerabilidades presentes ante posibles ataques de información.

Tabla 7.- Vulnerabilidades y ataques en cámaras de seguridad ip

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

Fuente: tomado a partir de(Ribero-Corzo & Prieto-Guerrero, 2021)

Es necesario determinar que los ataques frecuentes en cámaras ip provienes desde ataques de fuerza bruta, *sniffing* (intercepta datos a través de la red) y ataques *man in the middle* (hombre en el medio) (Mazon-Olivo & Pan, 2022) la cual permite una comunicación entre dos dispositivos al momento de adquirir datos relevante, durante el desarrollo de la investigación se puede determinar que los riesgos asociados a los cuatro modelos diferentes son aplicados a cada cámara ip sin tomar en cuenta el fabricante o modelo (Ribero-Corzo & Prieto-Guerrero, 2021).

Tabla 8.- Recomendaciones para prevenir fallos de seguridad en cámaras ip

RECOMENDACIONES
• Cambiar credenciales establecidas por defecto. • Utilizar credenciales fuertes y robustas con caracteres alfanuméricos por lo mínimo de 8 caracteres. • Las credenciales de las aplicaciones determinadas por los fabricantes deben ser diferentes a las cámaras ip. • Realizar una conexión VPN para encriptar y ocultar la información de la dirección ip del dispositivo. • Seguir los controles de seguridad sugeridos por el fabricante. • Leer el manual de instalación y configuración del dispositivo permite gestionar de mejor manera la información. • El personal técnico o el usuario final deben leer los manuales de instalación y seguridad determinados por el fabricante. • No ingresar a enlaces enviados por correo electrónico sin corroborar la información establecida por el fabricante • No permitir actualizaciones de firmware o software de sitios no oficiales. • Ingresar por direcciones URL únicas determinadas para el control del dispositivo. • Aplicar las nuevas actualizaciones firmware, parches de seguridad, certificados digitales • Realizar Backus de información de las tarjetas físicas de manera manual. • Formatear la información de manera periódica. • Realizar mantenimientos preventivos de limpieza para prevenir daños del dispositivo y realizar el desecho del mismo.

Fuente: tomado a partir de (Ribero-Corzo & Prieto-Guerrero, 2021)

El modelo determinado por (Ribero-Corzo & Prieto-Guerrero, 2021), establece una serie de requerimientos para salvaguardar la información de manera adecuada, desde guías de implementación de cámaras ip, amenazas, vulnerabilidades y medidas de prevención aplicable a cualquier dispositivo de diferentes fabricantes o modelos permite ser un modelo de seguridad viable y de fácil comprensión para el personal técnico como recomendaciones generales al momento de implementar este tipo de cámaras ip.

No obstante, el modelo de seguridad no adquiere información de las etapas que conlleva una cámara ip durante su vida útil, no establece problemas y medidas de prevención de seguridad en cada una de sus etapas y para finalizar no determina procedimientos adecuados para desechar este tipo de dispositivos una vez llegado a su uso obsoleto por nuevos dispositivos o tecnologías. Sin embargo, los procedimientos establecidos nos permiten identificar, seleccionar los problemas y medidas de prevención y clasificar en cada etapa que presenta las cámaras ip durante su periodo de duración.

CAPÍTULO II. DISEÑO METODOLÓGICO

El presente proyecto de desarrollo, adopta una investigación bibliográfica, de alcance descriptivo, no experimental para el MODELO DE GESTIÓN SEGURIDAD EN EL CICLO DE VIDA DE LOS DISPOSITVOS IOT, la información recolectada se utiliza para determinar la gestión de seguridad durante el ciclo de vida de los dispositivos por medio de su vida útil y las etapas de desarrollo desde su inicio.

El presente estudio ayudará a obtener información acerca de las vulnerabilidades presentes durante el ciclo de vida y la manera de mitigar los ataques que se presente mediante un conjunto de actividades necesarias para la gestión de seguridad, mediante una evaluación en cámaras ip aplicable a diferentes modelos y fabricantes con el fin de establecer requisitos de seguridad antes y durante su ciclo de vida desde la instalación hasta el retiro del dispositivo.

Enfoque metodología descriptiva

Debido a que el trabajo se basa en una investigación bibliográfica, la metodología descriptiva es concluyente la cual permite medir con mayor precisión la importancia del objetivo de estudio sobre problemas mecanismos de seguridad durante el ciclo de vida de los dispositivos, garantizando en su mayoría la veracidad de la información, evaluando como referencia dispositivos como cámaras IP.

2.1. Metodología de investigación

Tipo de investigación

El presente proyecto de desarrollo es bibliográfico, no comprobable de manera práctica, debido a que nos permite obtener información relevante del tema y determinar su confiabilidad, por ello se emplea material como investigaciones científicas en base a artículos de calidad como ScienceDirect, IEEE, Scopus, Google Scholar, Springer, etc relacionados con términos vinculados al ciclo de vida, vulnerabilidades y gestión de seguridad en el ciclo de vida de los dispositivos

inteligentes durante su periodo de implementación y eliminación del ambiente implementado.

La mayoría de los artículos académicos encontrados se encuentran escritos en inglés, no cuentan en mayor parte con datos o información accesible sobre el ciclo de vida de los dispositivos IoT y las vulnerabilidades de seguridad presentes en cada etapa, sin embargo como tal no se adquiere como tal información sobre modelos de gestión de seguridad en dispositivos IoT , los modelos presentados en el capítulo II basa su análisis en forma general como modelos de seguridad en cámaras IP aplicable a diferentes modelos y fabricantes, con procedimientos desde instalación, amenazas de seguridad, medidas de prevención, protocolos de seguridad, especificaciones técnicas, etc.

Enfoque metodología descriptiva

Debido a que el trabajo se basa en una investigación bibliográfica, la metodología descriptiva es concluyente la cual permite medir con mayor precisión la importancia del objetivo de estudio sobre problemas y medidas en seguridad durante el ciclo de vida de los dispositivos, garantizando en su mayoría la veracidad de la información.

2.2. Metodología de desarrollo

Para el presente proyecto de desarrollo se determinar realizar una revisión admisible, clara y concisa mediante la búsqueda en artículos, revisas científicos, etc basándose en la metodología PRISMA, la cual realiza revisiones sistemáticas de documentos viables para el desarrollo de la investigación evaluando etapas del ciclo de vida en dispositivos inteligentes o modelos de seguridad para determinar la factibilidad del presente proyecto de investigación(Page et al., 2021).

La metodología PRISMA se emplea para evaluar y mitigar amenazas en el ciclo de vida de los dispositivos con perspectiva en gestión de riesgos, privacidad y seguridad de la información siguiendo tres fases fundamentales:

- Fase I: Investigación Científica
- Fase II: Lectura y extracción de información.
- Fase III: Elaboración del documento final.

Se realiza una búsqueda exhaustiva de información en diferentes artículos académicos basándonos en términos clave como mecanismos de seguridad de los dispositivos IoT durante el ciclo de vida.

Se exponen aspectos a lo largo del periodo de implementación, conocimientos y relación en términos de ciclo de vida del producto(Hernando, 2015) o dispositivos IoT, entre los cuales se obtiene información de las etapas o mecanismos de seguridad para mitigar vulnerabilidades, al momento de realizar el análisis la mayoría emplea el término a nivel industrial y en sectores domésticos no es tan relacionado

Tabla 9. Artículos científicos enfocado al ciclo de vida en dispositivos IoT.

TEMA	DESCRIPCIÓN	APORTE AL TEMA	REFERENCIA
Evaluación del impacto ambiental de los dispositivos IoT: un enfoque basado en gráficos.	Realiza una evaluación de las fases del ciclo de vida aplicado al termino productos basado en IoT.	• Analiza el impacto ambiental empleando la terminología ciclo de vida por medio de gráficos. • Establece el aprendizaje automático para las evaluaciones del ciclo de vida en ambientes propicios.	(Mohamed et al., 2024)
Industria 4.0 y evaluación del ciclo de vida: Evaluación de las aplicaciones tecnológicas como activo para el inventario del ciclo de vida(Piron et al., 2024).	Determina e implementa un análisis corto sobre el ciclo de vida en la industria aplicado a dispositivo IIoT.	• Evalúa el ciclo de vida en sectores industriales. • Evalúa el internet de las cosas. Big data, sistemas ciber físicos, nube, IA, blockchain, etc.	(Piron et al., 2024)
Un esquema de autenticación de ciclo de vida completo para aplicaciones IoT inteligentes a gran escala	Establece un método de seguridad de autenticación de dispositivos a través de un modelo de ciclo de vida completo	• Estudia los problemas de autenticación de los dispositivos IoT. • Realiza un método de autenticación de dispositivos,	(Chen et al., 2023)

	desde la fabricación hasta el rehusó.	aplicaciones y servidores. • Establece un modelo de autenticación en cámaras inteligentes en hogares.	
El marco conceptual del sistema de soporte de decisiones basado en IoT para la gestión del ciclo de vida.(Kamalakkannan et al., 2020)	Gestionar el periodo de duración durante el ciclo de vida para productos del sector manufacturero e identificar los puntos necesarios para la gestión del producto mediante datos adquiridos en entornos reales.	• Evaluación del ciclo de vida en entornos reales. • Estándar ISO 14044 para implementar la ejecución del ciclo de vida. • Sostenibilidad en la elaboración de productos.	(Kamalakkannan et al., 2020)
Modelos de ciclo de vida de sistemas producto-servicio: revisión de la literatura propuesta(Cavalcante & Gzara, 2018).	Establece un enfoque de investigación basado en modelos de ciclo de vida desde la concepción del producto hasta el desarrollo del mismo	• Determina el ciclo de vida del producto(Hernando, 2015) desde el diseño hasta la eliminación. • Realiza una revisión del ciclo de vida desde perspectivas del usuario, venta, compra y servicio.	(Cavalcante & Gzara, 2018)
Comprensión de los sistemas IoT: un enfoque de ciclo de vida(Rahman et al., 2018)	Comprende cada una de las fases que posee el ciclo de vida desde el dispositivo, aplicaciones o servicio IoT con la finalidad de definir un modelo genérico.	• Definición de ciclo de vida en sistemas basados en IoT. • Determinar las soluciones en cada una de sus etapas.	(Rahman et al., 2018)
Ciclo de vida de los dispositivos IoT: un modelo genérico y un caso de uso para redes móviles celulares(Soós et al., 2018).	Busca determinar un modelo definido del ciclo de vida desde su inicio hasta su desmantelamiento desde cambios de corto a largo plazo y emplea un escenario de una red móvil celular para la seguridad del dispositivo.	• Determina las fases y subfases pertinentes en cada parte del ciclo de vida. • Utiliza las reglas de BPMN de Microsoft para un modelo genérico del ciclo de vida. • Ciclo de vida aplicado a teléfonos celulares.	(Soós et al., 2018)

Reduciendo la brecha entre la gestión del ciclo de vida del producto y la sostenibilidad en la fabricación mediante la creación de ontologías(Borsato, 2014).	Concede establecer ontologías para la viabilidad de los productos Iot que facilite el intercambio de información.	• Establece definiciones de las etapas del ciclo de vida BOL, EOL y MOL	(Borsato, 2014)

Fuente: elaboración propia

Como tal los hallazgos encontrados no se centran en determinar el ciclo de vida de los dispositivos mediante modelo de gestión de seguridad aplicado a hogares domésticos, sin embargo dado la investigación pertinente permite relacionar las etapas del ciclo de vida en dispositivos y modelos de seguridad en cámaras ip aplicado en hogares domésticos en el análisis del estado del arte, el cual requiere ser enfocado y dedicado a personal técnico con capacidades de implementación de cámaras de seguridad mediante una guía adecuada para gestionar la información en dichos dispositivos.

Contemplando en mayoría las vulnerabilidades y medidas de prevención para la gestión de seguridad en los dispositivos IoT, la mayoría emplea el término ciclo de vida en sector industriales, medicina, datos, etc y no conllevan el termino ciclo de vida de los dispositivos IoT en cámaras ip implementadas en hogares domésticos que son el uso más común hoy en día, para prevenir y solventar fallas de seguridad durante todo el ciclo de vida que se requiere ser evaluado.

Fase II: Lectura y extracción de información

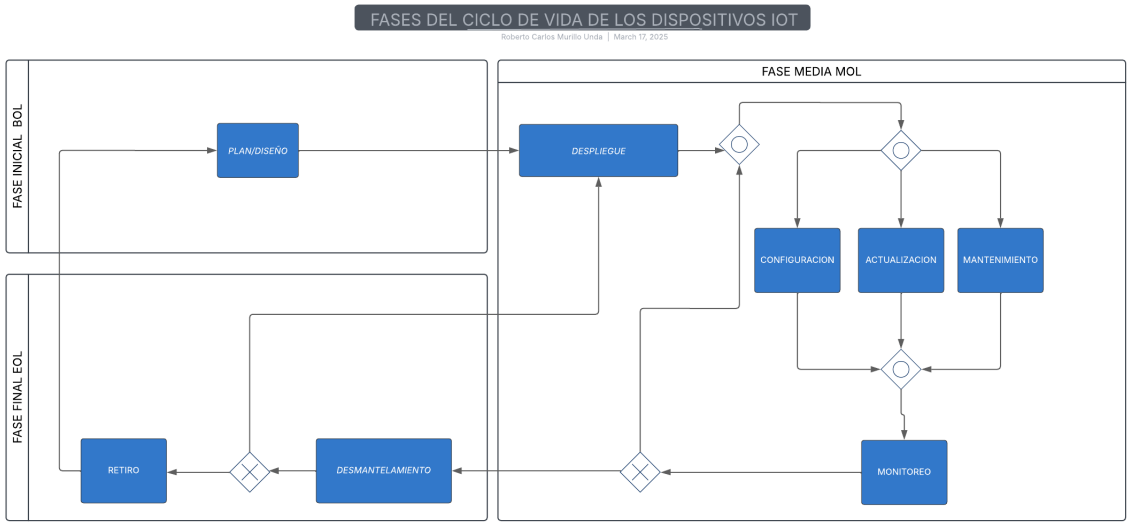
Se realiza la extracción de la información relevante de los temas y subtemas que posean información acerca de las fases empleadas durante el ciclo de vida de los dispositivos con el propósito de vincular medidas de seguridad en cada fase a largo de la vida útil que favorezcan el modelo de seguridad a elaborar.

Los datos obtenidos mediante modelos de seguridad IoT es de suma importancia, determina una serie de procedimientos necesarios para la implementación de cámaras IP en hogares domésticos, los cuales permite una visión clara a personal

técnico que opte por tomar las medidas necesarias de prevención y mediante la investigación del presente proyecto obtenga conocimientos adecuado de lo que representa el ciclo de vida en los dispositivos IoT.

Cada uno de los temas seleccionados poseen al menos una perspectiva de ciclo de vida, poseen actividades específicas para su desarrollo y funcionamiento del dispositivo, mediante el modelo BPMN(Späthe, 2021) de Microsoft permite realizar procesos detallados de fácil implementación y desarrollo en cada uno de los procesos y subprocesos, en las fases principales del ciclo de vida, las cuales se detallan en la respectiva ilustración 8:

Ilustración 8. Fases del ciclo de vida en dispositivos IoT



Fuente: modificado a partir de(Soós et al., 2018)

Las fases empleadas en cada bloque conllevan al análisis pertinente en cada una de las sub categorías asignadas a cada fase del ciclo de vida de los dispositivos, las cuales son necesarias para que el personal técnico obtenga una idea clara sobre el procedimiento o etapa que conlleva los dispositivos IoT durante su vida útil y la seguridad que deba poseer cada uno de ellos en cada etapa. A continuación, se detalla cada una de las subetapas con sus respectivos requerimientos, utilidad, vulnerabilidades y medidas de prevención.

FASE INICIAL

Como se ha mencionado el inicio de un dispositivo empieza desde su desarrollo hasta su implementación, nace de una idea, se convierten en especificaciones y finalmente su producción(Cavalcante & Gzara, 2018).

- **Plan**

  En la etapa de planificación se adquiere la información del dispositivo y los requisitos de funcionamiento, conocida como el inicio de la concepción del producto mediante el número de requerimientos y necesidad del usuario, con el propósito de cubrir las demandas de las personas y del mercado(Kozma et al., 2021).
- **Diseño**

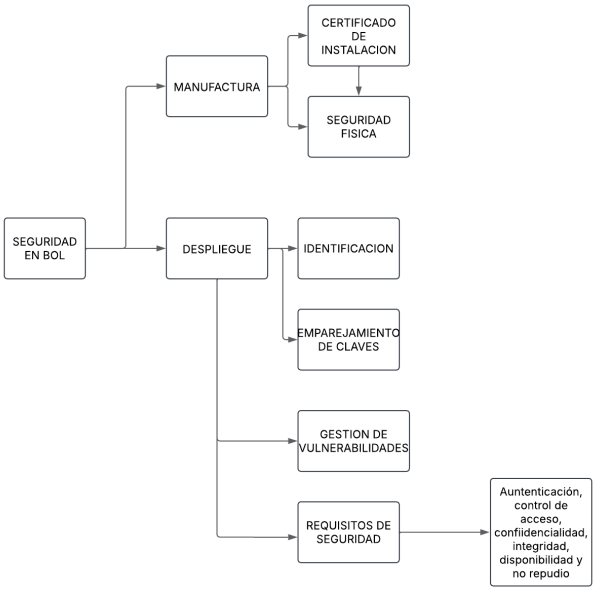
  Después realizar la fase de planeación, por consiguiente conlleva a su respectiva fase de diseño, con la finalidad de establecer dispositivos en óptimas condiciones y su funcionalidad para el que fue diseñado, tomando en cuenta las especificaciones que poseen a nivel de hardware y software del dispositivo final a diseñar(Soós et al., 2018).

DESPLIEGUE

Después del diseño y planificación del dispositivo se encuentra en condiciones para su implementación y da paso a su fase intermedia en la cual el dispositivo debe conectarse a la red y adquirir un identificador único , un ejemplo claro es la dirección IP(Soós et al., 2018). La entrega de los dispositivos por lo regular se da una única vez, en cambio el soporte del equipo debe ser continuo con el objetivo de dar vida a los dispositivos durante su vida útil.

Por consiguiente, en la etapa inicial se puede adquirir diversos problemas de amenazas que afecten al desarrollo en la ilustración 8 se puede apreciar cada problema obtenido, especificando en cada una de sus subetapas:

Ilustración 9.- Problemas de seguridad en el inicio del ciclo vida BOL



Fuente: modificado a partir de (Yousefnezhad et al., 2023b)

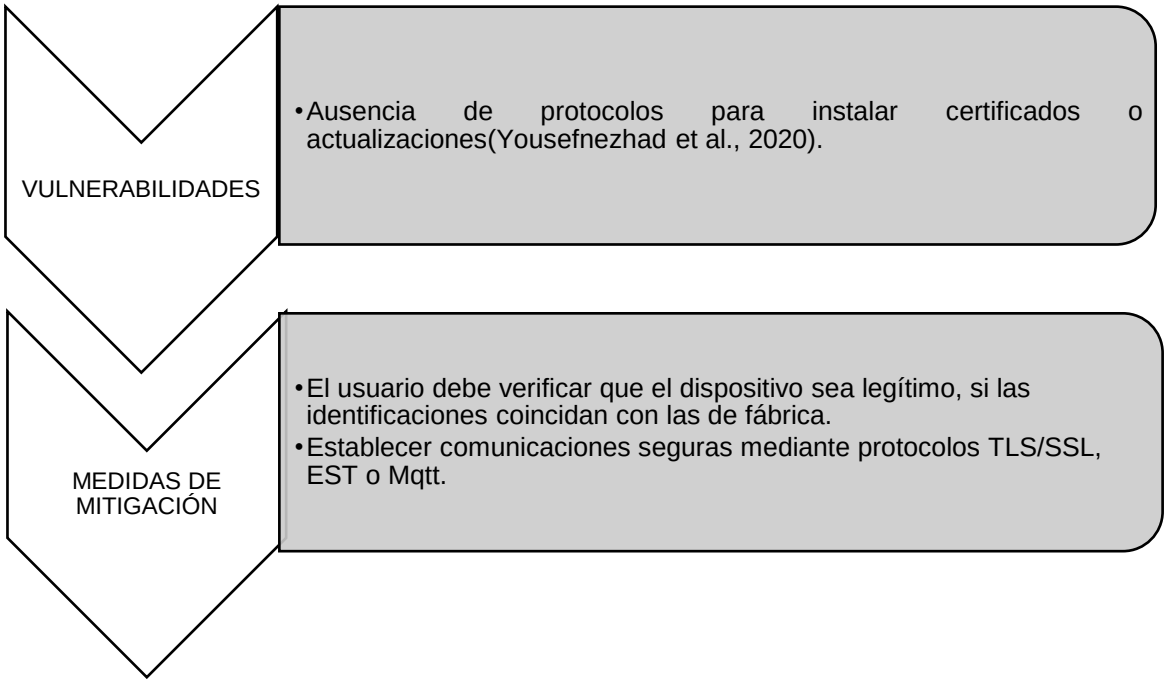
En la sub etapa del inicio del ciclo de vida de los dispositivos IoT, en la fabricación se adquieren dos tipos de problemas de seguridad:

Certificados de instalación. - Comienzan al inicio de vida de los dispositivos, aunque no se haya diseñado y elaborado el dispositivo final es necesario registrar su serie, versión, identificador o MAC del dispositivo(Späthe, 2021), el certificado se puede instalar de forma manual o de forma automática que se puede realizar mediante las páginas oficiales determinadas por los fabricantes(Yousefnezhad et al., 2020).

La implementación de certificados permite garantizar la comunicación y la autenticidad de los dispositivos para establecer comunicaciones confiables y seguras con otros dispositivos

Por lo cual una instalación de certificados de manera automática puede adquirir riegos de seguridad, no es una manera viable, entre los problemas destacados determinados en la ilustración 10:

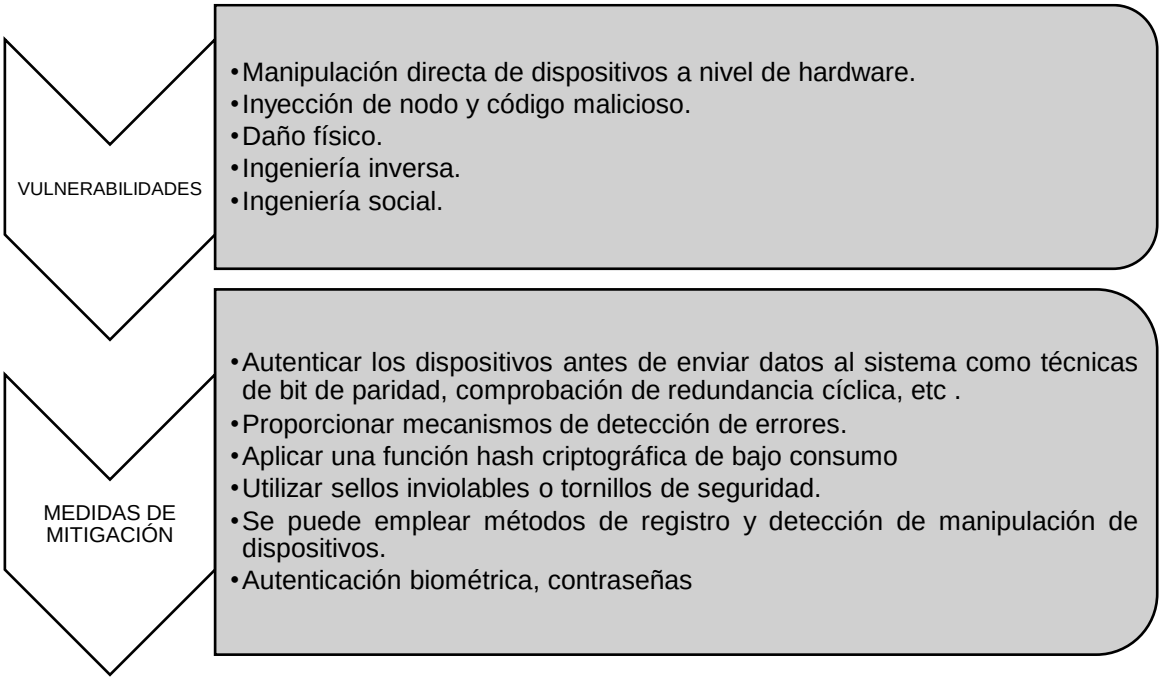
Ilustración 10.- Vulnerabilidades y medidas de mitigación en la sub etapa Manufactura



Fuente: elaboración propia

Seguridad física. - El acceso físico a los dispositivos son vulnerables porque son expuestos en diversas ubicaciones o entornos que son instalados y se requiere medidas necesarias para proteger la información contra accesos no autorizados, el atacante debería estar al menos cerca o dentro de los dispositivos IoT(Andrea et al., 2015), se estima que los ataques físico se puedan realizar en su mayoría a nivel de software(Yousefnezhad et al., 2020).

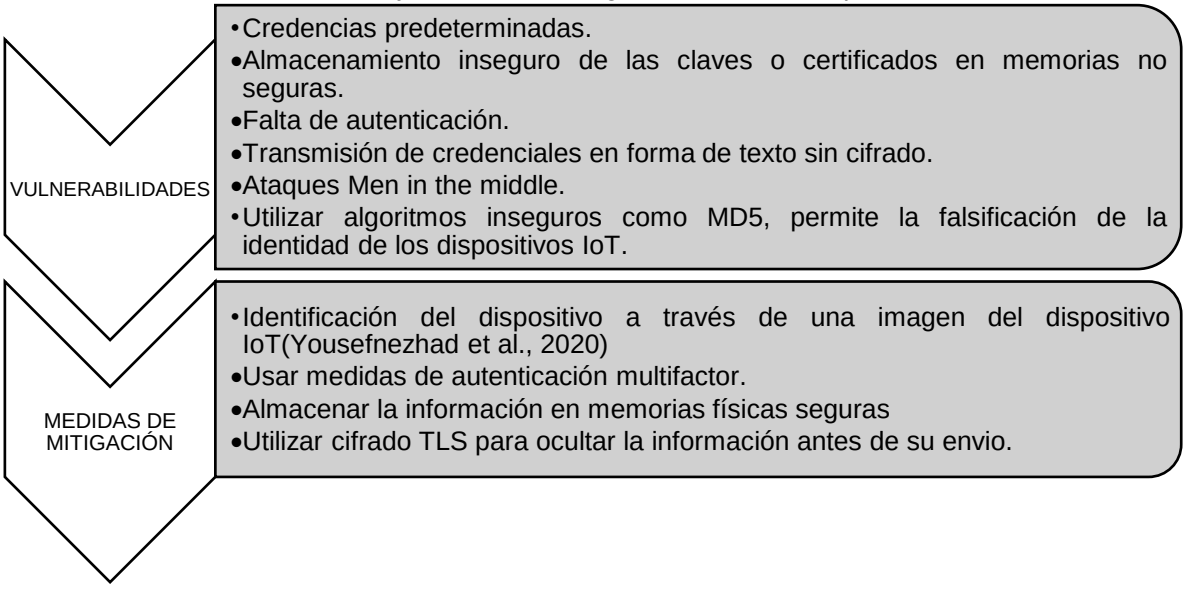
Ilustración 11.- Vulnerabilidades y medidas de mitigación en la sub etapa de Seguridad Física



Fuente: tomado a partir de (Andrea et al., 2015)

Identificación. - Los dispositivos IoT requieren verificar su identidad antes de establecer comunicación con otros dispositivos, garantizando que sea seguro y legítimo, si la etapa de identificación no se implementa de una manera adecuada pueden surgir problemas de seguridad a través de la red o en el medio que se propagan.

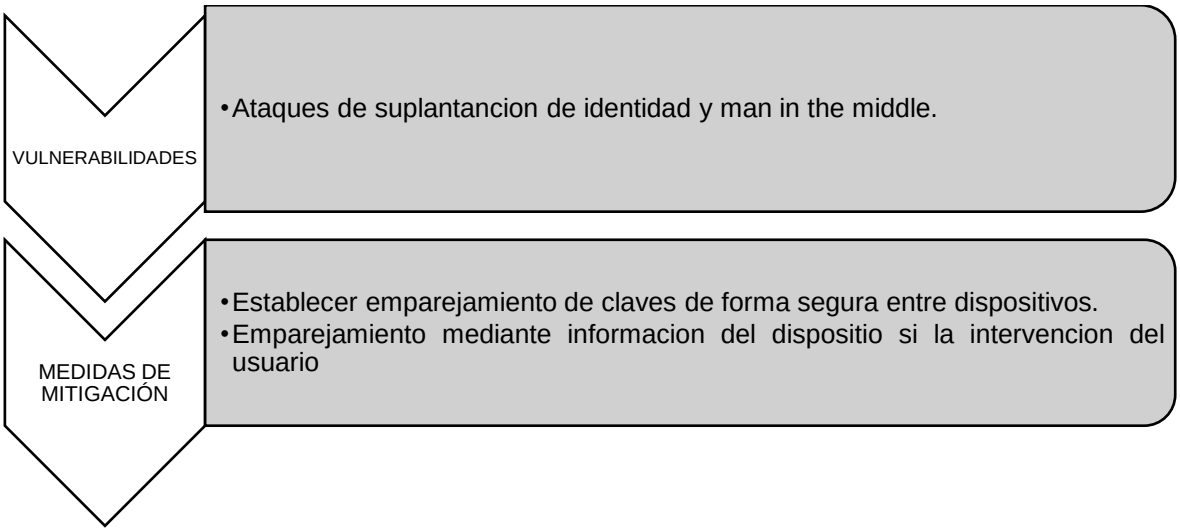
Ilustración 12.- Vulnerabilidades y medidas de mitigación en la sub etapa de Identificación



Fuente: elaboración propia

Emparejamiento de claves. - Es una etapa crítica para la seguridad de los dispositivos debido a que establece una comunicación segura mediante claves criptográficas, control de acceso y claves de autenticación durante todo el ciclo de vida (Miettinen et al., 2018).

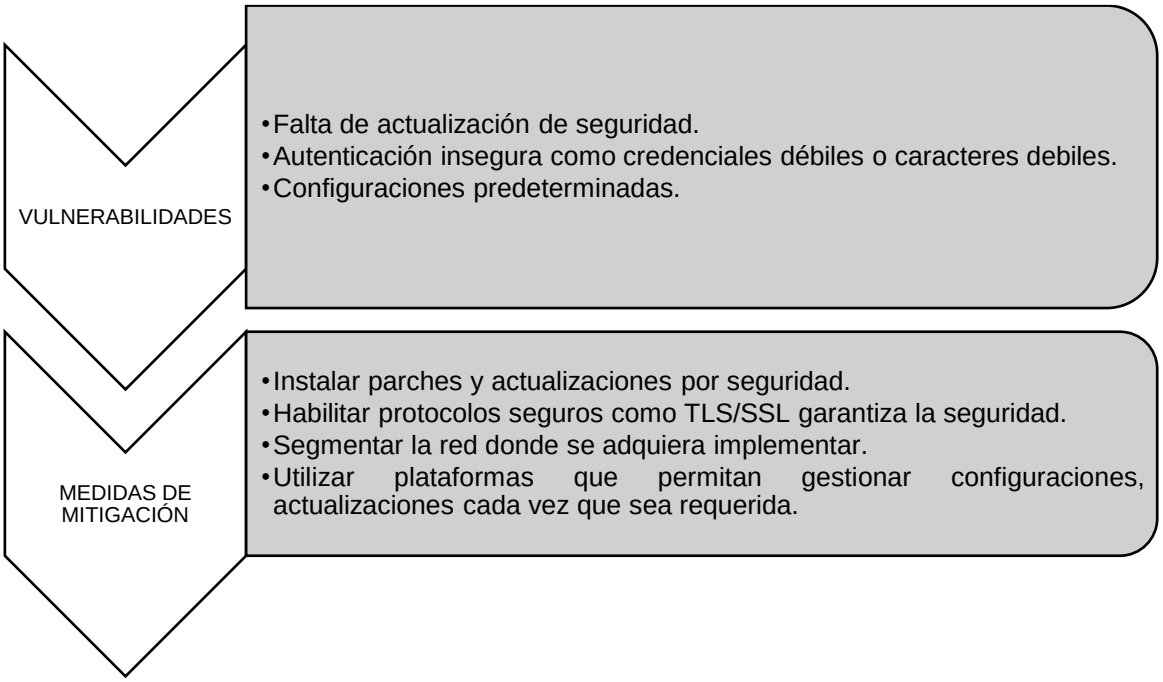
Ilustración 13.- Vulnerabilidades y medidas de mitigación en la sub etapa de seguridad Emparejamiento de claves



Fuente: tomado a partir de (Miettinen et al., 2014)

Gestión de vulnerabilidades. – Establece las debilidades de los dispositivos IoT cuando son instalados en un entorno real, esta etapa es el inicio de operación de los dispositivos y están expuestas a posibles ataques. En hogares inteligentes las vulnerabilidades se presentan en dispositivos que se encuentren conectados a la red.

Ilustración 14.- Vulnerabilidades y medidas de mitigación en la sub etapa de seguridad Gestión de vulnerabilidades



Fuente: tomado a partir de (Alrawi et al., 2019)

FASE MEDIA O DE USO NOMINAL

En esta etapa se desglosa con mayor claridad los procesos que conllevan cada uno de los dispositivos inteligentes que internamente se encuentran relacionados mediante la conexión a través de la red, en la actualidad la fase media es el proceso actual en el que los dispositivos se encuentran a nivel general, en esta etapa los dispositivos se monitorean constantemente desde la configuración, actualización o mantenimiento(Kozma et al., 2021).

Las siguientes etapas es el proceso más largo que conlleva la vida útil de los dispositivos IoT, debido a la constante supervisión del producto se dividen en las siguientes:

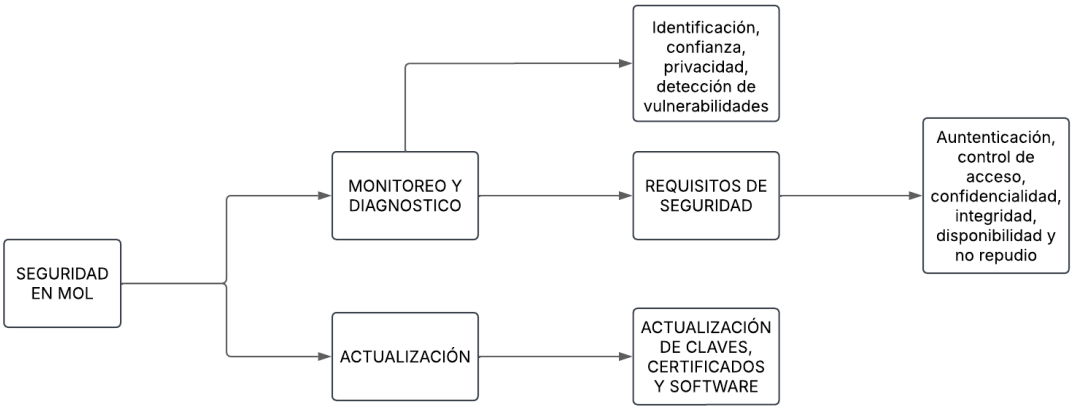
Tabla 10. Subetapas de la fase media del ciclo de vida en dispositivos IoT

SUB ETAPA	CARACTERISTICAS
Configuración	• Ajustes de configuración dependiendo del área a ejecutarse • Identificar la red. • La reconfiguración del dispositivo puede ser cíclica durante su vida útil. • Configuración de seguridad en la red para los dispositivos.
Actualización	• Permiten que los dispositivos actúen con nuevas habilidades para el usuario. • Actualización de firmware y software para mejoras las capacidades de los dispositivos • Las actualizaciones pueden ser programadas.
Mantenimiento	• No realizar manteniendo puede causar fallos de seguridad o de forma física. • Realizar mantenimiento preventivo o correctivo. • Puede provocar el desecho del dispositivo mucho antes de culminar su ciclo de vida. • Monitoreo continuo de las vulnerabilidades al sistema.
Monitoreo	• Monitoreo constante durante su ciclo de vida. • Se puede recopilar información necesaria del dispositivo para evaluar su disponibilidad activa en el entorno que se encuentra ejecutándose. • Proveer información a los usuarios del estado del dispositivo.

Fuente: tomado a partir de (Kozma et al., 2021),(Soós et al., 2018)

La etapa media del ciclo de vida de los dispositivos es mayormente vulnerable debido a la necesidad de monitorear y diagnosticar fallas de seguridad una vez que el dispositivo sea instalado en su entorno, en la ilustración 15 se menciona a detalle los problemas de seguridad:

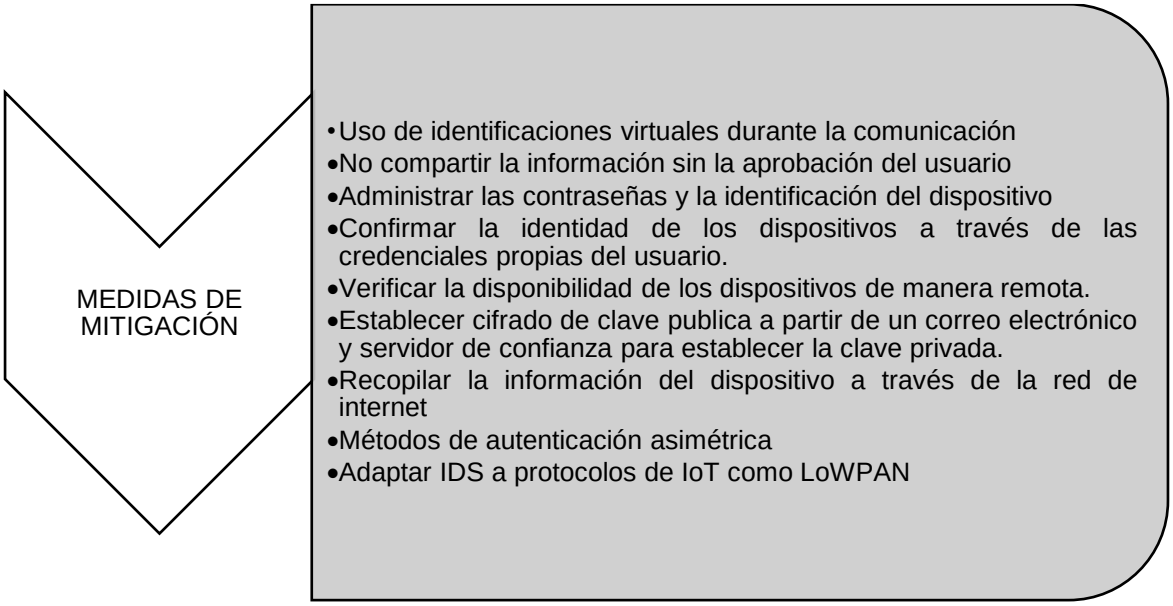
Ilustración 15.- Problemas de seguridad en la etapa media del ciclo de vida MOL



Fuente: modificado a partir de (Yousefnezhad et al., 2023b)

Una vez identificado las fallas de seguridad se puede apreciar en la etapa de monitoreo y diagnostico establece una relación entre el proveedor de los dispositivos, se detalla en la siguiente ilustración 16 las diversas soluciones de seguridad en cada una de las sub etapas que permita la identidad, confianza, privacidad y detección de vulnerabilidades.

Ilustración 16.- Medidas de mitigación en la sub etapa de Monitoreo y Diagnóstico

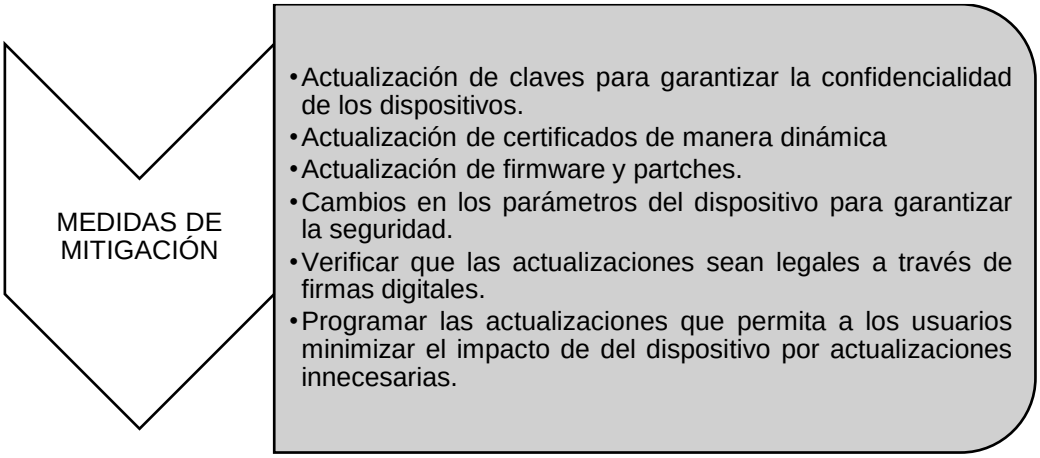


Fuente: tomado a partir de (Yousefnezhad et al., 2020)

Las actualizaciones requeridas durante el ciclo de vida en dispositivos inteligentes son parte fundamental y necesaria para adecuar la administración de seguridad

para salvaguardar la información de los ataques provenientes de manera externa o interna para mantener el rendimiento de los dispositivos a lo largo de su vida útil. A continuación, se presenta las medidas de prevención para cada actualización desde nivel de certificados, claves y software.

Ilustración 17.- Medidas de mitigación en la sub etapa de Actualizaciones



Fuente: elaboración propia

FASE FINAL EOL

La fase final del dispositivo se debe a muchas circunstancias, como el remplazo del dispositivo por una versión modificada o el dispositivo no soporte las actualizaciones actuales, no satisface las necesidades de las personas o simplemente el final de su vida útil(Späthe, 2021) que es alrededor de 2 a 5 años lo que es conocida como obsolescencia programada.

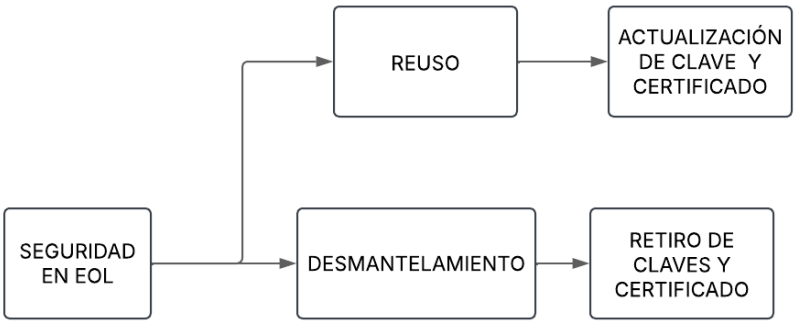
Sin embargo, el desecho de dispositivos incorrectamente genera una serie de vulnerabilidades de seguridad, sin tomar las medidas adecuadas de protección de información puede causar daños irreversibles.

En la etapa final de los dispositivos se puede tomar en cuenta las siguientes sub etapas como:

- **Reciclaje. –** El aumento de dispositivos en gran cantidad con el pasar de los años, muchos elementos, componentes o materiales pueden ser de utilidad para otros dispositivos, lo que reduce la contaminación(Kozma et al., 2021).
- **Reúso. -** Eliminar la información de los dispositivos, actualizar el dispositivo a versiones adecuadas para su funcionamiento se puede realizar siempre y cuando el dispositivo esté en condiciones óptimas de operación para usarse nuevamente(Kozma et al., 2021)
- **Remano factura. -** La actualización de software no es suficiente, se requiere mejoras de calidad en el hardware(Kozma et al., 2021).
- **Retiro. –** En esta etapa el dispositivo es el final del ciclo de vida, borrar los datos antes de desechar los dispositivos es necesario para proteger la información(Soós et al., 2018).

Los problemas de seguridad al final del dispositivo permiten establecer una manera adecuada de desechar los dispositivos en la siguiente ilustración 18 ampliamos las vulnerabilidades presentes en el reusó y desmantelamiento de los dispositivos:

Ilustración 18.- Problemas de seguridad en la fase final de seguridad del ciclo de vida EOL



Fuente: modificado a partir de (Yousefnezhad et al., 2023)

Tabla 11.- Vulnerabilidades y medidas de prevención en la etapa final del dispositivo IoT

Vulnerabilidades • Obtención de datos sensibles como las claves, configuraciones, registros de actividad. • Eliminación de datos de forma insegura. • Reutilización o reciclaje de los dispositivos sin un método adecuado. • Dispositivos conectados en la red, al final de su vida útil objetos a ataques. • Falta de actualizaciones cuando un dispositivo ya no recibe soporte por parte del fabricante. • Filtración de información del dispositivo. • Desecho de dispositivos en lugares no confiables.
Medidas de mitigación • Proteger los dispositivos del comprador para la reutilización. • Establecer actualizaciones de claves y certificados para el nuevo usuario. • Cifrar los datos antes de ser eliminados. • Desactivar la conexión de la red de internet y retirar el acceso a los servicios de los dispositivos. • Invalidar las claves o certificados. • Restablecer los dispositivos a sus valores de fábrica. • Realizar un registro de los dispositivos retirados, como usuarios y contraseñas determinadas. • Reciclaje de dispositivos por empresas destinadas a proveer del servicio • Implementar políticas de seguridad para el soporte técnico, eliminación y reciclaje de los dispositivos.

Fuente: elaboración propia

La evaluación realizada en cada etapa MOL, BOL, EOL es seleccionada debido al análisis en modelos de seguridad IoT en cámaras ip y la revisión exhaustiva del ciclo de vida en dispositivos inteligentes, permite garantizar que su información adquirida es empleable y entendible por personal técnico para mejores prácticas de seguridad, tomando en cuenta que la información al final de la vida útil o su desecho es establecida mediante el desarrollo del presente documento.

Se ha establecido previamente que el ciclo de vida conlleva un proceso bidireccional, gracias al ciclo de vida de los dispositivos IoT podemos obtener información sobre los problemas de seguridad que pueden afectar al sistema y tomar medidas de precaución en cada una de sus etapas.

El creciente aumento de dispositivos IoT, se encuentran expuestos a ataques de infiltración de información sin encontrar soluciones de seguridad que afectan a dispositivos inteligentes, cámaras ip, electrodomésticos, hogares inteligentes, persianas, aire acondicionado, televisores Smart tv, etc.

Para determina las soluciones de seguridad determinadas en cada fase a lo largo de operación del ciclo de vida, en cada una de las ilustraciones antes descritas se pueda destacar los requisitos de seguridad aplicables en la etapa inicial (BOL) y de uso nominal (MOL), las cuales se clasifican en:

- **Autenticación. –** Permite que solo los dispositivos autorizados puedan autenticarse a un servicio en específico, con el propósito de enviar y recibir información hacia su destino. Un elemento de autenticación puede ser simplemente una contraseña.
- **Confidencialidad. –** Encargada de mantener la información adecuada y reservada contra accesos no autorizados, si la información es vulnerada puede ser determinada por contraseñas expuestas por un usuario o los administradores, permitiendo el acceso a la información que netamente debe ser confiable.
- **Integridad. –** La información debe mantener su originalidad como su destino de donde proviene.
- **Disponibilidad. –** Los datos deben estar disponibles para el personal autorizado siempre que lo requieran, con los permisos previamente obtenidos.
- **No repudio. –** Determina que los datos obtenidos comprendan que la fuente de destino pueda o no negar la información, la información es verificada si realmente es enviada por su origen o destino.
- **Control de acceso. –** Normalmente es el control físico o lógico de los dispositivos del usuario, con el fin de proteger la información antes de los accesos no autorizado por terceros.

Dichos ataques de seguridad pueden afectar notablemente a cada una de fases estudiadas previamente, no obstante en la bibliografía sobre la seguridad en cada una de las fases del ciclo de vida no está definida de manera específica o en su totalidad no consta con los datos requeridos por el constante cambio en la tecnología, en la mayoría de los artículos no establece medidas de seguridad durante todo el ciclo de vida, es necesario encontrar o determinar en cada etapa las vulnerabilidades y medidas de mitigación en modelos de seguridad IoT dado

que su evaluación se realizara en cámaras Ip de manera específica para determinar cada uno los procesos en la gestión de seguridad de dichos dispositivos.

Con la finalidad de elaborar una guía adecuada de los problemas que se presenten, con el propósito de determinar medidas viables de seguridad en cada una de las etapas desde su producción, implementación hasta la eliminación.

Fase III: Elaboración del documento final

La elaboración del documento final del presente proyecto de investigación, se determina en el Capítulo III en el cual se plantea el modelo de gestión de seguridad del ciclo de vida en dispositivos a lo largo del modo de operación o su vida útil mediante procedimientos respectivos aplicado a dispositivos IoT en cámaras ip factible para diferentes modelos y fabricantes, mediante una serie de pasos para que el personal técnico emplee y obtenga conocimientos sobre el ciclo de vida que puede llevar un dispositivo en este caso cámaras ip, con el propósito de implementar un modelo de gestión para prevenir vulnerabilidades y medidas de prevención.

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

Luego de determinar cada una de las vulnerabilidades, medidas de mitigación durante el ciclo de vida de los dispositivos IoT, aplicado en cámaras IP dado la información obtenida en los modelos de seguridad en el capítulo I, se llevó a cabo un modelo de gestión de seguridad por medio de un conjunto de procedimientos y recomendaciones prácticas para gestionar la seguridad en cada una de las etapas determinadas.

3.1. Propuesta del modelo de gestión de seguridad en el ciclo de vida en dispositivos IoT (cámaras ip)

Para establecer una manera administrable sobre la seguridad aplicable en cámaras ip es primordial determinar los procedimientos adecuados antes de desarrollar un conjunto de procedimientos durante el ciclo de vida de las cámaras de seguridad.

Cada fase del ciclo de vida permite identificar una planificación detallada para garantizar que los dispositivos consten con las medidas adecuadas de seguridad.

El modelo aplicado en el ciclo de vida de las cámaras ip, entabla una relación para el personal técnico adquiera información relevante sobre la necesidad de generar confianza al momento de su implementación en hogares domésticos de dispositivos de diferente fabricantes y modelos, se puede definir en la siguiente ilustración 19:

Ilustración 19.- Ciclo de vida de los dispositivos IoT (cámaras ip)

Fuente: elaboración propia

Dado que cada una de las fases y las categorías del ciclo de vida de los dispositivos ex extensa, se establece un conjunto de procedimientos en las etapas principales las mismas que especifiquen de una manera clara**,** concisa y pueda ser entendible por el personal técnico antes de adquirir o implementar cámaras ip en hogares, en la fabricación se determina los requisitos de seguridad y su escalabilidad a largo plazo, su despliegue una vez el dispositivo sea adquirido por el personal técnico se implementan de manera física con la respectiva conexión a la red , asignando sus identificaciones y configuraciones únicas en el entorno a emplearse.

Sin embargo el monitoreo y mantenimiento permiten garantizar que los dispositivos funcionen de manera adecuada y correcta, las brechas de seguridad se debe identificar con la mayor brevedad posible para evitar perdida de información, las actualizaciones deben realizarse periódicamente para mantenerlos activos y funcionales, la gestión de seguridad una vez terminado su periodo de operación de cada dispositivo como las cámaras IP se deben realizar de manera adecuada, eliminar la información de manera correcta permite que el dispositivo sea reutilizado o desechado completamente tomando en cuenta que los dispositivos deben ser eliminados a través de entidades responsables de desechos electrónicos.

El desarrollo de un modelo de seguridad confiable y seguro no se puede establecer en su totalidad que sea eficiente debido al aumento y evolución de los dispositivos en el mercado, el presente modelo permite que en su mayoría se pueda determinar un conjunto de procedimientos mediante cámaras ip en forma general para que el personal técnico tengan en consideración cada una de las etapas de los dispositivos antes de ser expuestos e implementados y que evite en lo posible mitigar las amenazas de seguridad que pueda suceder durante su ciclo de vida y pueda afectar al sistema.

A continuación, se presenta un modelo de gestión de seguridad basado en las mejores prácticas y riesgos identificados en el capítulo I que determina información sobre el ciclo de vida que conlleva un dispositivo, seguridad y vulnerabilidades presentes en modelos de seguridad en cámaras ip.

En el capítulo II permite determinar y evaluar cada etapa del ciclo de vida así como las amenazas y medidas de prevención en cada una de ellas, con el único objetivo de planificar, identificar y controlar los procedimientos en el ciclo de vida den los dispositivos basados cámaras ip de manera centralizada y sea accesible la información al personal técnico que requiera poseer conocimientos sobre como interactúa en cada una de las fases ciclo de vida de las cámaras que son instaladas en hogares domésticos y lo que conlleva implementar o conocer medidas de seguridad.

Un modelo practico permite al personal técnico tener conocimiento sobre el proceso que conlleva los dispositivos IoT a lo largo de su vida útil, en la etapa de fabricación el personal técnico no posee conocimiento directo sobre el diseño de los dispositivos que están adquiriendo, sin embargo, en el siguiente modelo en la tabla 12 se aborda un conocimiento general que pueda realizar al momento de comprar un dispositivo disponible en el mercado

Tabla 12.- Modelo de gestión de seguridad para dispositivos IoT en cámaras Ip

Adquisición **Objetivo:** Determinar que las cámaras ip cumplan con los requisitos de seguridad desde su fabricación.
1. Valoración de riesgos en el diseño, arquitectura y construcción de los dispositivos. 2. Manejo de credenciales predefinidas, exclusivas y seguras 3. Verificar que el dispositivo posea protocolos de comunicación seguro (EST-TSL/SSL, Mqtt, etc). 4. Adquirir dispositivos de marcas reconocidas que cumplan con las normativas de seguridad o certificaciones especificas (ISO 27001, ZIGBEE, LoRaWAN, GSMA,etc). 5. Verificar que los dispositivos permitan actualizaciones de firmware, mecanismo de doble autenticación y encriptación. 6. Identificar que las credenciales como usuarios y contraseñas sean accesibles, seguras y permitan realizar cambios en su configuración inicial 7. Permita incorporar sistemas de verificación, autenticación multifactor y cifrado de contraseñas criptográficas. 8. Actualización de firmware y software seguros mediante paginas determinadas por el fabricante. 9. Permita plataformas administrables determinadas por el fabricante (Gdmss lite, hik-connect, tapo care) 10. Permita establecer seguridad el respaldo de la información.
DESPLIEGUE **Objetivo:** Determinar controles de seguridad desde su uso.
1. Leer las guías establecidas por los fabricantes para la implementación y seguridad de cámaras ip.

2. Cambiar la configuración de credenciales predeterminadas en la cámara ip y en su aplicación.
3. Establecer una guía de implementación de cámaras ip.
4. Configuración inicial segura de los dispositivos de manera adecuada según las instrucciones del fabricante.
5. Aplicar contraseñas de al menos 8 caracteres alfanuméricos.
6. Desactivar puertos o servicios innecesarios.
7. Establecer medidas de acceso con un privilegio de autenticación mínima.
8. Establecer requisitos de seguridad en la conectividad de los dispositivos
9. Establecer una guía práctica de red segura.
10. Realizar una conexión VPN para encriptar y ocultar la información de la dirección ip del dispositivo.
11. No permitir actualizaciones de firmware o software de sitios no oficiales.
12. Ingresar por direcciones URL únicas determinadas para el control del dispositivo.
13. Aplicar las nuevas actualizaciones firmware, parches de seguridad, certificados digitales
14. Realizar Backus de información de las tarjetas físicas de manera manual.
15. No ingresar a enlaces enviados por correo electrónico sin corroborar la información establecida por el fabricante

MONITOREO Y MANTENIMIENTO

Objetivo: Determinar actividades sospechosas y medidas de respuesta ante posibles fallos de seguridad o del dispositivo.

1. Actualizar el firmware y software de los dispositivos disponibles en las páginas oficiales de los fabricantes.
2. Confirmar la identidad de los dispositivos a través de las credenciales del usuario.
3. Establecer cambios de contraseñas multifactor de manera periódica.
4. Establecer sistemas de alerta ante incidentes y respuesta.
5. Identificar medidas de seguridad mediante auditorias periódicas.
6. Seleccionar cifrados adecuados para el dispositivo IoT (WPA2, WPA3, RSA, AES, etc.)
7. Administrar incidentes frente a problemas de seguridad.
8. Gestionar accesos de autenticación.
9. Permitir el monitoreo de amenazas y vulnerabilidades.
10. Monitorear el tráfico en la red e identificar el número de dispositivos conectados.
11. Determinar control de accesos y permisos para limitar el acceso de personas no deseables.
12. Formatear la información de manera periódica.
13. Realizar mantenimientos preventivos de limpieza para prevenir daños del dispositivo y realizar el desecho del mismo.
14. Desconectar el dispositivo de la red si detecta actividad sospechosa.

RETIRO

Objetivo: Prevenir filtraciones de información al momento de retirar el dispositivo

1. Restablecer a la configuración de fábrica una vez eliminado toda la información de la cámara ip.
2. Establecer mecanismos de *backup* de la información respaldados en los dispositivos.
3. Determinar avisos a los usuarios que el dispositivo no recibirá soporte de actualizaciones o asistencia técnica de seguridad por falta de disponibilidad del mismo.
4. Invalidar las claves o actualizaciones no seguras en los dispositivos.
5. Implementar guías y medidas de seguridad si el dispositivo requiere ser reutilizado.
6. Establecer una guía de desecho de dispositivos de manera responsable para prevenir riesgos ambientales y de seguridad.

Fuente: modificado a partir de (Ribero-Corzo & Prieto-Guerrero, 2021)

La tabla 12 establece un modelo de gestión de seguridad aplicable determinado a partir de los requerimientos de los dispositivos en cámaras ip, basado en el análisis del capítulo I en modelos de seguridad IoT y su factibilidad es determinada por la investigación de (Ribero-Corzo & Prieto-Guerrero, 2021).

Una vez adquirido el conocimiento del ciclo de vida que presentan los dispositivos IoT, permite identificar y clasificar los procesos en cada etapa de las cámaras ip, desde su diseño hasta su retiro con las medidas de prevención de seguridad para mitigar las amenazas que presentan los dispositivos IoT en cámaras IP.

Las empresas proveedoras de dispositivos IoT como cámaras de seguridad deben determinar procedimientos necesarios para evaluar la seguridad en el dispositivo disponible en el mercado antes de su despacho o puesta en marcha. Los procedimientos adquiridos durante cada etapa del ciclo de vida permiten determinar la confiabilidad del modelo de gestión a implementar.

Es importante desarrollar un modelo para casos prácticos en hogares inteligentes, así como un conjunto de procedimientos para el personal técnico antes de adquirí los dispositivos IoT basados en cámaras Ip, con el propósito de satisfacer los requisitos de seguridad básicos, sobre dispositivos de uso común presentes hogares domésticos que garanticen en lo posible la gestión de seguridad.

Realizar la configuración de cámaras ip en hogares domésticos requiere una serie de pasos de manera minuciosa para garantizar la seguridad de la información y mejorar la eficiencia para adaptarse a nuevos cambios a lo largo de los años. Una manera viable de evitar riesgos de seguridad es configurar una Red segura porque es el primer paso para la defensa de los dispositivos que vayan a ser implementados en un entorno seguro y el personal técnico adquiera guías de seguridad para la red doméstica.

Tabla 13.- Guía práctica para configurar una red segura, aplicable a hogares inteligentes

Configuración del Router:
1. Ingresar a la dirección IP determinada por defecto en la parte posterior del equipo (192.168.0.1/192.168.1.1)
2. Iniciar la sesión con las credenciales del router que se encuentran etiquetadas en el dispositivo ejemplo (usuario: admin, password: admin)
3. Cambiar las credenciales de usuario y contraseña: como recomendación claves complejas.
4. Evitar el uso de SSID (identificación de la red) con nombres relacionados a IoT.
5. Ocultar en lo posible el SSID del router.
6. Activar la opción aislamiento de cliente para evitar comunicaciones entre dispositivos.
7. Habilitar una red wifi de invitados separada para conectar dispositivos IoT.
8. Activas el cifrado WPA2 o WPA3(permite proteger los datos transmitidos en la red).
9. Desactivar el modo WPS, debido a que es vulnerable ataques.
10. Configurar un DNS seguro.
11. Actualizar el firmware del router para evitar fallos de seguridad

Fuente: elaboración propia

3.2. Validación del modelo de gestión de seguridad

Para evaluar el modelo de gestión de seguridad nos enfocaremos en dispositivos en hogares inteligentes dado que el número de dispositivos IoT es extenso nos enfocaremos como caso práctico de estudio en las cámaras ip conectadas a la red, presentan vulnerabilidades por su facilidad de acceso a la red a través de internet por medio del router doméstico sino se emplea medidas adecuadas de seguridad, las cámaras ip graban contenido de manera bidireccional debido al intercambio de información entre video y audio en muchos de los casos en tiempo real.

La mayoría del personal técnico que se dedica a la instalación de cámaras ip no implementan medidas de seguridad al momento de ser instaladas, adquiridos o mucho menos tienen una guía de cómo implementarlo y en el peor de lo casos no tienen conocimiento sobre los procedimientos que conllevan durante su ciclo de vida de los dispositivos al momento de ser implementados, dejando a la deriva la información necesaria como las especificaciones técnicas, medidas de seguridad, guías de instalación, guías de configuración de la red doméstica, etc optando por no cambiar en su mayoría como las claves predeterminadas.

Con la finalidad de evaluar el modelo de gestión de seguridad, se establece una serie de preguntas como se establece en el anexo 1 detallando las partes más elementales a lo largo de la vida útil de las cámaras Ip para que el personal técnico

tengan conocimiento al momento de adquirir una cámara ip sobre los procesos necesarios y no tan extensos al momento de comprar cámaras ip disponibles en el mercado, dicho modelo de gestión permite identificar las medidas de prevención necesarias en los dispositivos IoT antes o después de su uso.

Para evaluar el modelo de gestión de seguridad, se realiza de manera teórica debido a que las investigaciones enfocadas en cámaras ip son validadas en su desarrollo.

Un caso de estudio donde los autores(Ospina Rodríguez, 2024a) establecen un modelo de autenticación de seguridad en cámaras ip mediante la tecnología *Blockchain* con la finalidad de detectar brechas de seguridad en dispositivos por fabricantes distintos, tomando como referencia un solo modelo en específico para evaluar las medidas de seguridad. Gracias al estudio realizado podemos determinar las características del dispositivo y las medidas prevención disponibles que dispone en su configuración inicial desde parámetros de actividad hasta protocolos de seguridad provee la información requerida para su evaluación.

Tabla 14.- Modelo de evaluación de gestión de seguridad aplicado a cámaras Ip

Nombre del dispositivo:		
ADQUISICION		
Preguntas	**SI**	**NO**
1. El dispositivo adquiere protocolos de comunicación seguro (EST-TSL/SSL, Mqtt, etc)?		
2. ¿EL dispositivo cumpla con normativas de seguridad o certificaciones especificas?		
3. El dispositivo permite actualizaciones de firmware, mecanismo de doble autenticación y encriptación.		
4. ¿Permite gestionar las contraseñas en su configuración?		
5. ¿Adquiere plataformas administrables de forma segura y eficiente?		
DESPLIEGUE		
1. ¿Permite contraseñas de al menos 12 caracteres entre letras, números y símbolos?		
2. ¿Permite desactivar funciones innecesarias si no son requeridas (accesos remotos o sonido)?		

3. ¿Permite deshabilitar protocolo y servicios inseguros?		
4. ¿Permite eliminar accesos excesivos en aplicaciones?		
MONITOREO Y MANTENIMIENTO		
1. ¿Permite confirmar la identidad de los dispositivos a través de las credenciales del usuario?		
2. ¿Permite establecer contraseñas multifactor?		
3. ¿Puede enviar información sobre las actualizaciones si se encuentra disponibles?		
4. ¿Permite el control de acceso y permisos para limitar el acceso a terceras personas?		
RETIRO		
1. El dispositivo puede desconectarse de la red, cambiar credenciales predeterminar, ¿restaurar valores de fábrica y eliminar la información de manera segura?		

Fuente: elaboración propia

El modelo establecido para la evaluación en la tabla 15 de manera específica evalúa y adquiere información relevante al tema, determina su resultado en investigaciones relacionadas a cámaras ip y mediante un conjunto de procedimientos previamente analizados en la tabla 15, en las cuales se analiza los requerimientos como especificaciones técnicas, instalación y modos de seguridad.

Tabla 15.- Evaluación de las características de seguridad del dispositivo DS-2CV2Q21FDIW de hikvision

Nombre del dispositivo: DS-2CV2Q21FDIW HIKVISION		
ADQUISICION		
Pregunta	**SI**	**NO**
1. El dispositivo adquiere protocolos de comunicación seguro (EST-TSL/SSL, Mqtt, etc.)?		**X**
2. ¿EL dispositivo cumpla con normativas de seguridad o certificaciones especificas?		X
3. ¿El dispositivo permite actualizaciones de firmware, mecanismo de doble autenticación y encriptación?		X
4. ¿Permite gestionar las contraseñas en su configuración?	X	
5. ¿Adquiere plataformas administrables de forma segura y eficiente?	X	
DESPLIEGUE		
1. ¿Permite contraseñas de al menos 12 caracteres entre letras, números y símbolos?		X

2. ¿Permite desactivar funciones innecesarias si no son requeridas (accesos remotos o sonido)?		X
3. ¿Permite deshabilitar puertos y servicios inseguros?	X	
4. ¿Permite eliminar accesos excesivos en aplicaciones?	X	
MONITOREO Y MANTENIMIENTO		
¿Permite confirmar la identidad de los dispositivos a través de las credenciales del usuario?		X
¿Permite establecer contraseñas multifactor?		X
¿Puede enviar información sobre las actualizaciones si se encuentra disponibles?		X
¿Permite el control de acceso y permisos para limitar el acceso a terceras personas?	X	
RETIRO		
El dispositivo puede desconectarse de la red, cambiar credenciales predeterminadas, restaurar valores de fábrica y eliminar la información de manera segura	X	

Fuente: evaluación de la cámara ip DS-2CV2Q21FDIW Hikvision tomado a partir de (Ospina Rodríguez, 2024b)

El estudio realizado para determinar las brechas de seguridad en la cámara Ip DS-2CV2Q21FDIW de hikvision, no define en su mayoría los procedimientos adecuados para utilizar dicho dispositivo durante su ciclo de vida y no posee las características en cada etapa determinadas con el propósito de establecer fallos y medidas de prevención de seguridad, la falta de información sobre gestionar las contraseñas, plataformas administrables inseguras, eliminar puertos inseguros o control de acceso por terceras personas, son campos propicios para ataques de seguridad y no posee una guía adecuada de implementación o conocimientos específicos para que el personal técnico administre de manera segura.

Dado los fabricantes de cámaras ip puentes ser de distintas marcas como hikvision y dahua son las marcas reconocidas disponibles y al alcance de las personas en el mercado dedicado a la venta y distribución de modelos administrables de seguridad es aplicable a cualquier dispositivo IoT en específico a cámaras ip provenientes de cualquier modelo previamente mencionadas y valorada en la investigación del presente proyecto.

Evaluaremos el modelo de gestión en una cámara ip del modelo TPLINK (modelo tapo c310) (*TP-Link*, s. f.)para establecer la diferencia entre ambos dispositivos y determinar la cámara ip con las mejores especificaciones y condiciones de seguridad antes de ser implementado en un entorno seguro y que posea en su mayoría los procedimientos adecuados desde su adquisición del equipo hasta su retiro para su respectiva operación.

Una vez establecido el modelo de seguridad para gestionar los diferentes modelos de cámaras ip, el modelo de gestión de manera específica evaluaremos con una cámara ip en especifica TP-LINK (TAPO C310), dado que en la actualidad el personal técnico por lo regular adquiere cámaras de seguridad sin prever muchos aspectos de seguridad o no poseen una idea clara y precisa de lo que conlleva adquirir dichos dispositivos desde su compra.

La evaluación de la cámara ip en la tabla 16, determina los requerimientos necesarios útiles y viables para en lo posible mitigar posibles fallos de seguridad antes de ser implementados por el personal técnico, para ello se realiza su respectivo modelo de gestión de seguridad por medio de cinco etapas:

Tabla 16.- Modelo de gestión de seguridad mediante las especificaciones técnicas de la cámara ip (TAPO C310-TPLINK)

ADQUISICION
1. Adquirir cámaras ip TPLINK en distribuidores oficiales para evitar falsificación de dispositivos. 2. Proporciona actualizaciones de firmware. 3. Utiliza cifrado de datos para la transmisión AES de 128bits con seguridad SSL/TLS, WPA/WPA2-PSK/WPA3 4. Permite almacenamiento seguro en tarjetas internas micro SD o en la nube. 5. Aplicación administrable de forma local y en la web(app TAPO CARE) 6. Doble factor de autenticación. 7. Protocolo de seguridad IoT. 8. Cuenta con certificación ISO 27001/27701.
DESPLIEGUE
1. Autentifica el dispositivo por medio de correo electrónico antes de su instalación 2. Permite cambiar las credenciales predeterminadas por contraseñas robustas 8 caracteres alfanuméricos. 3. Se puede instalar la cámara a 2-3 metros de altura para maximizar la visión y evitar la manipulación física. 4. Permite Desactivar puertos no requeridos como UPnP y WPS.

5. Permite Conectar a una red wifi distinta solo para dispositivos IoT. 6. Activar el cifrado WPA3 o WPA2 como cifrado para wi-fi. 7. Limita el acceso remoto solo si es requerido. 8. Permite configurar el almacenamiento local o en la nube tomando en cuenta que datos se van a compartir. 9. Permite cifra el almacenamiento de tarjeta microSD. 10. Permite activar las notificaciones de actualización de firmware.
MONITOREO Y MANTENIMIENTO
1. Confirma la identidad del dispositivo a través de sus credenciales determinadas. 2. Permite cambiar las contraseñas de red wifi, aplicación tplink. 3. Verifica las actualizaciones disponibles. 4. Activa la sirena de detección de movimiento si es requerida. 5. Habilita el modo de actualizaciones de firmware de forma manual o automática. 6. Verifica la integridad de la información guardada. 7. Recomienda formatear la información de manera periódica. 8. Establece alertas y registros de acceso mediante los logs. 9. Permite revisar que la IP de la cámara no esté en uso en otro dispositivo a través del router. 10. Utilizar herramientas de monitoreo para dispositivos conectados (FING).
RETIRO
1. Permite restablecer a valores de fabrica antes de su reutilización o venta. 2. Borra toda la información almacenada de manera local y en la nube. 3. Permite eliminar el dispositivo de la cuenta de tplink. 4. Si el dispositivo no posee actualizaciones, envía una notificación por medio de correo electrónico. 5. Es reemplazable una vez borrada toda la información es decir establecida a sus valores de fábrica.

Fuente: tomado a partir de (TP-Link, s. f.)

El presente modelo de gestión aplicado a cámaras ip TPLINK (TAPO C310) permite tener una idea clara del dispositivo a lo largo de su modo de operación de su vida útil desde su compra o implementación hasta el retiro del equipo donde se ha colocado, permite identificar los procedimientos necesarios para implementar y mitigar en lo posible las falencias de seguridad previamente estudiadas durante cada etapa, con la finalidad de que el personal técnico adquiera este tipo de cámaras ip por poseer todos los requerimientos de seguridad y medidas de implementación en un ambiente adecuado.

Tabla 17.- Evaluación de las características de seguridad del dispositivo TAPO C310 de tplink

Nombre del dispositivo: TAPO C310 TPLINK		
ADQUISICION		
Preguntas	**SI**	**NO**
1. El dispositivo adquiere protocolos de comunicación seguro (EST-TSL/SSL, Mqtt,etc)?	X	
2. ¿EL dispositivo cumpla con normativas de seguridad o certificaciones especificas?	X	
3. ¿El dispositivo permite actualizaciones de firmware, mecanismo de doble autenticación y encriptación?	X	
4. ¿Permite gestionar las contraseñas en su configuración?	X	
5. ¿Adquiere plataformas administrables de forma segura y eficiente?	X	
DESPLIEGUE		
1. ¿Permite contraseñas de al menos 12 caracteres entre letras, números y símbolos?	X	
2. ¿Permite desactivar funciones innecesarias si no son requeridas (accesos remotos o sonido)?	X	
3. ¿Permite deshabilitar puertos y servicios inseguros?	X	
4. ¿Permite eliminar accesos excesivos en aplicaciones?	X	
MONITOREO Y MANTENIMIENTO		
5. 1. ¿Permite confirmar la identidad de los dispositivos a través de las credenciales del usuario?	X	
2. ¿Permite establecer contraseñas multifactor?	X	
3. ¿Puede enviar información sobre las actualizaciones si se encuentra disponibles?	X	
4. ¿Permite el control de acceso y permisos para limitar el acceso a terceras personas?	X	
RETIRO		
1. El dispositivo puede desconectarse de la red, cambiar credenciales predeterminadas, ¿restaurar valores de fábrica y eliminar la información de manera segura?	X	

Fuente: elaboración propia determinada a partir de las especificaciones técnicas de la cámara ip (TAPO C310)(*TP-Link*, s. f.).

Si establecemos un modelo de seguridad antes de adquirir un dispositivo para hogares inteligentes, podemos determinar la viabilidad del modelo aplicable a cualquier dispositivo IoT basados en cámaras ip de cualquier fabricante, desde la verificación de especificaciones técnicas por parte del fabricante desde gestión de

dispositivos conectados a la red, cambio de contraseñas, certificaciones internacionales, actualizaciones seguras, verificación de identidad, contraseñas multifactor, protocolo IoT, certificaciones internacionales mecanismos de seguridad, etc.

Mediante el empleo de guías prácticas de instalación y configuración de la red domiciliaria, permite solventar problemas de seguridad en cada una de las fases del ciclo de vida de las cámaras ip, red wifi del hogar y medidas de prevención durante y después de la vida útil del dispositivo.

Determina un modelo de gestión de seguridad eficiente capaz de determinar cada uno de los procesos en las fases del ciclo de vida, garantizando de mejor manera la disponibilidad de adquirir dispositivos antes de su compra.

Es rentable establecer un modelo de gestión de seguridad con procedimientos específicos antes de ser implementado por el personal técnico para la prevención de seguridad en ambientes adecuados garantizando que el personal técnico adquiera información relevante del proceso del ciclo de vida, medias de seguridad que poseen las cámaras ip incluidas en el mercado, dando la seguridad confiabilidad, integridad y disponibilidad de implementar el modelo de gestión de seguridad aplicado a dispositivos IoT específicamente a cámaras ip para prevenir una serie de vulnerabilidades presentes en el medio que se propagan.

CONCLUSIONES

- La revisión bibliográfica exhaustiva ha permitido establecer un determinado conjunto de procesos en las fases del ciclo de vida de los dispositivos IoT, y su importancia durante y después de la vida útil de los dispositivos, arrojando problemas de seguridad y medidas de prevención durante cada una de ellas.

- La elaboración del modelo de gestión de seguridad aborda la seguridad de los dispositivos durante todo el ciclo de vida, mediante guías de seguridad como la segmentación de la red wifi para evitar acceder a la información personal en la red principal o la red de invitados exclusiva para IoT.

- La evaluación del modelo de gestión de seguridad permite obtener información relevante y necesaria antes de adquirir un dispositivo en el mercado, durante este proceso permite validar la veracidad de la información que necesita el personal técnico al adquirir el dispositivo, determinando las vulnerabilidades y las medidas prevención para garantizar la gestión de seguridad.

- El mantenimiento de los dispositivos se realiza de manera continua, desde aplicaciones móviles, actualizaciones seguras, cambios de credenciales de manera periódica, autenticación multifactor y la eliminación de dispositivos de manera correcta es clave para la protección de información a largo plazo.

RECOMENDACIONES

- Comprar dispositivos IoT de manera segura en sitios autorizados y que contengan especificaciones técnicas ante posibles fallas de seguridad en el sistema o al menos información relevante sobre la durabilidad, confiabilidad, disponibilidad e integridad de la información.

- Dado el aumento de los dispositivos IoT es importante actualizar la información de cada dispositivo en el mercado desde sus actualizaciones hasta el tiempo de vida para identificar fallas de seguridad.

- Incorporar el término ciclo de vida en dispositivos IoT en las investigaciones es de gran ayuda con el objetivo de establecer valoraciones de seguridad y medidas de prevención empleables a cualquier dispositivo.

- Implementar sistemas de monitoreo continuo en hogares inteligentes o firmwares domésticos para detectar amenazas y responder ante ellas de manera eficiente. Como herramientas *Fing, glasswire, shodan*, etc.

- Configurar los dispositivos desde un inicio desde claves robustas, desactivación de puertos innecesarios, creación de redes separadas e inclusive revisión mensual del acceso de los dispositivos.

- Realizar un estudio en diferentes dispositivos IoT ya sea en la industria o en hogares domésticos.

- Finalmente establecer un modelo de gestión de seguridad accesibles para personas que poseen cámaras ip en sus hogares, de fácil comprensión e instalación del mismo.

BIBLIOGRAFÍA

Ali, B., & Awad, A. I. (2018). Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors*, *18*(3), Article 3. https://doi.org/10.3390/s18030817

Alrawi, O., Antonakakis, M., & Monrose, F. (2019, mayo). *SoK: Security Evaluation of Home Based IoT Deployments*. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8835392&utm_source=sciencedirect_contenthosting&getft_integrator=sciencedirect_contenthosting

Ameyed, D., Jaafar, F., Petrillo, F., & Cheriet, M. (2023). Quality and Security Frameworks for IoT-Architecture Models Evaluation. *SN Computer Science*, *4*(4), 394. https://doi.org/10.1007/s42979-023-01815-z

Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015). Internet of Things: Security vulnerabilities and challenges. *2015 IEEE Symposium on Computers and Communication (ISCC)*, 180-187. https://doi.org/10.1109/ISCC.2015.7405513

Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K. N., Nadeau, E., O'Rourke, D. G., Piccarreta, B., & Scarfone, K. (2021). *Consideraciones para la gesti n de riesgos a la ciberseguridad y la privacidad de internet de las cosas (IoT)* (NIST IR 8228es; p. NIST IR 8228es). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.IR.8228es

Borsato, M. (2014). Bridging the gap between product lifecycle management and sustainability in manufacturing through ontology building. *Computers in Industry*, *65*(2), 258-269. https://doi.org/10.1016/j.compind.2013.11.003

Burhan, M., Rehman, R. A., Khan, B., & Kim, B.-S. (2018a). IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors*, *18*(9), 2796. https://doi.org/10.3390/s18092796

Burhan, M., Rehman, R. A., Khan, B., & Kim, B.-S. (2018b). IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors*, *18*(9), Article 9. https://doi.org/10.3390/s18092796

Carmona, M., & Antonio, P. (2019). *Seguridad en los ecosistemas IoT*.

Cavalcante, J., & Gzara, L. (2018). Product-Service Systems lifecycle models: Literature review and new proposition. *Procedia CIRP*, *73*, 32-38. https://doi.org/10.1016/j.procir.2018.03.324

Chen, F., Xiao, Z., Xiang, T., Fan, J., & Truong, H.-L. (2023). A Full Lifecycle Authentication Scheme for Large-Scale Smart IoT Applications. *IEEE Transactions on Dependable and Secure Computing*, *20*(3), 2221-2237. IEEE Transactions on Dependable and Secure Computing. https://doi.org/10.1109/TDSC.2022.3178115

Cisneros, X. A. G., & Jacome, D. J. R. (2025). Ciberseguridad en los dispositivos IOT de uso doméstico: Una Revisión Sistemática de la Literatura. *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS*, *7*(1), 140-170. https://doi.org/10.59169/pentaciencias.v7i1.1371

Darwish, D. G., & Square, E. (2015). *Improved Layered Architecture for Internet of Things*. *4*(4).

DS-2CD2441G0-I(W). (s. f.). Hikvision. Recuperado 3 de abril de 2025, de http://www.hikvision.com/hu/products/IP-Products/Network-Cameras/Pro-Series-EasyIP-/ds-2cd2441g0-i-w-/

Enisa. (2018). *IoT security standards gap analysis: Mapping of existing standards against requirements on security and privacy in the area of IoT.* Publications Office. https://data.europa.eu/doi/10.2824/713380

Evans, D. (2011). *La próxima evolución de Internet lo está cambiando todo*.

Hernando, E. S. (2015). *CICLO DE VIDA DE PRODUCTO. MODELOS Y UTILIDAD PARA EL MARKETING*. 207-227.

IoT en América Latina: En 2023 habrá 996 millones de dispositivos conectados. (s. f.). Revista Innovación Seguridad. Recuperado 18 de febrero de 2025, de http://revistainnovacion.com/nota/11961/iot_en_america_latina_en_2023_habra_996_millones_de_dispositivos_conectados/

ISO-IEC-30147-2021.pdf. (s. f.). Recuperado 11 de marzo de 2025, de https://cdn.standards.iteh.ai/samples/53267/9e4a11b73e994b539fb202a9342c81e6/ISO-IEC-30147-2021.pdf

Jumbo, E., Llumiquinga, J., Uyaguari, F., Tenezaca, A., Pazmiño, L., & Rivera, R. (2023). Un breve Análisis de Vulnerabilidades en dispositivos IOT en Ecuador. *Ciencia Latina Revista Científica Multidisciplinar*, *7*(2), 5939-5953. https://doi.org/10.37811/cl_rcm.v7i2.5763

Kamalakkannan, S., Kulatunga, A. K., & Bandara, L. A. D. A. D. (2020). The conceptual framework of IoT based decision support system for life cycle management. *Procedia Manufacturing*, *43*, 423-430. https://doi.org/10.1016/j.promfg.2020.02.192

Karale, A. (2021). The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. *Internet of Things*, *15*, 100420. https://doi.org/10.1016/j.iot.2021.100420

Kärkkäinen, M., Holmström, J., Främling, K., & Artto, K. (2003). Intelligent products—A step towards a more effective project delivery chain. *Computers in Industry*, *50*(2), 141-151. https://doi.org/10.1016/S0166-3615(02)00116-1

Kiritsis, D., Bufardi, A., & Xirouchakis, P. (2003). Research issues on product lifecycle management and information tracking using smart embedded systems. *Advanced Engineering Informatics*, *17*(3), 189-202. https://doi.org/10.1016/j.aei.2004.09.005

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and Other Botnets. *Computer*, *50*(7), 80-84. https://doi.org/10.1109/MC.2017.201

Kozma, D., Varga, P., & Larrinaga, F. (2021). System of Systems Lifecycle Management—A New Concept Based on Process Engineering Methodologies. *Applied Sciences*, *11*(8), 3386. https://doi.org/10.3390/app11083386

Kozma, D., Varga, P., & Larrinaga, F. (2024). (PDF) System of Systems Lifecycle Management—A New Concept Based on Process Engineering Methodologies. *ResearchGate*. https://doi.org/10.3390/app11083386

Li, B. (2019). Efficiency Optimization for Communication Service Based on QoS Technology. *IEEE Access*, *7*, 48838-48848. https://doi.org/10.1109/ACCESS.2019.2910189

Li, X., Xu, L. D., Sigov, A., Ratkin, L., & Ivanov, L. a. (2025). Enterprise architecture of IoT-based applications: A review. *Future Generation Computer Systems*, *166*, 107584. https://doi.org/10.1016/j.future.2024.107584

Mazon-Olivo, B., & Pan, A. (2022). Internet of Things: State-of-the-art, Computing Paradigms and Reference Architectures. *IEEE Latin America Transactions*, *20*(1), 49-63. IEEE Latin America Transactions. https://doi.org/10.1109/TLA.2022.9662173

Miettinen, M., Asokan, N., Nguyen, T. D., Sadeghi, A.-R., & Sobhani, M. (2014, noviembre 3). *Context-Based Zero-Interaction Pairing and Key Evolution for Advanced Personal Devices | Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. https://dl.acm.org/doi/10.1145/2660267.2660334

Miettinen, M., Oorschot, P. C. van, & Sadeghi, A.-R. (2018). *Baseline functionality for security and control of commodity IoT devices and domain-controlled device lifecycle management* (arXiv:1808.03071). arXiv. https://doi.org/10.48550/arXiv.1808.03071

Mohamed, R., Meyer, S., & Bohnet, D. (2024). Environmental Impact Assessment of IoT Devices: A Graph-based Approach. *Procedia Computer Science*, *236*, 338-347. https://doi.org/10.1016/j.procs.2024.05.039

Molina, J. (2019). *La importancia de la gestión de riesgos y seguridad en el internet de las cosas (IOT)*. http://repository.unipiloto.edu.co/handle/20.500.12277/6754

Ospina Rodriguez, F. E. (2024a). *Modelo de autenticación mediante blockchain Ethereum para mitigar las brechas de seguridad en las cámaras IoT del sector masivo*. https://repositorio.itm.edu.co/handle/20.500.12622/6739

Ospina Rodriguez, F. E. (2024b). *Modelo de autenticación mediante blockchain Ethereum para mitigar las brechas de seguridad en las cámaras IoT del sector masivo*. https://repositorio.itm.edu.co/handle/20.500.12622/6739

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Alonso-Fernández, S. (2021). Declaración PRISMA 2020: Una guía actualizada para la publicación de revisiones sistemáticas. *Revista Española de Cardiología*, *74*(9), 790-799. https://doi.org/10.1016/j.recesp.2021.06.016

Piron, M., Wu, J., Fedele, A., & Manzardo, A. (2024). Industry 4.0 and life cycle assessment: Evaluation of the technology applications as an asset for the life cycle inventory. *Science of The Total Environment*, *916*, 170263. https://doi.org/10.1016/j.scitotenv.2024.170263

Rahman, L. F., Ozcelebi, T., & Lukkien, J. (2018). Understanding IoT Systems: A Life Cycle Approach. *Procedia Computer Science*, *130*, 1057-1062. https://doi.org/10.1016/j.procs.2018.04.148

Recuero, P. (2021a). *Breve historia de Internet de las cosas (IoT)* | *TIC, TAC, TEP: Aprender en el siglo XXI*. https://palomarecuero.wordpress.com/2021/07/30/breve-historia-de-internet-de-las-cosas-iot/

Recuero, P. (2021b). *Breve historia de Internet de las cosas (IoT)* | *TIC, TAC, TEP: Aprender en el siglo XXI*. https://palomarecuero.wordpress.com/2021/07/30/breve-historia-de-internet-de-las-cosas-iot/

Ribero-Corzo, S. M., & Prieto-Guerrero, Y. A. (2021). *Identificación de riesgos en la seguridad de la información de cámaras de vigilancia domésticas en entornos IOT*. https://repository.ucatolica.edu.co/entities/publication/64904c63-3163-4033-87e8-f8753b49e5c8

Rose, K., Eldridge, S., & Chapin, L. (2015). *LA INTERNET DE LAS COSAS— UNA BREVE RESEÑA*.

Soós, G., Kozma, D., Janky, F. N., & Varga, P. (2018). IoT Device Lifecycle – A Generic Model and a Use Case for Cellular Mobile Networks. *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*, 176-183. https://doi.org/10.1109/FiCloud.2018.00033

Späthe, S. (2021). Conception of a Generic IoT Device Life Cycle Model. *2021 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS)*, 1-7. https://doi.org/10.1109/IoTaIS53735.2021.9628736

Subramanian, S., CISA, Swaminathan, B., & CISSP. (2017, julio 18). *2017 Volume 3 Security Assurance in the SDLC for the Internet of Things*. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/security-assurance-in-the-sdlc-for-the-internet-of-things

TP-Link. (s. f.). TP-Link. Recuperado 31 de marzo de 2025, de https://www.tp-link.com/us/technology/tapo-privacy/

Wellsandt, S., Nabati, E., Wuest, T., Hribernik, K. A., & Thoben, K. D. (2016). A survey of product lifecycle models: Towards complex products and service offers. *International Journal of Product Lifecycle Management*, *9*(4), 353. https://doi.org/10.1504/IJPLM.2016.080985

Yeh, T., Chiu, D., & Kenney, L. (2017). *Persirai: Nueva botnet de IoT que ataca cámaras IP | Trend Micro (EE. UU.)*. https://www.trendmicro.com/en_us/research/17/e/persirai-new-internet-things-iot-botnet-targets-ip-cameras.html

Yoo, M.-J., Grozel, C., & Kiritsis, D. (2016). Closed-Loop Lifecycle Management of Service and Product in the Internet of Things: Semantic Framework for Knowledge Integration. *Sensors*, *16*(7), 1053. https://doi.org/10.3390/s16071053

Yousefnezhad, N., Malhi, A., & Främling, K. (2020). Security in product lifecycle of IoT devices: A survey. *Journal of Network and Computer Applications*, *171*, 102779. https://doi.org/10.1016/j.jnca.2020.102779

Yousefnezhad, N., Malhi, A., Keyriläinen, T., & Främling, K. (2023a). A Comprehensive Security Architecture for Information Management throughout the Lifecycle of IoT Products. *Sensors*, *23*(6), 3236. https://doi.org/10.3390/s23063236

Yousefnezhad, N., Malhi, A., Keyriläinen, T., & Främling, K. (2023b). A Comprehensive Security Architecture for Information Management throughout the Lifecycle of IoT Products. *Sensors*, *23*(6), Article 6. https://doi.org/10.3390/s23063236

ANEXOS

Anexo 1: Modelo de evaluación de gestión de seguridad aplicado a cámaras Ip

Nombre del dispositivo:		
DISEÑO SEGURO		
Pregunta	**SI**	**NO**
El dispositivo adquiere protocolos de comunicación seguro (EST-TSL/SSL, Mqtt, etc)?		
¿EL dispositivo cumpla con normativas de seguridad o certificaciones especificas?		
El dispositivo permite actualizaciones de firmware, mecanismo de doble autenticación y encriptación.		
¿Permite gestionar las contraseñas en su configuración?		
¿Adquiere plataformas administrables de forma segura y eficiente?		
CONFIGURACION INICIAL		
¿Permite contraseñas de al menos 12 caracteres entre letras, números y símbolos?		
¿Permite desactivar funciones innecesarias si no son requeridas (accesos remotos o sonido)?		
¿Permite deshabilitar protocolo y servicios inseguros?		
¿Permite eliminar accesos excesivos en aplicaciones?		
USO Y OPERACION		
¿Permite confirmar la identidad de los dispositivos a través de las credenciales del usuario?		
¿Permite establecer contraseñas multifactor?		
¿Puede enviar información sobre las actualizaciones si se encuentra disponibles?		
¿Permite el control de acceso y permisos para limitar el acceso a terceras personas?		
RETIRO		
El dispositivo puede desconectarse de la red, cambiar credenciales predeterminar, restaurar valores de fábrica y eliminar la información de manera segura		

Fuente: elaboración propia