UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN

RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:
ARTÍCULOS PROFESIONALES DE ALTO NIVEL

TEMA:
DISEÑO DE UNA SOLUCIÓN PARA MITIGAR LOS RIESGOS DE CONFIDENCIALIDAD DE INFORMACIÓN EN UNA SMART HOME QUE SEA FACTIBLE DE IMPLEMENTAR EN ECUADOR

AUTORES:
DIEGO EFRAÍN JÁCOME CUJI
VALERIA LIZETH PILACUÁN ERAZO

DIRECTOR:
JOSÉ LUIS AGUAYO MORALES

CUENCA – ECUADOR
2023

Autores:

Valeria Lizeth Pilacuán Erazo
Ingeniera en Sistemas – Informática para la Gestión.
Candidata a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
vpilacuan@est.ups.edu.ec

Diego Efraín Jácome Cují
Ingeniero en Sistemas Mención Telemático.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
djacomec@est.ups.edu.ec

Dirigido *por:*

José Luis Aguayo Morales
Ingeniero en Sistemas.
Magister en Sistemas Informaticos Educativos.
Magister en Redes De Comunicaciones.
Magister en Ciberseguridad.
jaguayo@ups.edu.ec

DEDICATORIA

Dedico mi esfuerzo a Dios por ayudarme a cumplir mis metas y sueños, a mis padres Sabina y Pedro, siempre han sido el pilar más importante en mi vida, son las personas que no me han fallado ni me han dejado sola, espero hacerlos sentir orgullos y no solo por un título que estoy logrando sino por la calidad de persona que me he convertido "valiente" ante cualquier circunstancia, que nunca se apaguen la luz de sus ojos papitos, nunca me ha faltado nada y ustedes se lo merecen todo, a mis hermanos Mónica y Rubén que con sus consejos y experiencia me han ayudado, no solo personal, sino académica y profesionalmente.

Le dedico también mi esfuerzo y perseverancia a mis tres pequeños, Taíz, Nicolas e Iker, que talvez no lean esto, pero siempre he querido ser un ejemplo para ustedes y sepan que todo lo que se propongan lo pueden lograr, no importan las desveladas, faltar a una fiesta o una reunión familiar, no están desperdiciando su tiempo, están ganando un mundo lleno de maravillas que van a disfrutar por todo su trabajo, los quiero desde el fondo de mi corazón.

Por último, lo dedico a Diego por tenderme la mano, para mí este reto a sido lleno de sorpresas, de maestros y sobre todo aprendizaje de un mundo que no todos en este momento puede aplicarlo.

DEDICATORIA

Dedico este éxito a mi familia que es el pilar fundamental de todo mi esfuerzo, para ellos todo lo mejor, porque han cultivado en mi la dedicación y las ganas de superación , para ellos mi amor y respeto porque a pesar de las circunstancias me han enseñado a levantarme y a salir adelante.

AGRADECIMIENTO

Muy agradecidos con Dios y la vida que nos a dado la oportunidad de conocernos y ser compañeros, amigos y colegas, nos hemos enseñado muchas cosas que han generado valor en nuestras vidas.

Muchas gracias Ingeniero Aguayo por darnos la oportunidad de realizar un tema muy importante para nuestro país, por la paciencia y sobre todo por guiarnos y facilitarnos el material para poder lograr nuestros sueños y a Valeria por ser mi apoyo en los momentos que ya queria colgar la toalla, siempre te agradeceré.

Y mi mayor agradecimiento a Dios, porque desde que era niño no me ha soltado, me ha llevado por muchos caminos y en todos he visto su grandeza; gracias Dios porque me he abrazado a tí y siempre he salido fortalecido

Tabla de Contenido

Diseño de una Solución para mitigar los riesgos de Confidencialidad de Información en una Smart Home que sea factible de Implementar en Ecuador

Autores:

Diego Efraín Jácome Cují
Valeria Lizeth Pilacuán Erazo

Resumen

La confidencialidad de la información en un ambiente de Smart Home en Ecuador, está amenazado por la inseguridad que estas redes puedan tener, esto lleva a la pérdida y robo de información. Este artículo se basa en el análisis de un ambiente con red doméstica y dispositivos críticos, en los cuales pueda existir un nivel de riesgo.

El resultado de este análisis llevó a realizar una política de seguridad, controles y roles de S.I., para los integrantes del hogar y terceros, cumplimiendo con las buenas prácticas de la norma ISO 27002:2022 y el uso de dispositivos IdC en la red, dicha política ayudará al contror de su uso, con esto se pretende lograr prevenir el robo de información de las personas que están conectadas a la red interna y mitigar riesgos de confidencialidad.

Palabras clave:

Smart Home, ataques, riesgos, domótica, seguridad, IdC, Ciberseguridad.

ABSTRACT

The confidentiality of the information in a Smart Home environment in Ecuador is threatened by the insecurity that these networks may have, this leads to the loss and theft of information. This article is based on the analysis of an environment with a home network and critical devices, in which there may be a level of risk.

The result of this analysis led to a security policy, controls and roles of IS, for members of the household and third parties, complying with the good practices of the ISO 27002:2022 standard and the use of IoT devices on the network, said This policy will help to control its use, with this it is intended to prevent the theft of information from people who are connected to the internal network and mitigate confidentiality risks.

Keys Words:
Smart Home, attacks, risks, home automation, security, IoT, cybersecurity.

1. Introducción

La confidencialidad es la garantía que los datos personales no sean difundidos (Investigación, 2017), en el Ecuador, de 18 millones de habitantes el 64.6% utiliza el internet (Digital A. M., 2022), Internet de las cosas (IdC) es una tendencia que facilita la vida de los usuarios, actualmente se encuentran empresas dedicadas a la personalización de aplicaciones para los dispositivos. Nos encontramos en la era de la tecnología donde se puede realizar cosas con un solo toque en el celular, los datos se encuentran en registros expuestos que son fáciles de atacar por hackers y otros protegidos por grandes estándares de Seguridad de la Información(S.I.) (D. Bastos).

Las redes implementadas con dispositivos inteligentes marcan una tendencia en el mercado de la tecnología, entre ellos IdC hace referencia a cualquier objeto que pueda conectarse a internet de forma inalámbrica, estos pueden ser equipos con sensores, software y tecnologías que transmitan o reciban datos (SAP, 2022), IdC es un modelo de automatización para crear una smart city, smart grid o Smart home. Una Smart home se crea según las condiciones y necesidades que se adapten a diferentes sistemas de automatización, como: control de persianas, luces inteligentes, interruptores, televisiones, etc., las mismas que están conectadas entre sí, a través de una red (Hotz Lothar, 2014), sin embargo, se plantean desafíos más grandes en cuanto al tratamiento de la información.

Los datos generados por los dispositivos IdC son aprovechados por los atacantes que buscan vulnerar la confidencialidad de los usuarios, se toma en cuenta que en el mercado hay dispositivos que no son seguros y se lanzan a la venta apresuradamente sin la seguridad necesaria, además existen estadísticas en la cual los dispositivos IdC son fáciles de hackear (Kaspersky, 2023). El alcance de este artículo profesional es elaborar y proponer una política que mitigue los problemas de seguridad, la metodología a realizar el ciclo Plan, Hacer, Verificar y Actuar o PHVA y el análisis de riego, para determinar qué tipo de activos se encuentran dentro de un escenario Smart home y la criticidad del riesgo.

La política de una Smarth Home de S.I. se realiza con el fin de mitigar riesgos de confidencialidad en los usuarios de una Smart home, basáda en la ISO 27002:2022 que hace referencia a iniciar, implementar o mantener un sistema de gestión de la Seguridad de la Información para establecer buenas prácticas, el objetivo es mitigar los riesgos de una posible violación de accesos de los usuarios y robo de información.

2. Determinación del Problema

El diseño de una Smart home muestra un impulso tecnológico de los dispositivos conectados en internet, como: focos, interruptores, Amazon Echo, ventiladores, sensores, etc., además de controladores de voz que capturan conversaciones y violan la S.I. (Abrar S. Alrumayh, 2019).

La confidencialidad es la protección contra el acceso o la divulgación de los datos (Max, 2019), IdC es un riesgo asociado a los servicios de las TIC´s que deben ser monitoreados, revisados, evaluados y gestionados periódicamente (Standar, 2022).

Los usuarios y no usuarios de los dispositivos de una Smart home deberán crear conciencia sobre amenazas, ataques, malware, phishing u otro tipo de vulnerabilidades que generen una interrupción significativa de operaciones o filtración de datos (Fabiha, Abbas, Sadaf, Taimur, & Waseem, 2022), una Smart home confiable debe aborda *"como informar sobre la confidencialidad de los datos utilizando salvaguardas"* (Chhetri, 2019).

3. Marco teórico

3.1 Smart home y la confidencialidad

El concepto de Smart home surge a principios del siglo XX, el primer experimento con éxito fue una aspiradora eléctrica y con el tiempo se sumaron más dispositivos electrónicos. La primera implementación se hizo en el año 1966, James Sutherland desarrollo el primer dispositivo para casas automatizadas, el ECHO IV (Electronic Computing Home Operator) ejecutaba acciones sencillas como prender y apagar el televisor, en el mismo año se presentó el primer chatbot ELIZA que reconoció palabras clave en frases y respondió escribiendo una frase asociada a la palabra clave reconocida (CHUANGO, 2023).

Hoy en día una Smart Home permite integrar tecnologías de información y comunicación, el mismo que responde de acuerdo al comportamiento de los habitantes y a su vez al ambiente inteligente que tiene características de dispositivos que se encuentran interconectados (Anónimo, Elementos que conformar una Smart grid, 2020).

La confidencialidad en el contexto de Smart home parte del usuario, es necesario el anonimato y consentimiento explícito para la divulgación de datos personales, se debe considerar los riesgos de confidencialidad en IdC (Gupta et al., 2019), los mismos que generan, procesan e intercambian gran cantidad de datos; algunos de estos datos pueden ser reservados y requieren altos niveles de seguridad y preservación de la privacidad (Meryem Ammi, 2021).

Además, para proteger los datos se debe sociabilizar medidas que garanticen que los usuarios protejan la información de IdC, estos dispositivos al tener soluciones de hardware y software protegen la información de posibles ataques tecnológicos, sin embargo, deben estar alineados a políticas y procedimientos que aseguren la información con planes de acción y manteniendo mejores prácticas (Milla, 2023).

4. Análisis de Metodología

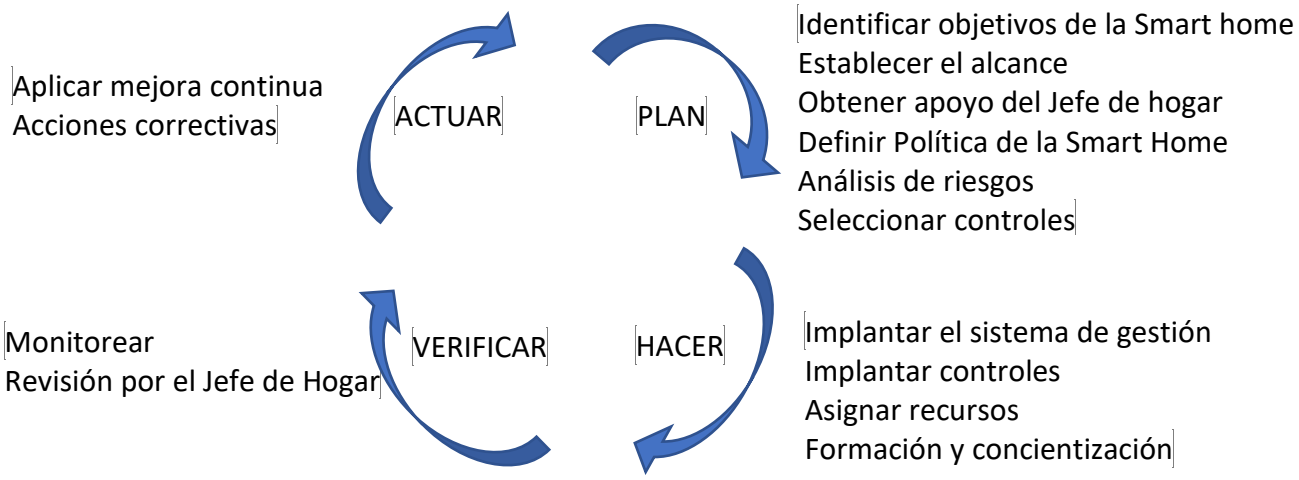
La ISO 27002:2022 establece mejores prácticas como: apoyo de un Sistema de Gestión de Seguridad de la Información., esta norma mantiene controles basados en la gestión de riesgos para los activos de información, estableciendo principios para iniciar, implementar, mantener y mejorar, los principales beneficios son:

- Concienciar sobre la Seguridad de la Información.
- Controlar los activos de información sensible
- Identificar y corregir puntos débiles.
- Reducir costos con la prevención de incidentes.
- Conformidad con la legislación y reglamentos.

5. Aplicación de la Metodología

Un Sistema de Gestión de la Seguridad de la Información es un conjunto de políticas de administración de la información, nuestra investigación esta enfocada en la confidencialidad,y lo hemos realizado según el ciclo PHVA que es una herramienta de gestión para la mejora continua.

Imagen 1: Autoría Propia

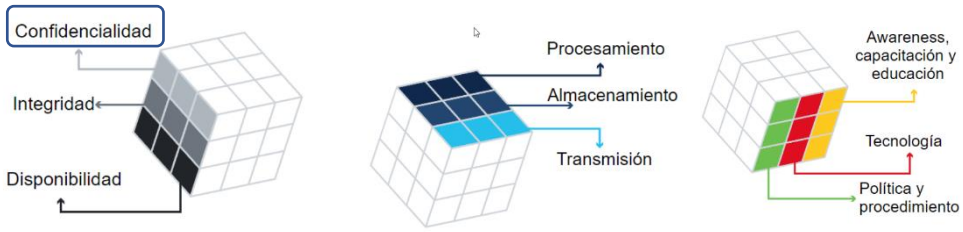


El proposito de la Smart home con la confidencialidad de los datos es mantenerlos en secreto, en este estudio se establece la configuración de una red, dispositivos y la política de Seguridad de la Información.

5.1. Cubo de McCumber

El cubo de ciberseguridad establece 3 caras que establecen y evaluan la seguridad de la información.

Imagen 2: Cubo MCCUMBER



Principios de seguridad: La primera cara identifica los objetivos para proteger dentro de la ciberseguridad.

Estado de los datos: la segunda cara se enfoca en los problemas para proteger el estado de los datos.

Medidas de ciberseguridad: la tercera cara identifica los tres tipos de poderes e instrumentos utilizados para proporcionar protección (Millá, 2023).

El diseño de una red LAN es una topología en árbol, los dispositivos centrales retransmiten señales y permiten la interconexión entre dispositivos, en caso de indisponibilidad las ramas del árbol se conecta a otra para que realice su trabajo, es decir que la información se va a distribuir en diferentes rutas. (Cableadas., 2021)

Los dispositivos IdC que se usaron en la Smart Home son:

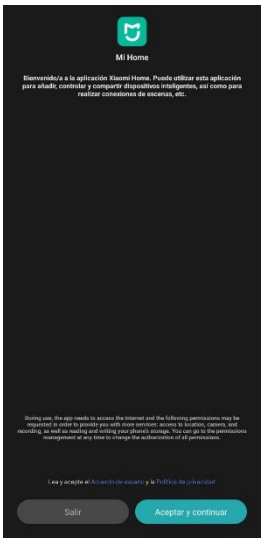
Tabla 1: Dispositivos Smart Home

DISPOSITIVOS
ROUTER INALÁMBRICO DEL ISP
FOCO LED BULB
AMAZON ECHO DOT 5TA GEN
SMART TV
SMARTPHONE

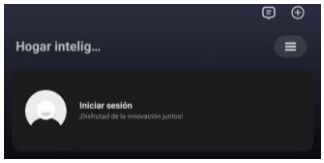
5.2. Procedimiento para configuración de Foco Led

Para lo cual, se realiza la configuración de una muestra de los dispositivos:

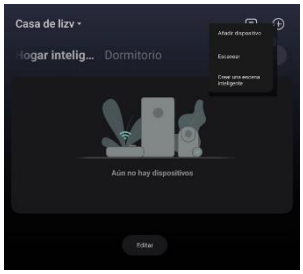
1. Descargue la aplicación “Mi Home” para la configuración del Foco Led.



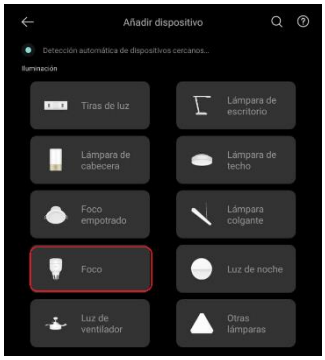
2. Inicie sesión desde el Smartphone



3. Escoja la opción “Añadir dispositivo”

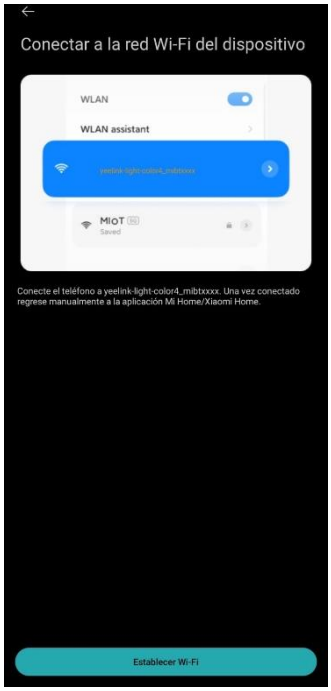


4. Escoja la opción “Foco”

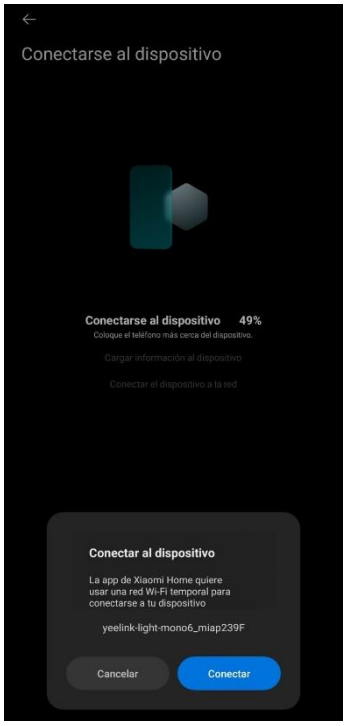


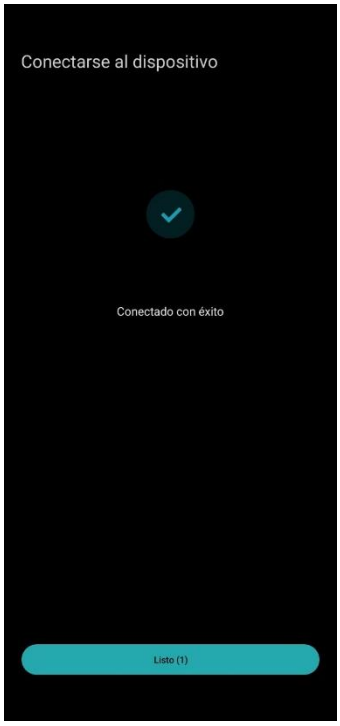
5. Ingrese a la opción de “Foco”, escoja el dispositivo que va a configurar.

6. Escoja la red wifi del “Foco”.



7. El dispositivo se conectará a la red de la casa, y a continuación el dispositivo se conectará.

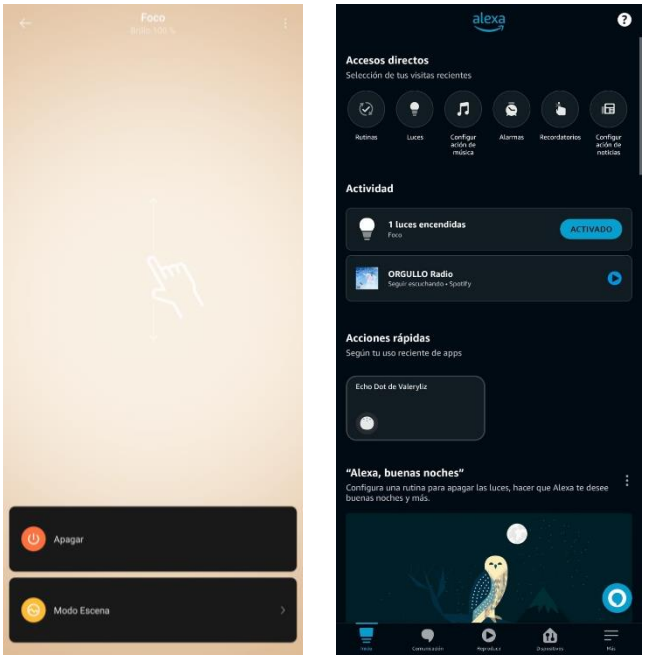




Evidencia del dispositivo *“Foco Led”* conectado a la red y a la aplicación del Smartphone.

A la derecha evidencia la configuración en el dispositivo ECHO DOT y a la izquierda se evidencia el Foco Led instalado en la aplicación.

Figura 1. Muestra de configuración del "Foco" a la red y a ECHO DOT.



Una buena práctica de diseño para mejorar la confidencialidad es basarse en estudios sobre gestión de riesgos de los activos, se deben tratar con metodologías, controles o dominios, de modo que los IdC administren una relación de confianza entre ellos con autenticación y autorización de transferencia para obtención de datos, en consecuencia, se protege los datos en reposo y tránsito.

A demás, los dispositivos tienen una MAC que al utilizar el protocolo de enrutamiento maximizan la vida útil de la red, y se convierte en solución de rendimiento y aprendizaje (Garg Hittu, 2019).

Se debe tomar en cuenta las características del hardware, como: dimensión, material del que se encuentra hecho, conexión de los dispositivos (cable o wifi) y marca, y en software las características de: almacenamiento, versión del dispositivo y versión del wifi.

La configuración de los dispositivos se debe realizar de forma individual para mitigar las vulnerabilidades como los puertos abiertos, y realizar las actualizaciones pertinentes de los IdC.

A nivel de normativa en Ecuador el *"Código Orgánico Integral Penal"* (COIP) tiene leyes que castigan delitos informáticos con penas de ausencia de libertad de 1 a 3 años dependiendo de la causa, entre las cuales están la divulgación ilegal de información (artículo 229), intercepción de comunicaciones (artículo 476), violación a la integridad de sistemas informáticos (artículo 232) y el no consentimiento de acceso a un sistema informático (artículo 234), cabe decir que son leyes nuevas que no tienen un conocimiento poblacional.

6. Resultados y discusión

Los pilares de la S.I. son: confidencialidad, integridad y disponibilidad. El estudio se fundamenta en la confidencialidad, se aborda con una política de seguridad para que la información no pueda ser accedida por individuos no autorizados.

Según los datos del INEC (Peña Andrés, 2020), se tiene las siguientes cifras de internet en Ecuador: porcentaje de usuarios que tienen un celular activo es de 81.8% y celulares inteligentes del 62.9%, entre el año 2019 y 2020, esta información es importante para saber que tan factible es tener una Smart home en el país.

Las aplicaciones que controlan los IdC, son asistentes como: Alexa, Siri, Google y otros que entienden el lenguaje humano, reconocen órdenes básicas y otras acciones un tanto complejas como "enciender la luz", "apagar la luz", responder preguntas básicas, dar información y más (Abrar S. Alrumayh, 2019), sin embargo, se debe tomar en cuenta los riesgos asumidos a la implementación de una Smart home, en el documento se plantean varios dispositivos para analizar el impacto que puede tener en el hogar.

En la Tabla 2 se puede observar en la fila de "Resultado" un resumen del impacto de la confidencialidad con los IdC según el usuario.

Tabla 2: Tipos de Información

Activos	Nombre del tipo de información	Confidencialidad La confidencialidad es la protección de la información contra el acceso o la divulgación no autorizados.			
		Impacto de la privacidad	Operacional	Reputación	Resultado
Amazon Dot	Contacto del Usuario	Alto	Alto	Alto	Alto
	Comportamientos y preferencias personales en la red	Alto	Bajo	Medio	Alto

Activos	Nombre del tipo de información	Confidencialidad La confidencialidad es la protección de la información contra el acceso o la divulgación no autorizados.			
		Impacto de la privacidad	Operacional	Reputación	Resultado
	Interacción con el usuario	Alto	Alto	Medio	Alto
	Condición médica del usuario	Alto	Medio	Alto	Alto
Camara Web	Contacto del Usuario	Alto	Medio	Medio	Alto
	Comportamientos y preferencias personales en la red	Bajo	Medio	Bajo	Medio
	Interacción con el usuario	Medio	Alto	Alto	Alto
Foco	Interacción con el usuario	Bajo	Bajo	Bajo	Bajo
SMART TV	Datos del Usuario	Medio	Bajo	Bajo	Medio
	Comportamientos y preferencias personales en la red	Bajo	Bajo	Medio	Medio
	Interacción con el usuario	Alto	Medio	Bajo	Alto
Enchufe	Interacción con el usuario	Bajo	Bajo	Bajo	Bajo
Router	Datos del Usuario	Alto	Medio	Medio	Alto

Estos dispositivos satisfacen la necesidad del usuario, las aplicaciones automatizan y analizan la información, los mismos que son responsables de procesar datos y transmitirlos.

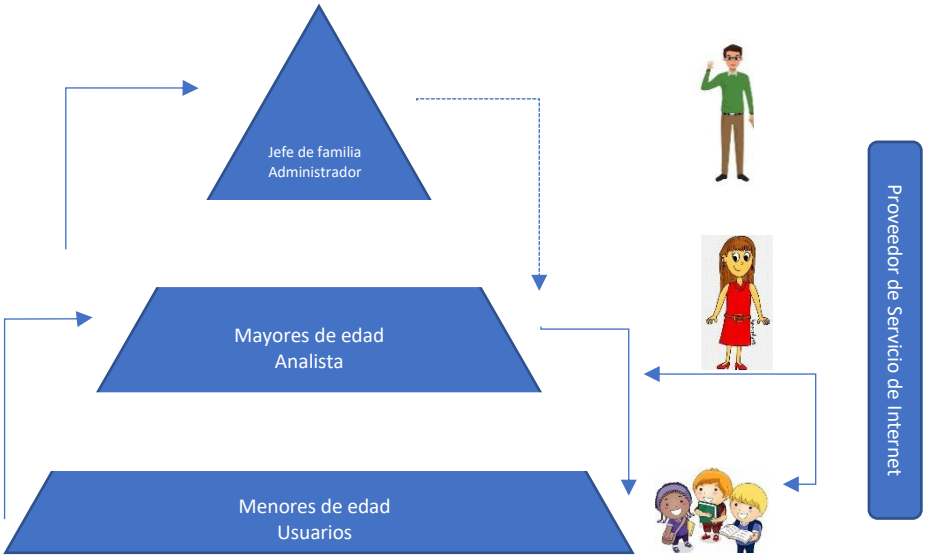
Se debe aplicar salvaguardas que reduzcan el riesgo a que se pierda la información, considerando planes de acción que no sean costosos para el usuario final.

Los usuarios y no usuarios de los dispositivos de una Smart home deben crear conciencia sobre las amenazas, ataques, malware, phishing u otro tipo de vulnerabilidades que generen una interrupción significativa de operaciones o filtración de datos (Fabiha, Abbas, Sadaf, Taimur, & Waseem, 2022), en una Smart

home confiable, se aborda la investigación de "como informar sobre las salvaguardas y asegurar la confidencialidad del usuario", disponiendo de un marco de referencia que gestione la información y toma de decisiones para crear soluciones que mejoren la eficiencia e implicaciones de confidencialidad en el hogar (Chhetri, 2019).

Los IdC son un riesgo asociado a los servicios de las llamadas Tecnologías de la Información y la Comunicación (TIC´s) que deben tener: monitoreo, revisión, evaluación y gestión periódica (Standar, 2022), además una Smart home debe tener políticas, procedimientos y roles asociados.

6.1. Modelo De Gobierno para Un Smart Home



Ejemplo de roles y funciones en una Smart Home.

Los roles son actores identificados para el correcto funcionamiento y responsabilidad de los procesos.

Jefe de familia - Administradora: Asume el riesgo que hay en la Smart home y responsable de la información.

Mayores de edad - Analista: Toma decisiones en torno al hogar, determina el contenido que se va a transmitir a los dispositivos.

Menores de edad - Usuario: Responsables de utilizar el contenido en redes y de la divulgación de información con consentimiento de sus padres.

6.1 Política para una Smart home de S.I.

Dentro de una Smart home se debe comunicar y conocer los cambios que se generan en las políticas, además, exigir a los usuarios según su rol aplicar su responsabilidad de S.I. y procedimientos para clasificar información sensible, reduciendo el riesgo de fraude, error y elusión, se debe garantizar el contacto con el administrador sobre el almacenamiento y analizar las amenazas del entorno cumpliendo con la clasificación de la información de las partes de interés.

En la Smart home deben existir reglas, procedimiento o acuerdos para la transferencia de información, estableciendo el acceso físico como lógico autorizado y previniendo el acceso no autorizado para revisión, modificación y eliminación. Establecer el uso de la nube para gestionar servicios e incidentes como cumplimiento de requisitos legales, estatutos, derechos de propiedad intelectual o acuerdos que no deberán ser divulgados.

Para esta política se utilizó los siguientes controles de la ISO 27002:2022:

- 5.1 Políticas para seguridad de la información.
- 5.2 Roles y responsabilidades de la seguridad de la información.
- 5.3 Segregación de deberes.
- 5.5 Contacto con las autoridades.
- 5.7 Inteligencia de amenazas.
- 5.12 Clasificación de la información.
- 5.14 Transferencia de información.
- 5.15 Control de acceso.
- 5.18 Derechos de acceso.
- 5.23 Seguridad de la información para el uso de servicios en la nube. (ISO/IEC27002:2022, 2022)

La política se realizó con base a una Smart home con un grupo objetivo de usuarios, con esta política se debe clasificar la información para el monitoreo, revisión y eliminación, además de controlar el manejo inadecuado de los activos asociados para reducir el riesgo de amenazas. En varios casos el activo no es seguro en una red doméstica, es muy probable que los datos sean utilizados por un tercero,

poniendo en riesgo y desventaja el tratamiento de su confidencialidad (kaspersky, 2023).

6.2. Valoración de los activos en una Smart home

Se realiza la valoración de los activos que intervienen dentro de la simulación, para lo cual los precios son referenciales al mercado y sitios comerciales. La valoración se estimó como estudio de justificación en caso de que se materializara un riesgo.

Tabla 3: Valoración de Activos

				Valoración del Impacto (pérdida)			
Nro. Activo	**Nombre de Activo**	**Tipo de Soporte**	**Ubicación**	**C**	**I**	**D**	**VA**
A1	Amazon Dot	Físico y Lógico	Sala	3	3	3	3,00
A2	Camara Web		Sala	3	2	2	2,33
A3	Foco		Sala, dormitorios, cocina	1	1	1	1,00
A4	Router		Sala	3	3	2	2,67
A5	SMART TV		Sala, dormitorios	1	1	1	1,00
A6	Enchufe		Sala	1	1	1	1,00

6.3 Análisis del Riesgo

La Evaluación del Riesgo según la tabla 4, dio como resultado que el Amazon Dot, cámara web y el router tienen riesgo crítico, los mismos que deben ser mitigados con planes de acción, en una Smart home se podría disminuir el riesgo con un antivirus para proteger los activos, además de revisar si los dispositivos cuentan con actualizaciones de software y parches.

Tabla 4: Evaluación de Nivel de Riesgo

Análisis de Riesgos					Evaluación de Riesgos					
					Impacto	Probabilidad		Controles Implementados existentes	Cálculo de Evaluación de Riesgos	Nivel de Riesgo
Subproceso	Nro. Activo	Nombre de Activo	Amenaza	Vulnerabilidad	CID	Nivel de Amenaza	Nivel de Vulnerabilidad			
Infraestructura Smart home	A1	Amazon Dot	Acceso a otros dispositivos	Incompatibilidad de software con dispositivos AI	3,00	3	2	Mantenimiento local	18,00	Alto
			Indisponibilidad de Servicios	No encontrar actualizaciones de software	3,00	3	2	Soporte local	18,00	Alto
	A2	Cámara Web	Borrado o edición de información de video	Perdida de información	2,33	3	3	Mantenimiento local	21,00	Alto
			Acceso de personas no deseadas	Vigencia tecnológica, equipo continuamente dañado	2,33	3	3	Soporte local	21,00	Alto
	A3	Foco	Indisponibilidad de Servicios	Error de uso	1,00	1	2	Soporte local	2,00	Bajo
				Fallo de hardware	1,00	1	1	Mantenimiento local	1,00	Bajo
	A4	Router	Intrusos en la red	Área sin vigilancia	2,67	2	2	Mantenimiento local	10,67	Alto
			Indisponibilidad de Servicios	No existe equipo de redundancia	2,67	3	2	Soporte local	16,00	Alto
	A5	SMART TV	Ataques de Ingeniería Social	Infección de malware	1,00	1	1	Mantenimiento local	1,00	Bajo
			Indisponibilidad de Servicios	No encontrar actualizaciones de software	1,00	2	2	Soporte local	4,00	Medio
	A6	Enchufe	Ataques de Ingeniería Social	No encontrar actualizaciones de software	1,00	1	1	Mantenimiento local	1,00	Bajo
			Mal uso del software	Fallo de hardware	1,00	1	1	Soporte local	1,00	Bajo

El Usuario debe considerar salvaguardas para una Smart home físico y lógico con controles de acceso que pueden ser: un módulo de reconocimiento de voz, sistemas con alertas 24 horas los 7 días que sean eficientes y que tengan facilidad de uso, seguridad multinivel con sensores que envíen en paralelo alertas por mensajes de texto, además, de antivirus y firewall (ShariqSuhail Md, 2016).

Planes de acción para la Seguridad de la Información.

1. Mejorar la "Política de una Smart Home de S.I." según el alcance que tiene la Smart Home del usuario final.
2. Cambio de dispositivos IdC que se encuentren descontinuados.
3. Sociabilizar la "Política de una Smart Home de S.I."

6.4. Discusión

Se debe mencionar que para activar cualquier plan de acción se puede probar con al menos una holgura de 6 meses, en este caso se decidió trabajar con la confidencialidad de los usuarios utilizando la ISO 27002:2022 para crear la sección de la "Política de una Smart Home de S.I.". También indicar que para la gestión de riesgos es posible que existan medios para justificar su criticidad.

6.5. Limitaciones para verificar la Política de una Smart Home de S.I.

La validación de la Política de una Smart Home de S.I. no se pudo completar dado por el tiempo que se tuvo para realizar la investigación, sin embargo, se logró iniciar el proceso de un Sistema de Gestión para S.I., escogiendo los IdC que se encuentran al alcance de un usuario de clase media en el Ecuador, como se describe en la "Tabla 3: Dispositivos Smart Home". Además, otro obstáculo fue comprobar la protección de los datos al no poder tener el monitoreo del flujo de datos, debido a que este fue contratado al ISP y no se tuvo un control para ver las diferentes alertas que se pudieron presentar.

6.6. Resumen de hallazgos

Al terminar con el análisis de los tipos de información, se conoce que los activos evaluados tienen un impacto alto para el usuario, puede darse por tener seguridad deficiente en el control de acceso, validaciones al ingreso de aplicaciones, a demás por código malicioso o la mal configuración de los dispositivos. En la línea para la valoración del impacto, el activo con más riesgo es el Amazon Dot, debido a la información que mantiene, esto puede ser: número de tarjetas de crédito o débito, cantidad de IdC que se encuentran conectados, entre otra información que circula.

6.7. Trabajo futuro.

Smart home es un tema que constantemente se menciona en el futuro, en esta vía de desarrollo se debe mantener el proyecto relacionado a la implementación de la confidencialidad tanto en dispositivos como en políticas de seguridad de la información. El desarrollo de más investigaciones pueden desencadenar una metodología para apoyar a un usuario común para que pueda entender la complejidad del riesgo e impacto al no tener las salvaguardas adecuadas.

Finalmente, plantear la evaluación de riesgos de más IdC´s para tener resultados más reales a lo que puede terminar costando un ataque cibernético por falta de seguridades en los dispositivos.

7. Conclusiones

En el Ecuador tener una Smart home es costoso, debido a los precios de los IdC que tienen precios entre $60 a $150, esto dependiendo del dispositivo, además se toma en cuenta el precio de los incidentes que involucran un hackeo o la probabilidad de ocurrencia, de igual forma se suma el valor de los costos de antivirus, firewall u otros, que protejan la información del usuario.

La información de todos los familiares o usuarios deben estar protegidos por los dispositivos de la Smart home que se encuentren en la red. Además, se debe de implementar políticas y reglas internas que permitan navegar de forma segura para no caer en engaños de hackers o diferentes malwares, una buena iniciativa es contratar o instalar un antivirus que ayude al monitoreo y proteger la confidencialidad de la información.

Se concluye que el caso de estudio en Ecuador debe abordar diferentes frentes como la privacidad e integridad, teniendo en cuenta que en la actualidad ya se cuenta con la Ley de Protección de Datos vigente y puede facilitar el alinearse a la ciberseguridad.

8. Recomendaciones

Después de realizar este caso de estudio, se debe analizar el riesgo dentro de un ambiente Smart Home controlado y validar si la Política para una Smart home de S.I se encuentra alineada a las necesidades de los habitantes, se recomienda la elaboración de un prototipo en el cual se pueda plasmar todo lo que se ha evidenciado en este documento.

El objeto de estudio está enfocado a la confidencialidad de la información de los usuarios, se podría dar un alcance a la disponibilidad e integridad y analizar los diferentes enfoques que un ambiente Smart Home ofrece a nivel de seguridad.

Además el estudio para mitigar los riesgos de confidencialidad en un Smart home puede ser recomendado para otros ambientes dentro de los cuales puede ser un Smart Block o un Smart City, para lo cual se debe tener en cuenta que la familia es un bien que debe ser asegurado y no limitar gastos al momento de pensar en la seguridad de su intimidad e información personal.

La confidencialidad es la garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona. Dicha garantía se lleva a cabo por medio de un grupo de reglas que limitan el acceso a ésta información

9. Anexos

Tabla 3: Magerit, análisis de confidencialidad

MAGERIT - versión 3.0
Metodología deAnálisisy Gestión de Riesgos de los SistemasdeInformación

					Dimensiones						Tipos de activos					
Errores y fallos no intencionados	Fallos no intencionales causados por las personas. La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.	Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, datos, etc.	38 - ERROR DE USO	✔	✔	✔	✔		✔					✔	
		Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	38 - ERROR DE USO	✔	✔	✔	✔	✔	✔		✔			✔	
		Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	no disponible	✔	✔										
		Errores de [re-]encaminamiento	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de qué el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.	no disponible	✔	✔			✔	✔						
		Errores de secuencia	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.		✔											
		Fugas de información	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.	no disponible	✔	✔	✔	✔		✔				✔	✔	
		Vulnerabilidades de los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.	no disponible	✔	✔										
		Pérdida de equipos	La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de infor mación los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	22 - RECUPERACIÓN DE SOPORTES RECICLADOS O DESECHADOS	✔						✔	✔			✔	
		Indisponibilidad del personal	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, ...	42 - DAÑO A LA DISPONIBILIDAD DEL PERSONAL												
		Manipulación de la configuración	Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	no disponible	✔											✔
		Suplantación de la identidad del usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	40 - USURPACIÓN DE DERECHO	✔	✔	✔	✔	✔	✔						
		Abuso de privilegios de acceso	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.	39 - ABUSO DE DERECHO	✔	✔	✔	✔		✔		✔				
		Difusión de software dañino	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc	no disponible	✔	✔										
		[Re-]encaminamiento de mensajes	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.	no disponible	✔	✔			✔	✔						
		Alteración de secuencia	Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.	36 - ALTERACIÓN DE DATOS		✔			✔	✔						
		Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización	33 - USO ILÍCITO DEL HARDWARE	✔	✔	✔	✔	✔	✔	✔	✔		✔	✔	
		Análisis de tráfico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina "monitorización de tráfico".	no disponible	✔				✔							
		Repudio	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.	41 - NEGACIÓN DE ACCIONES						✔						✔
		Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.	19 - ESCUCHA PASIVA	✔				✔							
		Divulgación de información	Revelación de información.	23 – DIVULGACIÓN 27 – GEOLOCALIZACIÓN 34 - COPIA ILEGAL DE SOFTWARE	✔	✔	✔	✔		✔				✔	✔	
		Manipulación de programas	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza	26 - ALTERACIÓN DE PROGRAMAS	✔	✔										
		Manipulación de los equipos	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indi recto cuando una persona autorizada lo utiliza.	25 - SABOTAJE DEL HARDWARE	✔						✔		✔		✔	
		Robo	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas con tratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	20 - ROBO DE SOPORTES O DOCUMENTOS 21 - ROBO DE HARDWARE	✔						✔	✔			✔	
		Ocupación enemiga	Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.	no disponible	✔									✔		
		Extorsión	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.	no disponible	✔											
		Ingeniería social	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	no disponible	✔											

10. Referencias

Abrar S. Alrumayh, S. M. (2019). ABACUS: Audio Based Access Control Utility for Smarthomes. *ICM DIGITAL LIBRARY*, 12.

Anónimo. (2020). *Elementos que conformar una Smart grid.* Anónimo.

Anónimo. (2022). *https://www.idrix.com.ec/servicios/internet-de-las-cosas-iot-ecuador*. (iDrix Technology S.A) Recuperado el 12 de 09 de 2022, de https://www.idrix.com.ec/servicios/internet-de-las-cosas-iot-ecuador

Cableadas., R. I. (2021). *Redes Inalambricas y Cableadas.* Obtenido de Redes Inalambricas y Cableadas.: https://redesinalambricasycableadas.wordpress.com/redes-cableadas/diferentes-topologias-de-red/topologia-de-arbol/

Calles-García, J., & González-Pérez, P. (2011). *La Biblia del Footprinting.*

Chhetri, C. (2019). Towards a Smart Home Usable Privacy Framework. *ACM DIGITAL LIBRARY*, 4.

CHUANGO. (25 de 05 de 2023). *La historia de los antecesores del hogar inteligente - Gruesos y complicados*. Obtenido de https://chuango.de/es/blogs/news/smart-home-history

D. Bastos, M. S.-M. (s.f.). Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments. pág. 7.

DAWEX. (2022). *DAWEX*. Obtenido de https://www.dawex.com/es/seguridad-confidencialidad/

Digital, A. M. (08 de 11 de 2022). *Cifras Estadísticas Digitales 2022 Ecuador*. Obtenido de Cifras Estadísticas Digitales 2022 Ecuador: https://agenciadigitalamd.com/marketing-digital/estadisticas-digitales-ecuador/

Fabiha, H., Abbas, S. G., Sadaf, H., Taimur, B., & Waseem, A. (4 de 02 de 2022). Computer Communications. *Science Direct*.

Garg Hittu, M. D. (2019). Protección de dispositivos IoT y conexción segura de los puntos usando REST API y Middleware. *IEEE*, 6.

Hotz Lothar, W. K. (2014). Model de configuración de Smarthome. *IEEE*, 15.

Investigación, D. d. (28 de Diciembre de 2017). *INCMNSZ*. Obtenido de https://www.incmnsz.mx/opencms/contenido/investigacion/comiteEtica/confidencialidadInformacion.html#:~:text=La%20confidencialidad%20es%20la%20garant%C3%ADa,el%20acceso%20a%20%C3%A9sta%20informaci%C3%B3n.

ISO/IEC27002:2022. (2022). Information security, cybersecurity and privacy protection — Information security controls. *INTERNATIONAL STANDARD*, 164.

Kaspersky. (2023). Obtenido de https://latam.kaspersky.com/resource-center/threats/how-safe-is-your-smart-home

kaspersky. (2023). *¿Son seguros los hogares inteligentes?* Obtenido de https://latam.kaspersky.com/resource-center/threats/how-safe-is-your-smart-home

Max, F. (10 de 10 de 2019). *IoT: grandes oportunidades… y grandes riesgos*. (HIKVISION) Recuperado el 12 de 09 de 2022, de

https://www.hikvision.com/es/newsroom/blog/IoT-grandes-oportunidades-y-grandes-riesgos/
Meryem Ammi, S. A. (2021). Customized blockchain-based architecture for secure smart home for lightweight IoT. *ELSEVIER*, 22.
Milla, A. (1 de 05 de 2023). *McCumber Cube*. Obtenido de https://www.alexmilla.net/mccumber-cube-el-cubo/
Nacional, A. (26 de 05 de 2021). *Ley Orgánica de Protección de Datos del Ecuador.* Obtenido de Ley Orgánica de Protección de Datos del Ecuador: https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf
Nikolaos-Foivos, P., Pierre-Henri, T., Maxime, P., & Vincent, B. (2022). A Comprehensive Survey of Attacks without Physical Access Targeting Hardware Vulnerabilities in IoT/IIoT Devices, and Their Detection Mechanisms.
Peña Andrés, H. L. (2020). Indicadores de tecnología de la información y comunicación. *Encuesta MULTI PORPÓSITO*, 25.
Rose Karen, E. S. (10 de 2015). *internet society*. Recuperado el 2022, de https://www.internetsociety.org/wp-content/uploads/2017/09/report-InternetOfThings-20160817-es-1.pdf
S&P. (11 de 03 de 2019). *Smart home: qué es una casa inteligente y cuáles son sus ventajas*. Obtenido de https://www.solerpalau.com/es-es/blog/smart-home/
SAP. (13 de 09 de 2022). *¿Qué es IoT y cómo funciona?* (SAP) Recuperado el 13 de 09 de 2022, de https://www.sap.com/latinamerica/insights/what-is-iot-internet-of-things.html
ShariqSuhail Md, V. R. (2016). Multi-Functional Secured Smart Home. *IEEE*, 6.
Sociedad, M. d. (2019). *Libro Blanco de Territorios Digitales en Ecuador.* Quito: Ecuador Digital.
Standar, I. (2022). ISO/IEC 27002. *Information security, cybersecurity and privacy protection — Information security controls*, 164.
www.elhacker.net. (s.f.). *www.elhacker.net*. Obtenido de https://www.elhacker.net/trucos_google.html
Xianbin Xu, Y. G. (2022). Fog-enabled private blockchain-based identity authentication scheme for smart home. *ELSEVIER*, 11.