UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

*Resolución: **RPC-SO-02-No.053-2021***

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del proyecto:
Guía para el uso de dispositivos IoT de tipo doméstico y estrategias de mitigación basadas en aprendizaje automático
Línea de Investigación:
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autor/a:
Cristian Daniel Toapanta Vega
Tutor/a:
PhD. Maryory Urdaneta Herrera PhD. Renato Mauricio Toasa Guachi

Quito – Ecuador

2025

APROBACIÓN DEL TUTOR

Yo, **Renato Mauricio Toasa Guachi** con C.I: **1804724167** en mi calidad de Tutor del proyecto de investigación titulado: **Guía para el uso de dispositivos IoT de tipo doméstico y estrategias de mitigación basadas en aprendizaje automático**.

Elaborado por: **Cristian Daniel Toapanta Vega**, de C.I: **0503271546**, estudiante de la Maestría: Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2025

Firmado electrónicamente por:
RENATO MAURICIO
TOASA GUACHI

_____

Firma

APROBACIÓN DEL TUTOR

Yo, **Maryory Urdaneta Herrera** con C.I: **1759316126** en mi calidad de Tutor del proyecto de investigación titulado: **Guía para el uso de dispositivos IoT de tipo doméstico y estrategias de mitigación basadas en aprendizaje automático**.

Elaborado por: **Cristian Daniel Toapanta Vega**, de C.I: **0503271546**, estudiante de la Maestría: Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2025

MARYORY URDANETA HERRERA

Firmado digitalmente por MARYORY URDANETA HERRERA
Fecha: 2025.03.11 03:33:15 -05'00'

_____

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, **Cristian Daniel Toapanta Vega** con C.I: **0503271546**, autor del proyecto de titulación denominado: **Guía para el uso de dispositivos IoT de tipo doméstico y estrategias de mitigación basadas en aprendizaje automático**. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., marzo de 2025

Firmado electrónicamente por:
CRISTIAN DANIEL
TOAPANTA VEGA

_____

Firma

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

Actualmente, las personas viven en un mundo globalizado donde es necesario entender la importancia de la integración mundial en los diferentes aspectos, sean estos económicos, sociales, incluso políticos, pero sobre todo tecnológicos.

Los dispositivos IoT (Internet de las cosas) son de uso diario ya que han alcanzado integrarse mediante aplicaciones a dispositivos médicos, electrodomésticos, sistemas industriales, etc. Los mismos dan paso a la automatización e intercambio de información, todo esto en tiempo real, permitiendo de esa manera la eficiencia en los diferentes procesos que se llevan en todos los ámbitos.

Sin embargo, la gran acogida que los dispositivos IoT (Internet de las cosas) que ha tenido en los últimos años ha marcado vulnerabilidades significativas en el tema de seguridad, contraseñas débiles, fallos en las actualizaciones en el software, permitiendo de esta manera ataques cibernéticos.

Un desafío adicional es la falta de estandarización global en términos de seguridad IOT. Aunque algunos países han implementado regulaciones específicas, como la Ley de Mejora de la Ciberseguridad IOT en Estados Unidos, estos esfuerzos no se han adoptado de manera uniforme en todo el mundo (Ruiz et al., 2023).

Problema de investigación

Sectores empresariales, educativos, industriales y financieros han formado parte del crecimiento acelerado del uso de la internet de las cosas (IoT), debido a su compatibilidad en los dispositivos de uso industrial, de salud, doméstico, financiero como, por ejemplo, el uso en cámaras de seguridad.

Sin embargo, el internet de las cosas (IoT), hoy en día no solo ha traído consigo los grandes beneficios a las organizaciones o sus propios usuarios como se puede especificar, sino también detrás de todos estos, presenta diferentes riesgos de seguridad, debido a sus fallos, como el uso de contraseñas débiles, la transmisión de datos sin cifrado, el uso de software sin actualizar ha generado el aumento de ciberataques a estos dispositivos.

La investigación que se propone tiene como objetivo formular una guía eficaz y flexible para el uso de dispositivos IoT (Internet de las Cosas) en el ámbito doméstico, considerando los aspectos de seguridad, privacidad y eficiencia. En los hogares cada vez se está incrementando el uso de los dispositivos IoT, proporcionando comodidad, automatización y control a los usuarios

a través de varias aplicaciones. Sin embargo, el uso de estos dispositivos está generando riesgos relacionados tanto a la seguridad, como a la privacidad sobre el manejo de la información.

La investigación busca desarrollar estrategias basadas en aprendizaje automático con el uso de machine learning que ayude a mitigar los riesgos en los dispositivos IoT, de esta manera se busca que el entorno doméstico este seguro.

Con la presente guía se pretende responder: ¿De qué manera las estrategias basadas en aprendizaje automático mitigaran la vulnerabilidad de los dispositivos IoT?

Objetivo general

Desarrollar una guía integral para el uso seguro y eficiente de dispositivos IoT de tipo doméstico, implementando estrategias de mitigación basadas en aprendizaje automático para la detección y prevención de riesgos de seguridad, para el mejoramiento de la protección e integridad de la seguridad en el ecosistema IoT.

Objetivos específicos

- Desarrollar un contexto de los fundamentos teóricos sobre la IoT.
- Identificar las debilidades más comunes en los dispositivos (IoT) de tipo doméstico y estrategias de mitigación basadas en aprendizaje automático.
- Elaborar una guía que proporcione el uso seguro de los dispositivos IoT de tipo doméstico.
- Valorar la propuesta por medio de las opiniones o criterios de expertos/especialistas en seguridad informática.

Vinculación con la sociedad y beneficiarios directos:

En la vivienda, la seguridad familiar es de suma importancia al momento de utilizar dispositivos IoT. La investigación que se plantea tiene como objetivo desarrollar una guía sólida para el uso de dispositivos IoT de tipo doméstico y estrategias de mitigación basadas en aprendizaje automático.

Este estudio está alineado con el Objetivo nueve de Desarrollo Sostenible (ODS) q: "Industria, Innovación e Infraestructura", el cual trata de la búsqueda de la construcción de infraestructuras resilientes, promoviendo que la industrialización sea tan inclusiva como sostenible, y el fomento de la innovación.

Específicamente, la implementación de soluciones innovadoras basadas en aprendizaje automático para mitigar los riesgos en dispositivos IoT contribuye a la innovación tecnológica en

el ámbito doméstico, porque permite la fabricación de nuevos dispositivos con mayor seguridad e inteligencia.

Por lo que el objeto de este trabajo es el brindar a las personas un adecuado uso de los dispositivos IoT para el aseguramiento tanto de la rectitud como la confiabilidad de la información manejada residencias u hogares.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

En la última década los dispositivos de Internet de las cosas (IoT) han cambiado la interacción de los hogares con la tecnología, estos dispositivos pueden ser: sistemas de seguridad, altavoces inteligentes, cerraduras inteligentes, enchufes inteligentes, cámaras de timbre inteligentes, dispositivos para monitoreo de energía, electrodomésticos inteligentes, controles de temperatura, permiten a los usuarios tener una mejor calidad de vida, sin embargo todos estos dispositivos dan lugar a vulnerabilidades de seguridad, poniendo en grave peligro la privacidad de los hogares.

1.1. Contextualización general del estado del arte

En la actualidad los dispositivos de la IoT ofrecen muchas comodidades ya que se conectan con una gran facilidad en los hogares ecuatorianos todo esto implica que presenten muchas vulnerabilidades a hackeos, control no autorizado y filtración de datos.

Según Atiaja (2024), el escaneo de la red, permite la determinación de las diversas vulnerabilidades que podrían estar presentes, las cuales son cruciales para la estructuración de las políticas que forman parte del desarrollo del manual de políticas de seguridad de comunicación entre los dispositivos IoT.

Bermúdez (2022), realizó un estudio, el cual consistió en la realización encuestas dirigidas a los usuarios acerca de los dispositivos IoT, para determinar tanto la percepción como la implementación de las seguridades que debe tener los usuarios en sus hogares. El cual trajo consigo el desarrollo de una guía de mejores prácticas, el cual tuvo como resultado el establecimiento de una seguridad integral a través de los servicios de la IoT en la vivienda.

En cambio, Villacís (2024), a través de su estudio hace uso tanto de técnicas como herramientas de inteligencia artificial, todo esto para analizar las debilidades de las redes LAN y de esta manera buscar la mejora la detección y respuesta de las posibles amenazas cibernéticas. Concluyendo en la investigación que una IA bien entrenada ayuda de mejor manera a identificar rápidamente y de forma precisa posibles pautas de ataque para mejorar la seguridad informática, optimizando los recursos humanos y/o técnicos para su administración.

Para proteger dispositivos IoT de manera adecuada contra ataques cibernéticos, es muy importante revisar documentos o guías donde se valide las políticas y normativas de seguridad. Estas directrices deben asegurar que los dispositivos IoT sean gestionados de manera correcta conforme a las prácticas de seguridad.

Para evitar ataques de internet por medio de nuestros dispositivos IoT que tenemos en nuestros hogares es muy importante tener una infraestructura IoT bien segura.

1.2. Proceso investigativo metodológico

El desarrollo de esta guía para el uso de dispositivos IoT de tipo doméstico y estrategias de mitigación basadas en aprendizaje automático tiene un enfoque metodológico cuantitativo, se aplicará una encuesta a una muestra seleccionada de manera intencional de profesionales en el área de Tecnologías de la Información (TI) y de Seguridad Informática.

Mientras que la población a ser encuestada se compone de profesionales en el área de las TI y de Seguridad Informática, las cuales administran las redes domésticas. La muestra será seleccionada de manera no probabilística, fue realizada de manera intencional, se conformó por 10 personas profesionales encargados en la gestión de seguridad y de las Tics tanto en sus empresas como en sus hogares.

Mientras que, respecto al diseño de la encuesta, la misma posee preguntas cerradas que estén claramente asociadas con los objetivos de la investigación. Estas preguntas abordarán aspectos como la percepción existente acerca de las vulnerabilidades en dispositivos IoT de tipo doméstico, el manejo de herramientas de aprendizaje automático y la disposición con respecto a la adopción de tecnologías nuevas.

Los resultados del análisis estarán dados en función de los objetivos presentes en el estudio. Los hallazgos encontrados proporcionarán una sólida base, en pro del desarrollo de varias estrategias de mitigación basadas en aprendizaje automático.

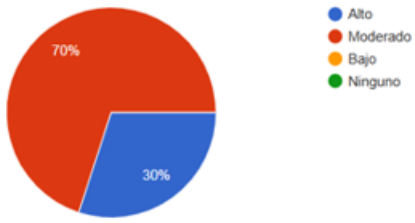
1.3. Análisis de resultados

En el Anexo 1 se adjunta la encuesta realizada, a continuación, se procede hacer la tabulación:

En la Figura 1 el 70% de los encuestados afirman que tienen un conocimiento moderado sobre el conocimiento de Internet de las Cosas IoT y el 30% afirman que tiene un conocimiento alto.

Figura 1.

Pregunta 1. ¿Qué nivel de conocimiento tiene sobre Internet de las Cosas (IoT)?

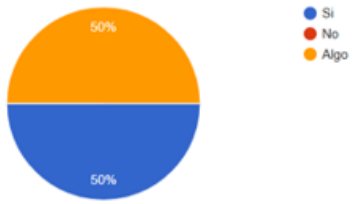


Nota. Elaboración propia

En la Figura 2, el 50% de las personas encuestadas tienen conocimiento sobre las debilidades de los dispositivos IoT de tipo doméstico y el otro 50% afirman que conocen algo, el equilibrio de las respuestas resalta acerca de la necesidad de mejora respecto al conocimiento sobre los dispositivos IoT y proponer estrategias que mitiguen estas vulnerabilidades.

Figura 2.

Pregunta 2. ¿Conoce las vulnerabilidades de seguridad, en los dispositivos IoT de uso doméstico?

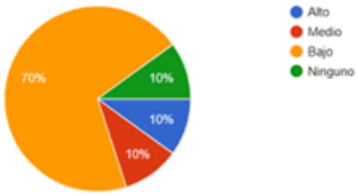


Nota. Elaboración propia.

En la Figura 3 el 10% de los encuestados mencionan que un hogar los usuarios no conocen sobre las amenazas de seguridad en los dispositivos IoT, el otro 10% tiene un conocimiento bajo, el otro 10% tiene un conocimiento medio, mientras que el 70% conocen sobre las amenazas que pueden tener en su hogar.

Figura 3.

Pregunta 3. ¿Cómo evaluaría el grado de conocimiento de los usuarios sobre las amenazas de seguridad de los dispositivos IoT de tipo doméstico?

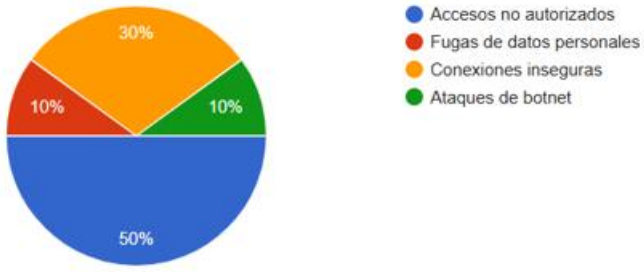


Nota. Elaboración propia.

Como se puede ver, la Figura 4 tenemos como resultado que el 50% de los encuestados consideran que los accesos no autorizados son la vulnerabilidad más frecuente en los dispositivos IoT, el 30% menciona las conexiones inseguras, el 10% señala las fugas de datos personales y el 10% menciona que los ataques de botnet.

Figura 4.

Pregunta 4. ¿Qué tipo de vulnerabilidades son más frecuentes en los dispositivos IoT domésticos?

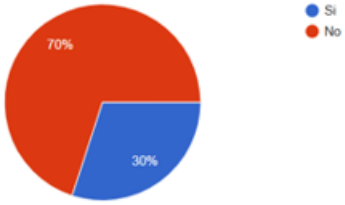


Nota. Elaboración propia.

En la Figura 5 afirma el 70% de los encuestados que tienen alguna herramienta para proteger los dispositivos IoT y el 30% no utiliza ninguna seguridad.

Figura 5.

Pregunta 5. ¿En su hogar utiliza alguna herramienta de seguridad para proteger los dispositivos IoT?

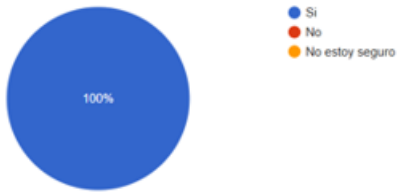


Nota. Elaboración propia.

Se puede ver, que en la Figura 6 el 100% de los encuestados mencionan que, hacer uso de aprendizaje automático mejorara la detección de amenazas en dispositivos IoT, de tipo doméstico.

Figura 6.

Pregunta 6. ¿Cree que el uso de aprendizaje automático (machine learning) puede mejorar la detección de amenazas en dispositivos IoT, de tipo doméstico?

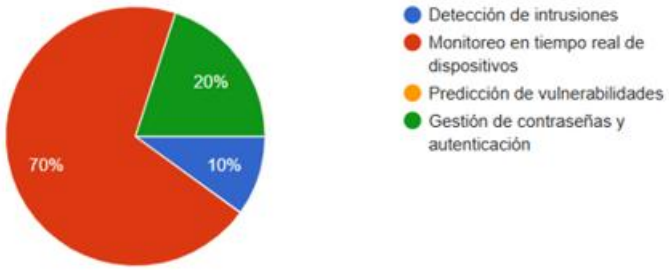


Nota. Elaboración propia.

En la Figura 7 tenemos como resultado que el 70% de los encuestados consideran que el monitoreo en tiempo real de dispositivos podría tener un mayor impacto al hacer uso de aprendizaje automático, el 20% escoge gestión de contraseñas y el 10% detección de intrusiones.

Figura 7.

Pregunta 7. ¿En qué área considera que el aprendizaje automático podría tener un mayor impacto?

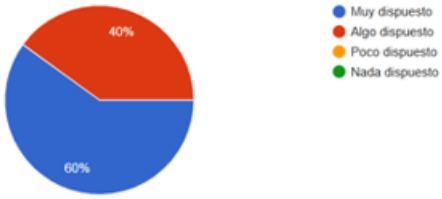


Nota. Elaboración propia.

En la Figura 8 el 60% de los encuestados están muy dispuestos a implementar soluciones basadas en aprendizaje automático para el mejoramiento de la seguridad de los dispositivos IoT, mientras que el 40% estaría algo dispuesto.

Figura 8.

Pregunta 8. ¿Estaría dispuesto a implementar soluciones basadas en aprendizaje automático para mejorar la seguridad de los dispositivos IoT de tipo doméstico?



Nota. Elaboración propia.

Se puede ver que la Figura 9, un 60% de los encuestados menciona que la falta de conocimiento o capacitación es el desafío más grande para implementar soluciones basadas en aprendizaje automático, el 20% menciona el costo y el 20% se preocupa sobre la privacidad de los datos.

Figura 9.

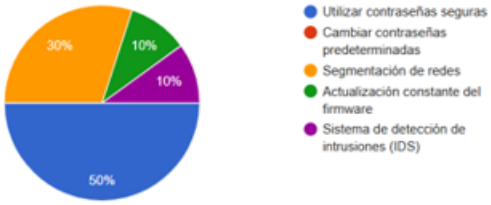
Pregunta 9. ¿Qué factor considera como desafío para implementar soluciones basadas en aprendizaje automático para la seguridad de los dispositivos IoT de tipo doméstico?

Nota. Elaboración propia.

Se puede verificar que en la figura 10 el 60% de los encuestados mencionan que utilizar contraseñas seguras, cambiar contraseñas predeterminadas, segmentación de redes, actualización constante del firmware y sistema de detección de intrusiones (IDS) serian buenas medidas de implementar para proteger los dispositivos IoT y el 40% menciona que actualización constante del firmware y sistema de detección de intrusiones (IDS) sería una buena medida de implementación.

Figura 10.

Pregunta 10. ¿Qué medidas de seguridad recomienda implementar para proteger los dispositivos IoT en un hogar?

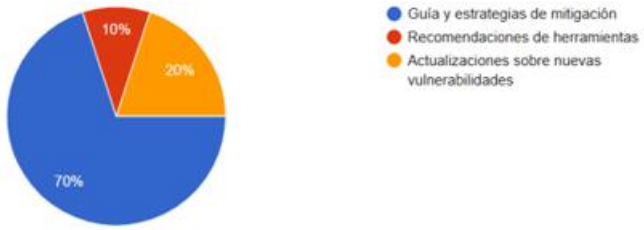


Nota. Elaboración propia.

En la Figura 11 el 70% de los encuestados considera que una guía y estrategias de mitigación ayudaría a los usuarios a mejorar la seguridad de sus dispositivos IoT de tipo doméstico, el 20% menciona que las actualizaciones sobre nuevas vulnerabilidades mejoran la seguridad y el 10% recomienda herramientas para garantizar la seguridad en el hogar.

Figura 11.

Pregunta 11. ¿Qué tipo de recursos considera necesarios para ayudar a los usuarios a mejorar la seguridad de sus dispositivos IoT de tipo doméstico?



Nota. Elaboración propia.

CAPÍTULO II: PROPUESTA

2.1. Fundamentos teóricos aplicados

2.1.1. Internet de las cosas IoT (Internet of Things)

Este término es referente a la red de maquinarias, vehículos y otros objetos físicos, los cuales se vinculan con el software, sensores y se conecta a la red integrada, permitiendo de esta manera tanto la recopilación como el compartimiento de datos (IBM, 2025).

Este concepto se ha desarrollado en cinco etapas distintas (Kalla et al., 2019). Donde en la primera, se enfocó en la conectividad entre computadoras. Mientras que, en la segunda, con la creación de la World Wide Web, permitió la conexión global de computadoras. Posteriormente, surgió la fase del Internet móvil, facilitando el acceso a la red desde dispositivos móviles. Posteriormente, las identidades digitales personales se incorporaron en el entorno del Internet por medio de redes sociales. Por último, la etapa actual está marcada por el advenimiento del IoT, cuyo propósito es la conexión de los objetos físicos a la red.

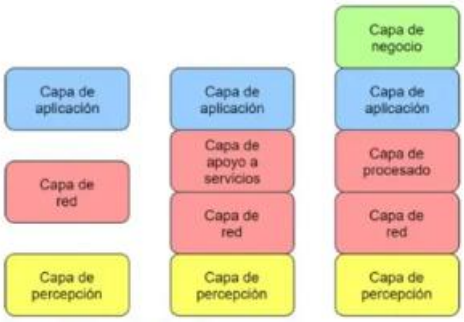
Este enfoque de IoT pretende transformar varios sectores, por ejemplo, en hogares inteligentes, servicios enfocados en el área de la salud hasta la gestión de cadenas de suministros e infraestructuras urbanas, por medio de la recolección de información en tiempo real, automatizando los procesos para procurar la eficiencia, mejoramiento del nivel de vida, brindando comodidad al usuario, además de dar impulso tanto a la innovación, como también a la competitividad económica.

2.1.2. Arquitectura IoT

Aunque los modelos TCP/IP y OSI han sido fundamentales para las redes tradicionales, las complejidades y requisitos del IoT exigen un modelo más flexible. Esto se debe a la diversidad de dispositivos IoT, que tienen funcionalidades variadas, diferentes necesidades de comunicación y recursos limitados, lo que representa un desafío para las arquitecturas existentes. Además, la naturaleza dinámica y la necesidad de escalabilidad en IoT suman complicaciones, mientras que los problemas de seguridad y privacidad requieren soluciones especializadas. la Figura 12 se muestra la arquitectura IoT de tres, cuatro y cinco capas. Por lo tanto, los modelos de red tradicionales no son suficientes para cubrir las demandas de IoT. Es esencial desarrollar una arquitectura que aborde estos retos, pero aún no existe un acuerdo generalizado ni un modelo estándar para la arquitectura de IoT, pese a los esfuerzos incesantes en investigación e industria (Kalla et al., 2019).

Figura 12.

Tipos de arquitectura IoT tres, cuatro y 5 capas



Nota. Referencia (Peris, 2021).

En el esquema de tres niveles, cada nivel lleva a cabo las tareas siguientes:

- La capa de aplicación: Esta se ocupa en ofrecer servicios/ funcionalidades tanto a los usuarios como a otros sistemas, basándose en la información procesada y analizada. Esta capa abarca interfaces para usuarios, automatización, gestión e integración de información.
- La capa de red o de comunicación: Gestiona el enrutamiento y transmisión eficiente de datos a través de las redes. Todo esto se logra a través de la conexión de diversos dispositivos con la ayuda de protocolos y tecnologías de comunicación. Siendo esto crucial, para el establecimiento de conexiones con otros dispositivos, servidores e infraestructura de red, para la transferencia y tratamiento de datos a través de sensores de manera eficiente.
- La capa de percepción o de dispositivo: Funciona como interfaz entre los objetos físicos, permitiendo a los dispositivos IoT interactuar con su entorno. Su función principal es recopilar datos y transmitirlos a las capas superiores, además ayuda a la identificación de otros objetos inteligentes presentes en el área. Esta capa incluye una variedad de sensores, como en teléfonos inteligentes hasta sensores biométricos o químicos empleados en dispositivos de la salud.

En el modelo de cinco capas, como se ve en la Figura 13, además de las tres básicas (percepción, red y aplicación), las capas adicionales son:

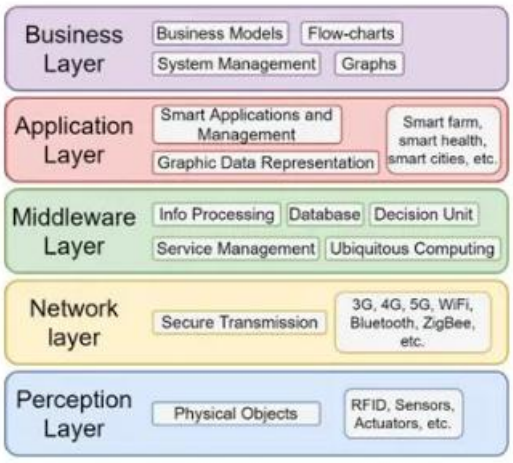
- La capa de procesamiento, o middleware, la cual ayuda al almacenamiento, análisis y procesamiento de los datos provenientes de la capa de red. Todo esto a través de tecnologías como big data, bases de datos, computación en la nube e inteligencia

artificial, con el objeto de gestionar grandes volúmenes de información, donde se tiene como funciones tanto el análisis de datos como la localización de anomalías. Además, proporciona servicios a las capas inferiores de la infraestructura IoT.

- La capa de negocio se encarga de la gestión global del sistema IoT, abarcando aspectos como privacidad del usuario, aplicaciones y análisis de datos.

Figura 13.

Arquitectura IoT de cinco capas



Nota. Referencia (Peris, 2021).

2.1.3. Redes de corto alcance y bajo consumo

Son aquellas de corto alcance, como también de consumo bajo, ideales para hogares, oficinas y otros espacios reducidos. Generalmente requieren baterías pequeñas y su utilización es bastante económica (Azure, 2024). A continuación, se presenta ejemplos comunes:

- Bluetooth: Trasmite voz y datos a un rango de 10 metros, siendo ideal para la transmisión de datos a una velocidad alta.
- NFC: Son un conjunto de protocolos que sirves para la comunicación entre dos dispositivos electrónicos, los cuales están localizados a una distancia de 4cm o menos. Estos proporcionan una conexión como una velocidad baja, a través de una simple configuración, lo cual permite la iniciación de conexiones inalámbricas cuya capacidad es mayor.
- Wi-Fi/802.11: Aunque este tenga bajo costo con respecto a la utilización del WI-FI y a su vez sea utilizado tanto en hogares como oficinas, el mismo no es adecuado para todos los escenarios, tanto por su consumo ininterrumpido energético y su limitado alcance.

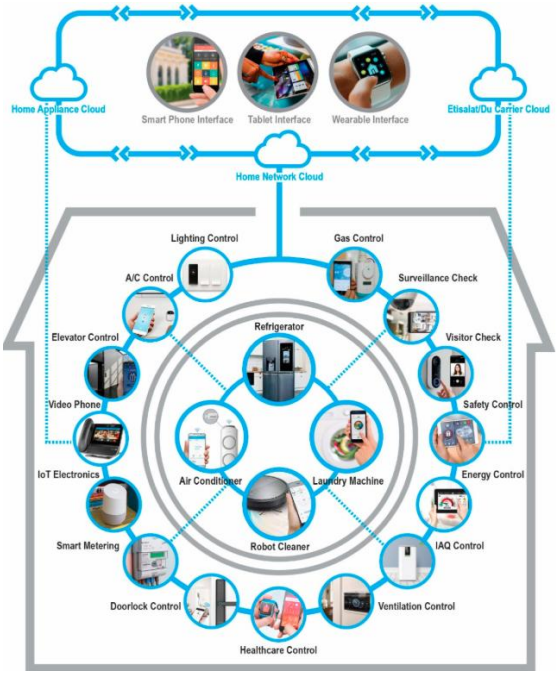
- Z-Wave: Es una red en malla, la cual uso ondas de radio de baja potencia para comunicar los dispositivos.
- Zigbee: Se basa en IEEE 802.15.4 para una serie de protocolos de comunicación de alto nivel, que se utilizan para el establecimiento de redes de área personal con una radio digital de baja potencia y pequeña en tamaño (Azure, 2024).

2.1.4. Aplicación en hogares

En el ámbito doméstico Figura 14, IoT abarca dispositivos como: bombillas, altavoces, cámaras de seguridad para hogares, detectores de humo inteligentes, sistemas de altoparlantes multi-habitación, etc. Que se conectan a un gateway (enrutador) que facilita su comunicación entre sí y mediante un teléfono inteligente, tableta inteligente o reloj inteligente se puede controlar.

Figura 14.

Casa inteligente con dispositivos IoT



Nota. Referencia (Arar et al., 2021).

En el contexto de hogares el termino smart home hace referencia a una residencia equipada con tecnologias que permiten la automatización y control remoto de diversos aspectos en un entorno doméstico mediante un ordenador o smartphone, la principal carcteristica de estos dispositivos es que se conectan a internet. Existen varios dispositivos inteligentes para el

hogar como se muestra en la tabla 1, junto a sus principales características (García y Apolinario, 2024).

Tabla 1.

Tipos de dispositivos IoT para el hogar

DISPOSITIVOS	CARACTERÍSTICAS PRINCIPALES
Asistentes virtuales	- Interacción conversacional - Automatización de tareas - Capacidad de procesamiento de lenguaje natural reconocimiento de voz
Iluminación inteligente	- Control remoto - Eficiencia energética - Ajuste de intensidad de brillo y color
Termostatos inteligentes	- Automatización - Ahorro energético - Programación de horarios
Detectores y sensores	- Detección de movimiento - Detección de humo - Sensores de puertas y ventanas
Cámaras de seguridad inteligente	- Conectividad Wifi - Detección de sonido y movimiento - Resolución 4K / FULLHD / HD, visión nocturna, audio
Electrodomésticos inteligentes	- Control mediante apps - Monitoreo y notificaciones - Integración con asistentes virtuales, funciones especiales
Enchufes y regletas inteligentes	- Control de energía - Programación remota, monitoreo de consumo energético - Protección contra sobrecargas de voltaje
Wereables	- Monitoreo de salud, de estrés y actividad física - Notificaciones en tiempo real y GPS integrado - Pagos móviles

Nota. Referencia (García y Apolinario, 2024).

2.1.5. Vulnerabilidades IoT

Para la reducción de los riesgos y garantizar la seguridad de los sistemas IoT, es esencial entender sus vulnerabilidades. En este sentido, la lista de las 10 principales debilidades de seguridad de los dispositivos IoT, compilada por OWASP, ofrece una visión clara de las fallas más frecuentes, como se ve en la Tabla 2. Estas incluyen contraseñas débiles, servicios de red inseguros, falta de actualizaciones, componentes desactualizados y configuraciones predeterminadas vulnerables (Toback, 2024). La lista resalta los desafíos que enfrentan tanto los usuarios como las empresas para proteger sus dispositivos IoT. A continuación, se detalla:

- Contraseñas débiles o codificadas: Usar credenciales fáciles de adivinar o almacenadas de manera insegura puede permitir accesos no autorizados.

- Servicios de red inseguros: Los servicios innecesarios o vulnerables pueden comprometer la seguridad de los dispositivos.
- Interfaces inseguras: Interfaces no protegidas, como APIs o accesos web, pueden permitir comprometer los dispositivos.
- Falta de actualizaciones: La ausencia de actualizaciones seguras o la incapacidad para validar el firmware deja los dispositivos expuestos a ataques.
- Componentes inseguros/obsoletos: La utilización de software o hardware de terceros vulnerables puede incrementar el riesgo de explotación.
- Protección de privacidad deficiente: El almacenamiento inseguro de datos del usuario puede comprometer la privacidad y la confianza.
- Transmisiones inseguras: La falta de cifrado en la transferencia de datos permite la interceptación y manipulación.
- Falta de administración: La ausencia de prácticas de gestión y monitoreo de seguridad deja a los dispositivos vulnerables a ataques.
- Configuraciones predeterminadas inseguras: Muchos dispositivos vienen con configuraciones predeterminadas que no se pueden mejorar fácilmente.
- Falta de refuerzo físico: La falta de medidas de protección ante ataques físicos aumenta el riesgo de que los sistemas sean comprometidos.

Tabla 2.

Vulnerabilidades IoT más comunes según OWASP

1	Contraseñas débiles o codificadas
2	Servicios de red inseguros
3	Interfaces inseguras
4	Falta de actualizaciones
5	Componentes inseguros u obsoletos
6	Protección de privacidad deficiente
7	Transmisiones inseguras
8	Falta de administración
9	Configuraciones predeterminadas inseguras
10	Falta de refuerzo físico

Nota. Referencia (Sasi et al., 2024).

Aparte de las vulnerabilidades de OWASP, otros factores que afectan la seguridad de los dispositivos IoT incluyen falta de protección adecuada, diversidad de dispositivos y protocolos, y los problemas derivados de la incapacidad de actualizar o mantener los dispositivos.

Control de acceso inadecuado

Es una vulnerabilidad común en los dispositivos IoT, ya que muchos no requieren contraseñas seguras ni el cambio de las predeterminadas. Además, frecuentemente se otorgan privilegios elevados a los usuarios y no se implementan métodos de verificación más robustos, como la autenticación multifactorial, que podría combinar contraseñas, tarjetas de acceso o biometría para mejorar la seguridad.

Falta de filtrado de tráfico

Muchos dispositivos IoT no filtran el tráfico de manera adecuada, lo que permite que el tráfico malicioso, como en los ataques DDoS, sobrecargue la red y dificulte la respuesta a solicitudes legítimas.

Protocolos de comunicación inseguros

Vulnerabilidades en protocolos como MQTT y CoAP pueden ser explotadas por atacantes para la intercepción, modificación o falsificación de las comunicaciones, complicando la integridad de los datos y controlando los sistemas afectados.

Prácticas de programación débiles

Muchas actualizaciones de firmware o software conservan vulnerabilidades conocidas debido a malas prácticas de programación, lo que deja a los dispositivos expuestos a ataques.

Energía insuficiente

Los dispositivos IoT con fuentes de energía limitadas pueden agotarse rápidamente cuando son bombardeados con mensajes, lo que impide su funcionamiento legítimo.

Falta de sistemas de cifrado

Un gran porcentaje de dispositivos IoT no cifran sus datos, dejando el 98% de su tráfico sin protección, lo que expone la información confidencial de los usuarios a posibles atacantes.

2.1.6. Aprendizaje automático (Machine Learning)

Es un tipo de inteligencia artificial (IA), que permite a las computadoras (y a dispositivos de IoT) aprender de los datos, identificar patrones y hacer predicciones sin programación explícita. Es un potente procesador de datos que aprende de la experiencia de manera eficaz y se reprograma a sí mismo (Intellias, 2024).

Métodos de machine learning

Machine learning supervisado

Son aquellos que utilizan conjuntos de datos etiquetados para entrenar algoritmos estos son categorizados o predicen resultados con exactitud a medida que se introducen datos de entrada en el modelo. Este modelo modifica las ponderaciones hasta su ajustable correcto. Además, este aprendizaje posibilita a las empresas afrontar varios problemas prácticos de gran envergadura como identificar y trasladar automáticamente el correo no deseado a una carpeta diferente.

Machine learning no supervisado

Es el que gestiona algoritmos para el análisis y agrupación de grupos de datos no etiquetados (subgrupos conocidos como clústeres). Los algoritmos se generan con el objetivo de identificar patrones de datos que pueden estar escondidos o agrupados, todo esto sin la intervención humana. Este procedimiento tiene la capacidad de identificar analogías y/o discrepancias en la información. Este es perfecto para múltiples usos como el análisis exploratorio de datos, las tácticas de venta cruzada, la segmentación de clientes y la identificación de imágenes y patrones.

Machine learning semisupervisado

Ofrece un equilibrio entre los dos tipos de aprendizajes antes vistos. Empleando un grupo limitado de datos etiquetados para guiar la clasificación y obtener características de un grupo más amplio de datos sin etiquetar. Este método resuelve el problema de la escasez de datos etiquetados adecuados para un algoritmo supervisado y resulta beneficioso cuando etiquetar grandes volúmenes de datos es excesivamente costoso(IBM, 2025)**.**

2.1.7. Aprendizaje automático (Machine Learning ML) e Internet de las Cosas (IoT)

Los dispositivos IoT son sensores inteligentes que capturan una gran cantidad de datos. Por ejemplo, su reloj de actividad física o anillo inteligente es un dispositivo IoT complejo que recopila datos sobre su actividad diaria. Pero son las capacidades de aprendizaje automático asociadas las que lo convierten en un dispositivo inteligente. Los algoritmos de IA/ML procesan todos esos datos para decirle cuántas calorías quemó durante su última carrera o con qué frecuencia se despertó anoche (Intellias, 2024).

En la Tabla 3, podemos observar que los datos son el vínculo entre el aprendizaje automático y el internet de las cosas, los dispositivos IoT producen grandes volúmenes de datos y los algoritmos de aprendizaje automático se benefician de ellos, estas dos tecnologías en conjunto

permiten descubrir información y patrones que serían imposibles de identificar por los seres humanos.

Tabla 3.

Aprendizaje automático e internet de las cosas

Características	Internet de las cosas (IoT)	Aprendizaje automático (ML)
¿Qué hace?	Conecta dispositivos y recopila datos.	Analiza datos para descubrir patrones.
Datos	Genera grandes cantidades para su análisis.	Funciona mejor cuando se proporcionan grandes volúmenes de datos.
Inteligencia	Sin inteligencia inherente.	Aprende y mejora con el tiempo.
Aplicaciones	Relojes inteligentes, rastreadores de actividad física, audífonos inteligentes, gafas inteligentes, hogares inteligentes, dispositivos médicos conectados, maquinaria conectada.	Personalización, detección de voz, clasificación de actividades, procesamiento del lenguaje natural, detección de anomalías.

Nota. Referencia (Intellias, 2024).

2.1.8. Tipos de ataques

La ciberseguridad es muy importante, protege sistemas informáticos, base de datos y redes contra ciberataques y accesos no autorizados garantizando la seguridad de la información y este se basa en principios de la confidencialidad, integridad y disponibilidad. A continuación, se presenta una sinopsis de los ciberataques más comunes (García y Apolinario, 2024).

Tabla 4.

Tipos de ataques

Tipos de Ataques	Impacto	Objetivo principal	Consecuencias
Ransomware	ALTO	Encriptar datos	- Bloquear acceso a los datos - Pago por rescate
Phishing	ALTO	Obtener información confidencial	- Accesos no autorizados a cuentas financieras - Robo de identidad
Inyección SQL	ALTO	Acceder a las bases de datos	- Acceso a datos sensibles - Modificación o eliminación de datos.
Cross – Site – Scripting (XSS)	MEDIO	Inyectar Scripts en sitios web	- Suplantación de identidad - Robo de cookies
Denegación de Servicio Distribuida (DDoS)	MEDIO	Sobrecargar servicios	- Interrupción de los servicios - Daño a la reputación
Adware	BAJO	Mostrar publicidad no deseada	- Afectar el rendimiento del sistema - Exposición a malware

Nota. Referencia (García y Apolinario, 2024).

2.2. Descripción de la propuesta

En este momento, el uso de dispositivos IoT cada vez es más frecuente en los hogares ya que pueden estar presentes en un pequeño enchufe inteligente o cámaras inteligentes conectados al internet estos dispositivos pueden sufrir un ciberataque. Por lo que es de gran importancia, el mantenimiento la seguridad de todos los dispositivos utilizados en un hogar inteligente.

Para mitigar estos riesgos respecto al uso de aprendizaje automático (machine learning), se puede recopilar los datos de los dispositivos IoT mediante las plataformas AWS IoT (plataforma de la nube de Amazon), Azure IoT (plataforma de la nube de Microsoft) y Google Cloud IoT (plataforma de Google), con el uso de estas plataformas se puede monitorear y detectar anomalías en el comportamiento de todos los dispositivos IoT que estén conectados en un hogar, en el Anexo 3 se observa la guía propuesta.

a. Estructura general

A continuación, se puede visualizar el bosquejo general del proyecto desarrollado (Figura 15), donde se detalla las fases que posee el mismo.

Figura 15.

Guía para el uso de dispositivos IoT de tipo doméstico

Nota. Elaboración propia.

b. Explicación del aporte

El proyecto de investigación inició con la investigación de los dispositivos IoT de tipo doméstico y las vulnerabilidades de los mismos. El siguiente proceso se basa en recopilar los datos de los dispositivos IoT mediante las plataformas AWS IoT, Azure IoT y Google Cloud IoT, escanear la red, esto ayudará a la determinación de las debilidades que se localizan en el hogar y aplicar las estrategias de mitigación.

Dispositivos IoT de tipo hogar

En esta parte se identifica los principales dispositivos IoT Asistentes virtuales, iluminación inteligente, termostatos inteligentes, detectores y sensores, cámaras de seguridad inteligentes, electrodomésticos inteligentes, enchufes y regletas inteligentes, wereables, estos dispositivos permiten automatizar tareas creando entornos más eficientes.

Recopilación de información

Mediante las plataformas AWS IoT, Azure IoT y Google Cloud IoT podemos monitorear los dispositivos IoT y detectar anomalías gracias a la gran cantidad de datos que se administra en las plataformas con el propósito de generar estrategias de mitigación.

Identificación de vulnerabilidades en dispositivos IoT de tipo hogar

Con toda la recopilación de la información obtenida de cada dispositivo IoT, se puede identificar las brechas de vulnerabilidad como: contraseñas débiles o codificadas, servicios de red inseguros, interfaces inseguras, ausencia de actualizaciones en los dispositivos IoT, componentes inseguros o anticuados, insuficiente protección de la privacidad, transmisiones inseguras, ausencia de gestión, configuraciones preestablecidas inseguras, ausencia de fortalecimiento.

Tipos de ataques

En un hogar inteligente los dispositivos IoT están cada vez más presentes esto permite que los usuarios sufran ataques de ciberdelincuentes que tiene el fin de extorsionar, causar daños o robar la información.

A continuación, se detalla los principales ataques:

Ransomware: Los atacantes pueden infectar con malware que pueden cifrar archivos o bloquear los dispositivos inteligentes, luego exigen un rescate para la liberación de los archivos.

Phishing: Mediante correos electrónicos los atacantes pueden intentar atacar a los usuarios para que proporcionen información personal como datos bancarios, contraseñas todo esto con enlaces o formularios de mala reputación.

Inyección SQL: En un hogar inteligente los dispositivos que están conectados a bases de datos pueden sufrir ataques por ciberdelincuentes mediando inyección SQL donde envían consultas para robar datos, modificar la configuración de equipos y hasta obtener accesos no autorizados.

Cros-Site-Scripting (XSS): Los ciberdelincuentes pueden atacar a través de las aplicaciones web que controlan a los dispositivos IoT, mediante el uso de scripts maliciosos insertados en las aplicaciones que esté haciendo uso el usuario, los ciberdelincuentes puedo robar cookies, datos se sesión sin el consentimiento de un usuario.

Denegación de servicios distribuida (DDoS): Los ciberdelincuentes inundan de tráfico masivo a los dispositivos IoT causando fallos en su funcionamiento o bloqueándolos completamente.

Aware: Los ciberdelincuentes atacan con software publicitario a los dispositivos IoT, robando datos personales de los usuarios, mostrando anuncios no deseados afectando la privacidad de los usuarios.

Aplicación de estrategias de mitigación

La información obtenida con aprendizaje automático mediante las plataformas AWS IoT, Azure IoT y Google Cloud IoT nos sirve para proponer las siguientes estrategias:

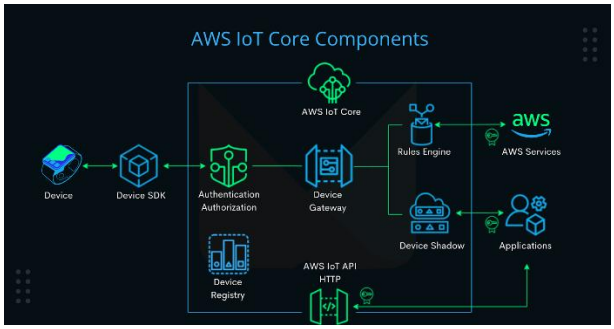
- Utilizar contraseñas seguras: Se recomienda contraseñas de al menos 12 caracteres que combinen tanto letras mayúsculas, como también minúsculas, adicionalmente se debe colocar números y signos especiales.
- Cambiar contraseñas predeterminadas: Las que viene de fábrica son fáciles de ser descifradas por los ciberdelincuentes es muy importante cambiar las mismas.
- Segmentar la red: Muy importante separar las redes en segmentos para limitar el acceso de los dispositivos IoT a otras redes.
- Actualizar el software constantemente: Con las actualizaciones constantes en los dispositivos garantiza que tenga todas las mejoras a nivel de la seguridad y ayuda a proteger de vulnerabilidades.
- Desactivar funciones no utilizadas: Al desactivar lo innecesario en los dispositivos IoT, disminuye los ciberataques.
- Sistema de detección de intrusiones (IDS): Es una herramienta diseñada para buscar vulnerabilidades, monitorea el tráfico e informa los resultados.

c. Estrategias y/o técnicas

Mediante el uso de las plataformas AWS IoT Figura 16, Azure IoT Figura 17 y Google Cloud IoT Figura 18, recopilamos la información de los dispositivos IoT y podemos analizar el comportamiento de los mismos.

Figura 16.

AWS IoT



Nota. Referencia (Cloud, 2025).

Figura 17.

Azure IoT

Nota. Referencia (Dsouza, 2025).

Figura 18.

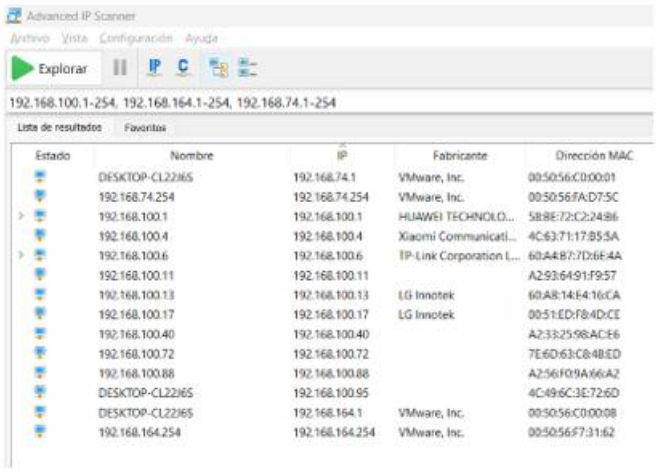
Google Cloud IoT

Nota. Referencia (Arif, 2023).

Con la herramienta gratuita de escaneo Advanced Ip Scanner se puede verificar cuantos dispositivos que están conectados en un hogar como se aprecia en la Figura 19.

Figura 19.

Escaneo de red local con la herramienta Advanced Ip Scanner



Nota. Referencia herramienta gratuita de escaneo Advanced Ip Scanner.

Con Kali Linux con la herramienta nmap se escanea toda la red hogar para determinar las vulnerabilidades a través de los puertos como se observa en la Figura 20.

Figura 20.

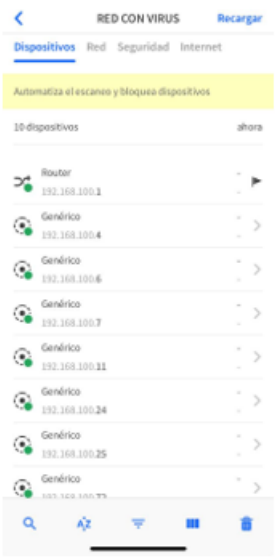
Escaneo con nmap en kali linux

Nota. Referencia sistema operativo Kali Linux.

Con la App gratuita Fing realizamos un escaneo rápido de toda la red en el hogar en la cual se identifica el dispositivo IoT que esté conectado y se puede ver la dirección ip, dirección mac y el fabricante del hardware observado en la Figura 21.

Figura 21 .

Escaneo de red con App Fing



Nota. Referencia App gratuita Fing.

Para mitigar los riesgos de dispositivos IoT de tipo doméstico considerar lo siguiente:

- Utilizar contraseñas seguras: Se recomienda contraseñas de al menos 12 caracteres que combinen letras mayúsculas, minúsculas, números y signos especiales.
- Cambiar contraseñas predeterminadas: Las contraseñas que viene de fábrica son fáciles de ser descifradas por los ciberdelincuentes es muy importante cambiar las mismas.
- Segmentar la red: Muy importante separar las redes en segmentos para limitar el acceso de los dispositivos IoT a otras redes.
- Actualizar el software constantemente: Con las actualizaciones constantes en los dispositivos garantiza que tenga todas las mejoras a nivel de la seguridad y ayuda a proteger de vulnerabilidades.
- Desactivar funciones no utilizadas: Al desactivar lo innecesario en los dispositivos IoT, disminuye los ciberataques.
- Sistema de detección de intrusiones (IDS): Es una herramienta diseñada para buscar vulnerabilidades, monitorea el tráfico e informa los resultados.

2.3. Validación de la propuesta

En esta parte del estudio, se contó con el aporte y conocimiento de especialistas, el cual fue necesario para evaluar la propuesta de la guía para el uso de dispositivos IoT de tipo doméstico y estrategias de mitigación basadas en aprendizaje automático.

- Especialista #1. Ing. Francisco Valverde PhD
- Especialista #2. Ing. Alex Cruz Mg

En el Anexo 2 se adjunta la validación de los especiales.

2.4. Matriz de articulación de la propuesta

En este punto, se presenta la matriz de articulación que resume una guía planteada, junto con los fundamenticos teóricos, enfoques metodológicos y estrategias empleadas.

Tabla 5.

Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Investigación de dispositivos IoT de tipo doméstico.	Teoría de Internet de las cosas (IoT) y tipos de dispositivos IoT de tipo doméstico.	Metodología bibliográfica, revisión de artículos y tesis.	Fuente bibliográfica.	Definir el concepto de IoT y dispositivos IoT de tipo doméstico.	Fuente bibliográfica.
Vulnerabilidades en dispositivos IoT de tipo doméstico.	Teoría de las vulnerabilidades más comunes de dispositivos IoT de tipo doméstico.	Gracias a los métodos de investigación bibliográfica se obtiene las principales vulnerabilidades.	Fuente bibliográfica.	Información necesaria para entender la propuesta.	Fuente bibliográfica.
Encuestas a profesionales en Seguridad Informática y Tecnologías de la Información (TI).	Investigación cuantitativa.	Encuestas a profesionales.	Elaboración de encuestas.	Los encuestados confirman que una guía es viable para que los usuarios hagan un buen uso de los dispositivos IoT	Encuestas.
Elaboración de guía.	Definiciones consideradas para la estructura.	Alcance descriptivo del procedimiento.	Elaboración del flujo del proceso.	Elaboración de estrategias de mitigación basadas en aprendizaje automático para el uso de dispositivos IoT de tipo doméstico.	Fuente bibliográfica, encuestas, herramientas para el análisis de las vulnerabilidades.

Nota. Elaboración propia

CONCLUSIONES

Es ineludible que se deben describir los fundamentos teóricos del IoT y de dispositivos IoT, para de esta manera mitigar las vulnerabilidades de manera eficaz con ayuda de aprendizaje automático, estas estrategias de mitigación deben adaptarse a las características de los dispositivos IoT en el ambiente en el que se utilicen.

Las vulnerabilidades existentes en los dispositivos IoT de tipo doméstico, pueden ser manipulados por los ciberdelincuentes para el robo de datos/ información como también para la posesión del control de los dispositivos, en pro de asegurar la seguridad en los dispositivos IoT deben aplicarse estrategias anticipadas que mitiguen las vulnerabilidades, es muy importante que los usuarios conozcan las amenazas que puede afectar en su hogar.

Es muy importante diseñar una guía de estrategias de mitigación basadas en aprendizaje automático para que los usuarios hagan un buen uso de dispositivos IoT de tipo doméstico, estas estrategias garantizan la integridad y confiabilidad de los datos que transmitan los dispositivos IoT, adicional es de suma importancia estar actualizado con las nuevas tecnologías y seguridad que cuentan los dispositivos IoT.

El criterio de los especialistas fue un factor decisivo importante para la realización de la propuesta, su experiencia permitió el identificar posibles riesgos en los dispositivos IoT de tipo hogar. Estas sugerencias incorporar en la guía garantiza las mejores prácticas de seguridad.

RECOMENDACIONES

Se recomienda la implementación de una guía para el uso de dispositivos IoT de tipo doméstico y estrategias de mitigación basadas en aprendizaje automático.

Se sugiere técnicas avanzadas de aprendizaje automático para la recopilación de los datos de los dispositivos IoT y poder generar estrategias para mitigar el riesgo en los dispositivos IoT de tipo doméstico.

Se recomienda para una siguiente etapa en la investigación, la guía se socialice de manera general hacia los sectores empresariales, educativos, industriales y financieros, campos donde están presentes los dispositivos IoT.

Se recomienda crear una red exclusiva para la conexión de los dispositivos IoT de tipo hogar al internet todo esto avalado por especialistas en Seguridad Informática.

BIBLIOGRAFÍA

Arar, M., Jung, C., Awad, Y., & Chohan, A. (5 de Noviembre de 2021). *designs*. Obtenido de Analysis of Smart Home Technology Acceptance and Preference for Elderly in Dubai, UAE: https://doi.org/10.3390/designs5040070

Arif, R. (19 de Diciembre de 2023). *Rise Up Labs*. Obtenido de Google Cloud IoT Solutions Guide: https://riseuplabs.com/google-cloud-iot-solutions-guide/

Atiaja, D. (03 de 2024). *Propuesta de un manual de políticas de seguridad para el proceso de comunicación entre los dispositivos IoT, mediante métodos de encriptación.* Obtenido de http://repositorio.uisrael.edu.ec/handle/47000/4070

Azure, M. (2024). Obtenido de Protocolos y tecnologías de IoT: https://azure.microsoft.com/es-mx/solutions/iot/iot-technology-protocols

BBVA. (15 de Julio de 2024). *'Machine learning': ¿qué es y cómo funciona el maestro en reconocer patrones?* Obtenido de https://www.bbva.com/es/innovacion/machine-learning-que-es-y-como-funciona/

Bermudez, A. (2022). *Ciberseguridad en los servicios que usan dispositivos IoT para los usuarios del sector residencial*. Obtenido de UNIVERSIDAD LATINA DE COSTARICA: https://repositorio.ulatina.ac.cr/bitstream/20.500.12411/1697/1/TFG_Ulatina_Aurora_Bermudez_Lopez_200403009921.pdf

Cloud Ausum. (2025). *¿Qué es la plataforma AWS IoT Core?* Obtenido de ausum cloud: https://ausum.cloud/aws-iot-core/

Dsouza, R. (18 de Febrero de 2025). *Bacancy*. Obtenido de Azure IoT Hub: su puerta de entrada a soluciones de IoT más inteligentes: https://www.bacancytechnology.com/blog/what-is-azure-iot-hub

García, K., & Apolinario, O. (21 de Agosto de 2024). *Minerva Journal*. doi:https://doi.org/10.47460/minerva.v5i15.171

IBM. (Febrero de 2025). *IBM*. Obtenido de ¿Qué es el machine learning (ML)?: https://www.ibm.com/es-es/topics/machine-learning

IBM. (25 de Julio de 2025). *Internet de las cosas*. Obtenido de www.ibm.com: https://www.ibm.com/mx-es/topics/internet-of-things

Intellias. (22 de Noviembre de 2024). Obtenido de El uso del aprendizaje automático en la IoT: una combinación perfecta para la innovación: https://intellias.com/machine-learning-in-iot/

Peris, J. (29 de 07 de 2021). *Service Management Institute*. Obtenido de Arquitectura de la ciberseguridad basado en IoT: https://news.itsmf.es/arquitectura-de-la-ciberseguridad-basado-en-iot/

Ruiz et al. (2023). *Regulaciones globales para la seguridad en IOT : Un análisis comparativo.* Derecho y Tecnología.

Toback, M. (27 de Agosto de 2024). *OWASP IoT Top 10 Vulnerabilities.* Obtenido de smallbizepp.com: https://smallbizepp.com/owasp-iot-top-10-vulnerabilities/

Villacís, B. (Marzo de 2024). *Análisis de Vulnerabilidades basado en Técnicas de Inteligencia Artificial para la Seguridad Informática en Redes de Área Local.* Obtenido de http://repositorio.uisrael.edu.ec/handle/47000/4140

.

ANEXOS

ANEXO 1: Formato de encuesta

GUÍA PARA EL USO DE DISPOSITIVOS IOT DE TIPO DOMÉSTICO Y ESTRATEGIAS DE MITIGACIÓN BASADAS EN APRENDIZAJE AUTOMÁTICO

La siguiente encuesta tiene como objetivo recopilar datos sobre las vulnerabilidades en dispositivos IoT de tipo doméstico. Su participación nos ayudara a proponer estrategias de mitigación basadas en aprendizaje automático. La información que se recopile se usaran únicamente con fines investigativos.

1. ¿Qué nivel de conocimiento tiene sobre Internet de las Cosas (IoT)?

- Alto
- Moderado
- Bajo
- Ninguno

2. ¿Conoce las vulnerabilidades de seguridad, en los dispositivos IoT de uso doméstico?

- Si
- No
- Algo

3. ¿Cómo evaluaría el grado de conocimiento de los usuarios sobre las amenazas de seguridad de los dispositivos IoT de tipo doméstico?

- ○ Alto
- ○ Medio
- ○ Bajo
- ○ Ninguno

4. ¿Qué tipo de vulnerabilidades son más frecuentes en los dispositivos IoT domésticos?

- ○ Accesos no autorizados
- ○ Fugas de datos personales
- ○ Conexiones inseguras
- ○ Ataques de botnet

5. ¿En su hogar utiliza alguna herramienta de seguridad para proteger los dispositivos IoT?

- ○ Si
- ○ No

6. ¿Cree que el uso de aprendizaje automático (machine learning) puede mejorar la detección de amenazas en dispositivos IoT, de tipo doméstico?

- ○ Si
- ○ No
- ○ No estoy seguro

7. ¿En qué área considera que el aprendizaje automático podría tener un mayor impacto?

- ☐ Detección de intrusiones
- ☐ Monitoreo en tiempo real de dispositivos
- ☐ Predicción de vulnerabilidades
- ☐ Gestión de contraseñas y autenticación

8. ¿Estaría dispuesto a implementar soluciones basadas en aprendizaje automático para mejorar la seguridad de los dispositivos IoT de tipo doméstico?

- ○ Muy dispuesto
- ○ Algo dispuesto
- ○ Poco dispuesto
- ○ Nada dispuesto

9. ¿Qué factor considera como desafío para implementar soluciones basadas en aprendizaje automático para la seguridad de los dispositivos IoT de tipo doméstico?

- ○ Costo
- ○ Complejidad en la implementación
- ○ Falta de conocimiento o capacitación
- ○ Preocupaciones sobre la privacidad de los datos

10. ¿Qué medidas de seguridad recomienda implementar para proteger los dispositivos IoT en un hogar?

- ☐ Utilizar contraseñas seguras
- ☐ Cambiar contraseñas predeterminadas
- ☐ Segmentación de redes
- ☐ Actualización constante del firmware
- ☐ Sistema de detección de intrusiones (IDS)

11. ¿Qué tipo de recursos considera necesarios para ayudar a los usuarios a mejorar la seguridad de sus dispositivos IoT de tipo doméstico?

- ○ Guía y estrategias de mitigación
- ○ Recomendaciones de herramientas
- ○ Actualizaciones sobre nuevas vulnerabilidades

ANEXO 2: Resultados de la encuesta

10 respuestas

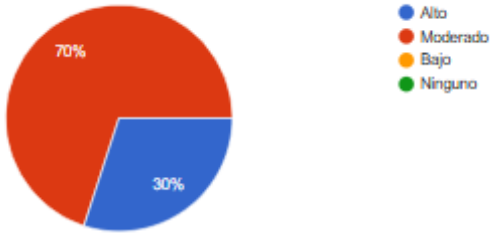
Ver en Hojas de cálculo

Resumen | Pregunta | Individual

1. ¿Qué nivel de conocimiento tiene sobre Internet de las Cosas (IoT)?

Copiar gráfico

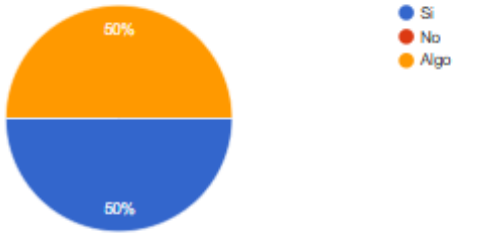
10 respuestas



2. ¿Conoce las vulnerabilidades de seguridad, en los dispositivos IoT de uso doméstico?

Copiar gráfico

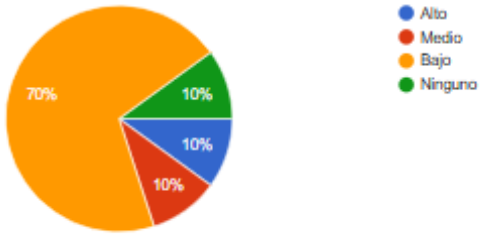
10 respuestas



3. ¿Cómo evaluaría el grado de conocimiento de los usuarios sobre las amenazas de seguridad de los dispositivos IoT de tipo doméstico?

Copiar gráfico

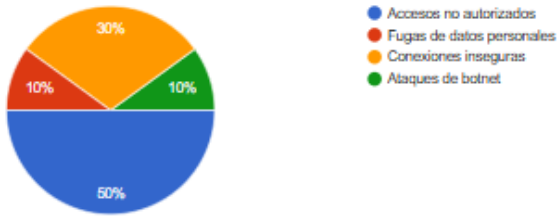
10 respuestas



4. ¿Qué tipo de vulnerabilidades son más frecuentes en los dispositivos IoT domésticos?

Copiar gráfico

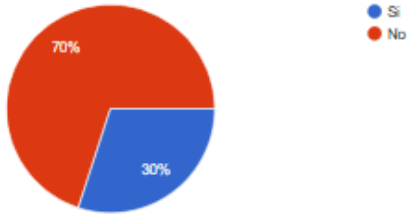
10 respuestas



5. ¿En su hogar utiliza alguna herramienta de seguridad para proteger los dispositivos IoT?

Copiar gráfico

10 respuestas



6. ¿Cree que el uso de aprendizaje automático (machine learning) puede mejorar la detección de amenazas en dispositivos IoT, de tipo doméstico?

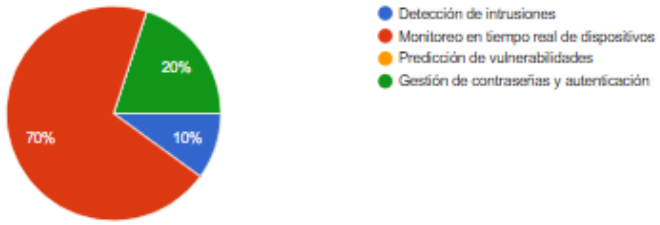
Copiar gráfico

10 respuestas

7. ¿En qué área considera que el aprendizaje automático podría tener un mayor impacto?

Copiar gráfico

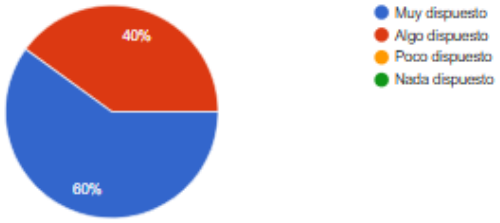
10 respuestas



8. ¿Estaría dispuesto a implementar soluciones basadas en aprendizaje automático para mejorar la seguridad de los dispositivos IoT de tipo doméstico?

Copiar gráfico

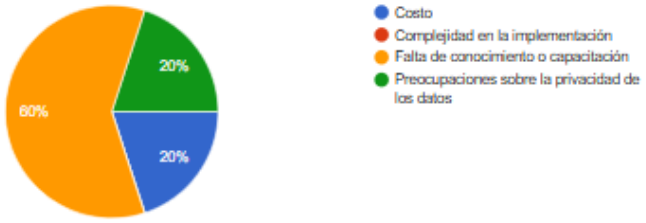
10 respuestas



9. ¿Qué factor considera como desafío para implementar soluciones basadas en aprendizaje automático para la seguridad de los dispositivos IoT de tipo doméstico?

Copiar gráfico

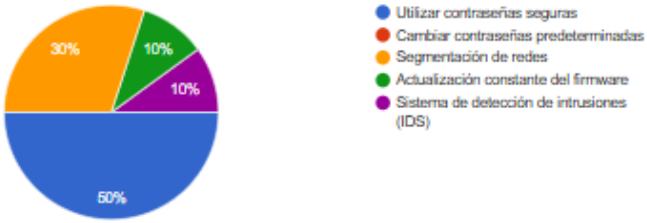
10 respuestas



10.¿Qué medidas de seguridad recomienda implementar para proteger los dispositivos IoT en un hogar?

Copiar gráfico

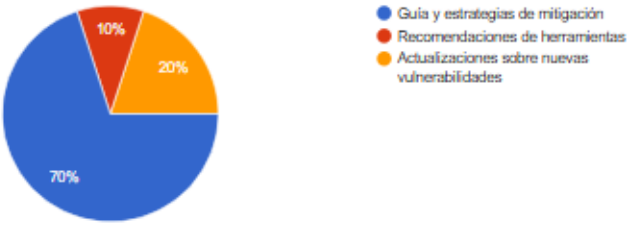
10 respuestas



11. ¿Qué tipo de recursos considera necesarios para ayudar a los usuarios a mejorar la seguridad de sus dispositivos IoT de tipo doméstico?

Copiar gráfico

10 respuestas



ANEXO 3: Validación de especialistas

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"Guía para el uso de dispositivos IoT de tipo doméstico y estrategias de mitigación basadas en aprendizaje automático"**. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: FRANCISCO VALVERDE
Título obtenido: PhD en Informática
C.I.: 1712156684
E-mail: fvalverde@uisrael.edu.ec
Institución de Trabajo: Universidad Israel
Cargo: Docente
Años de experiencia en el área: 15

Universidad Israel

ESPOG | Escuela de Posgrados

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "Guía para el uso de dispositivos IoT de tipo doméstico y estrategias de mitigación basadas en aprendizaje automático"

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	x				
Aplicabilidad			x		
Factibilidad		x			
Novedad	x				
Fundamentación pedagógica	x				
Fundamentación tecnológica		x			
Indicaciones para su uso			x		
TOTAL	15	8	6		

Observaciones: El proyecto es innovador y viable.

Recomendaciones: Presentar diagramas de proceso del funcionamiento del o los elementos integrados de IoT en la guía por cada estrategia propuesta.

Lugar, fecha de validación: Quito, 08 de marzo de 2025

FRANCISCO XAVIER VALVERDE ALULEMA

Firmado digitalmente por FRANCISCO XAVIER VALVERDE ALULEMA
Fecha: 2025.03.08 21:48:10 -05'00'

Firma del especialista
Ing. Francisco Valverde PhD

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"Guía para el uso de dispositivos IoT de tipo doméstico y estrategias de mitigación basadas en aprendizaje automático"**. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Mg. Alex Samuel Cruz Román
Título obtenido: Ingeniero en Sistemas Informáticos y de Computación / Magister en Administración de Empresas Mención Finanzas
C.I.: 1709554040
E-mail: comercial@distritotech.com
Institución de Trabajo: Distrito Tech Ecuador S.A.
Cargo: Gerente General
Años de experiencia en el área: 22

Universidad Israel

ESPOG | Escuela de Posgrados

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "Guía para el uso de dispositivos IoT de tipo doméstico y estrategias de mitigación basadas en aprendizaje automático"

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	x				
Aplicabilidad	x				
Factibilidad	x				
Novedad	x				
Fundamentación pedagógica	x				
Fundamentación tecnológica	x				
Indicaciones para su uso	x				
TOTAL	35				

Observaciones: No se presentan observaciones, la guía es un recurso muy importante para los usuarios, el proyecto es viable.

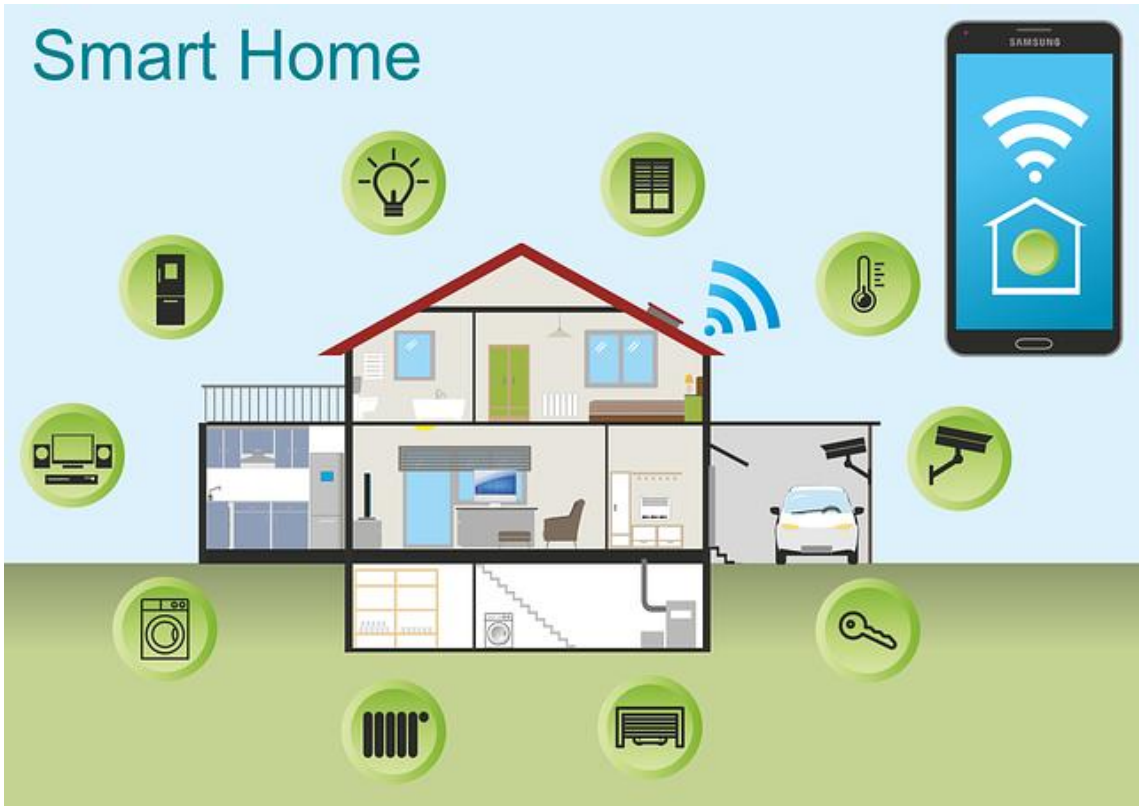
Recomendaciones: Los pasos descritos en la presente guía están bien detallados, por lo que es recomendable el uso de la misma.

Lugar, fecha de validación: Quito, 09 de marzo de 2025

Firma del especialista
Mg. Alex Cruz

ANEXO 3:

GUÍA PARA EL USO DE DISPOSITIVOS IOT DE TIPO DOMÉSTICO Y ESTRATEGIAS DE MITIGACIÓN BASADAS EN APRENDIZAJE AUTOMÁTICO



Responsable: Cristian Toapanta **marzo 2025**

Tabla de contenidos

1. Introducción

1.1. Contextualización del problema

Los dispositivos IoT (Internet de las cosas) han revolucionado la forma en que interactuamos con nuestro entorno, permitiendo la automatización de tareas y la mejora de la eficiencia energética en los hogares. Sin embargo, su expansión ha creado nuevas amenazas para la seguridad informática. Estos dispositivos son cada vez más comunes, pero muchos carecen de una protección adecuada, lo que los convierte en blancos vulnerables para los ciberdelincuentes.

1.2. Objetivo de la guía

El objetivo de esta guía es proporcionar un enfoque estructurado para la identificación y mitigación de vulnerabilidades en dispositivos IoT domésticos, utilizando aprendizaje automático para detectar anomalías y aplicar medidas preventivas de manera efectiva.

1.3. Público objetivo

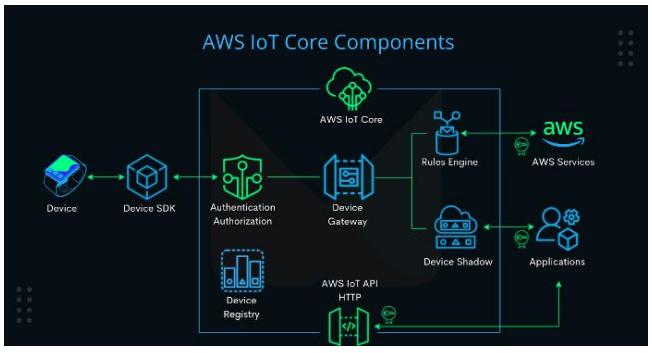
Esta guía está dirigida a hogares con dispositivos IoT, profesionales de la seguridad informática, desarrolladores de tecnología IoT y expertos en redes. También es útil para empresas tecnológicas y centros de investigación que deseen aplicar medidas de seguridad en dispositivos IoT.

1.4. Metodología utilizada

Se utilizaron plataformas de nube como AWS IoT, Azure IoT y Google Cloud IoT para la recopilación de datos de dispositivos, realizando un escaneo de la red para detectar vulnerabilidades y aplicar estrategias de mitigación basadas en aprendizaje automático.

Figura 22

AWS IoT



Nota. Referencia (Cloud, 2025).

Figura 23

Azure IoT

Nota. Referencia (Dsouza, 2025).

Figura 24

Google Cloud IoT

Nota. Referencia (Arif, 2023).

1.5. Cómo utilizar la guía

Esta guía proporciona pasos detallados sobre cómo implementar estrategias de mitigación para asegurar dispositivos IoT domésticos, empleando herramientas como AWS IoT, Azure IoT, Google Cloud IoT, y plataformas de escaneo como Advanced IP Scanner y Kali Linux.

2. Fundamentos Teóricos y Conceptuales

2.1. Revisión de conceptos

IoT (Internet de las cosas)

Conjunto de dispositivos físicos interconectados que recopilan y comparten datos. Estos incluyen asistentes virtuales, cámaras de seguridad, termostatos inteligentes, entre otros.

Vulnerabilidades en IoT

Los dispositivos IoT, por su naturaleza, pueden estar expuestos a riesgos como contraseñas débiles, conexiones inseguras y falta de actualizaciones de seguridad.

Aprendizaje Automático (Machine Learning)

Técnica que utiliza algoritmos para analizar grandes volúmenes de datos, detectar patrones y realizar predicciones sobre comportamientos sospechosos.

Redes de corto alcance y bajo consumo

Son aquellas cuyo alcance es corto y consumo es bajo, ideales para hogares, oficinas y otros espacios reducidos.

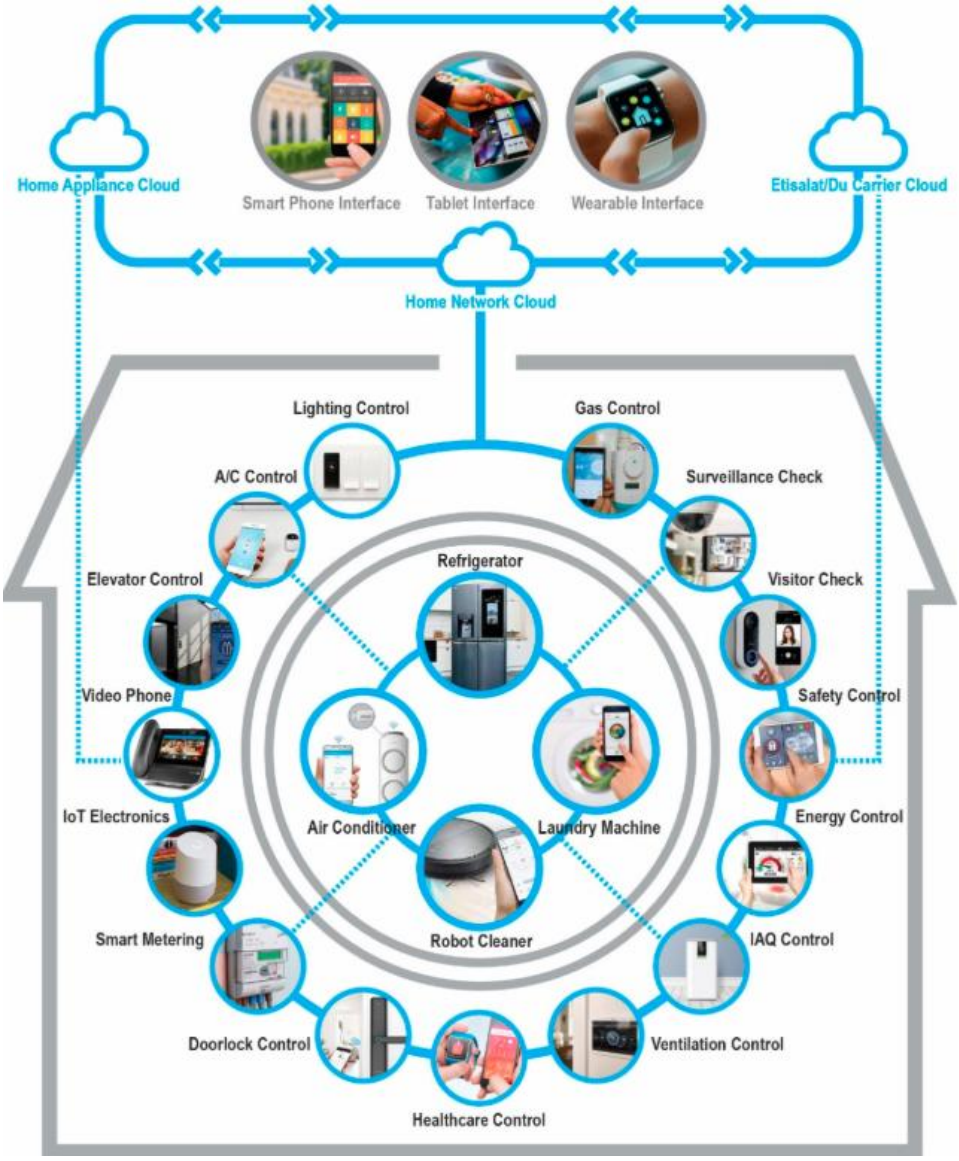
- Bluetooth: Trasmite voz y datos a un rango de 10 metros, siendo ideal para la transmisión de datos a una velocidad alta.
- NFC: Son un conjunto de protocolos que sirves para la comunicación entre dos dispositivos electrónicos, los cuales están localizados a una distancia de 4cm o menos. Estos proporcionan una conexión como una velocidad baja, a través de una simple configuración, lo cual permite la iniciación de conexiones inalámbricas cuya capacidad es mayor.
- Wi-Fi/802.11: Aunque este tenga bajo costo con respecto a la utilización del WI-FI y a su vez sea utilizado tanto en hogares como oficinas, el mismo no es adecuado para todos los escenarios, tanto por su consumo ininterrumpido energético y su limitado alcance.
- Z-Wave: Es una red en malla, la cual uso ondas de radio de baja potencia para comunicar los dispositivos.
- Zigbee: Se basa en IEEE 802.15.4 para una serie de protocolos de comunicación de alto nivel, que se utilizan para el establecimiento de redes de área personal con una radio digital de baja potencia y pequeña en tamaño (Azure, 2024).

Aplicación en hogares

En el ámbito doméstico Figura 4, IoT abarca dispositivos como: bombillas, altavoces, cámaras de seguridad para hogares, detectores de humo inteligentes, sistemas de altoparlantes multi-habitación etc. Que se conectan a un gateway (enrutador) que facilita su comunicación entre sí y mediante un teléfono inteligente, tableta inteligente o reloj inteligente se puede controlar. En la Tabla 1 se valida las características de los dispositivos.

Figura 25

Casa inteligente con dispositivos IoT



Nota. Referencia (Arar et al., 2021).

Tabla 6

Tipos de dispositivos IoT para el hogar

DISPOSITIVOS	CARACTERÍSTICAS PRINCIPALES
Asistentes virtuales	- Interacción conversacional - Automatización de tareas - Capacidad de procesamiento de lenguaje natural reconocimiento de voz
Iluminación inteligente	- Control remoto - Eficiencia energética - Ajuste de intensidad de brillo y color
Termostatos inteligentes	- Automatización - Ahorro energético - Programación de horarios
Detectores y sensores	- Detección de movimiento - Detección de humo - Sensores de puertas y ventanas
Cámaras de seguridad inteligente	- Conectividad Wifi - Detección de sonido y movimiento - Resolución 4K / FULLHD / HD, visión nocturna, audio
Electrodomésticos inteligentes	- Control mediante apps - Monitoreo y notificaciones - Integración con asistentes virtuales, funciones especiales
Enchufes y regletas inteligentes	- Control de energía - Programación remota, monitoreo de consumo energético - Protección contra sobrecargas de voltaje
Wereables	- Monitoreo de salud, de estrés y actividad física - Notificaciones en tiempo real y GPS integrado - Pagos móviles

Nota. Referencia (García y Apolinario, 2024).

Tipo de ataques

La ciberseguridad es muy importante, protege sistemas informáticos, base de datos y redes contra ciberataques y accesos no autorizados garantizando la seguridad de la información y este se basa en principios de la confidencialidad, integridad y disponibilidad. A continuación, en la Tabla 4, se presenta una sinopsis de los ciberataques más comunes.

Tabla 7

Tipos de ataques

Tipos de Ataques	Impacto	Objetivo principal	Consecuencias
Ransomware	ALTO	Encriptar datos	- Bloquear acceso a los datos - Pago por rescate
Phishing	ALTO	Obtener información confidencial	- Accesos no autorizados a cuentas financieras - Robo de identidad
Inyección SQL	ALTO	Acceder a las bases de datos	- Acceso a datos sensibles - Modificación o eliminación de datos.
Cross – Site – Scripting (XSS)	MEDIO	Inyectar Scripts en sitios web	- Suplantación de identidad - Robo de cookies
Denegación de Servicio Distribuida (DDoS)	MEDIO	Sobrecargar servicios	- Interrupción de los servicios - Daño a la reputación
Adware	BAJO	Mostrar publicidad no deseada	- Afectar el rendimiento del sistema - Exposición a malware

Nota. Referencia (García y Apolinario, 2024).

2.2. Importancia de la guía en el contexto actual

La creciente adopción de dispositivos IoT en los hogares ha creado un panorama propenso a ciberataques. La guía propuesta permite identificar y mitigar vulnerabilidades específicas, proporcionando un enfoque adaptativo para proteger los hogares inteligentes.

2.3. Relación con estándares internacionales

La guía se basa en estándares internacionales como:

ISO/IEC 27001: Estándar para la gestión de la seguridad de la información.

NIST: Marco de trabajo para mejorar la ciberseguridad.

COBIT: Buenas prácticas en gobernanza de TI.

3. Descripción de la guía

3.1. Elementos de la guía

Los elementos clave de esta guía incluye:

Plataformas de nube: AWS IoT, Azure IoT y Google Cloud IoT para la recopilación de datos.

Herramientas de escaneo: Advanced IP Scanner, Kali Linux, Fing.

Estrategias de mitigación: Contraseñas seguras, actualización de software, desactivar funciones no utilizadas, segmentación de redes, y el uso de IDS.

3.2. Procedimiento

Es necesario:

- Recopilar información de dispositivos IoT mediante las plataformas de nube.
- Escanear la red local para detectar dispositivos conectados y vulnerabilidades.

La información obtenida con aprendizaje automático mediante las plataformas AWS IoT, Azure IoT y Google Cloud IoT nos sirve para ejecutar las siguientes estrategias:

- Utilizar contraseñas seguras: Se recomienda contraseñas de al menos 12 caracteres que combinen letras mayúsculas, minúsculas, números y signos especiales.
- Cambiar contraseñas predeterminadas: Las contraseñas que viene de fábrica son fáciles de ser descifradas por los ciberdelincuentes es muy importante cambiar las mismas.
- Segmentar la red: Muy importante separar las redes en segmentos para limitar el acceso de los dispositivos IoT a otras redes.
- Actualizar el software constantemente: Con las actualizaciones constantes en los dispositivos garantiza que tenga todas las mejoras a nivel de la seguridad y ayuda a proteger de vulnerabilidades.
- Desactivar funciones no utilizadas: Al desactivar lo innecesario en los dispositivos IoT, disminuye los ciberataques.
- Sistema de detección de intrusiones (IDS): Es una herramienta diseñada para buscar vulnerabilidades, monitorea el tráfico e informa los resultados.

3.3. Controles de seguridad y buenas prácticas

Algunas de las mejores prácticas incluyen:

- Contraseñas seguras y la modificación de contraseñas predeterminadas.
- Segmentación de redes para evitar accesos no autorizados.
- Uso de un sistema de detección de intrusiones (IDS).

3.4. Evaluación y validación de la guía

La guía debe ser evaluado mediante pruebas periódicas de penetración (pen-testing), monitoreo continuo del tráfico de red, y análisis de la efectividad de las estrategias implementadas.

4. Aplicaciones y Beneficios de la guía

4.1. Sectores o áreas en los que se puede aplicar

Este modelo es aplicable en cualquier hogar que utilice dispositivos IoT, empresas de desarrollo tecnológico, y proveedores de servicios de Internet.

4.2. Beneficios esperados

- Mejora de la seguridad en el hogar inteligente.
- Protección de datos personales de los usuarios.
- Prevención de ciberataques mediante un enfoque preventivo.

4.3. Posibles limitaciones y estrategias de mitigación

La guía proporciona una protección robusta, los ataques pueden evolucionar. La constante actualización de los dispositivos y la mejora continua de las estrategias son esenciales para mantener la seguridad.

5. Conclusiones y Recomendaciones

Conclusiones

- Es ineludible que se deben describir los fundamentos teóricos del Internet de las Cosas (IoT) y de dispositivos IoT, para de esta manera mitigar las vulnerabilidades de manera eficaz con ayuda de aprendizaje automático, estas estrategias de mitigación deben adaptarse a las características de los dispositivos IoT en el ambiente en el que se utilicen.
- Las vulnerabilidades existentes en los dispositivos IoT de tipo doméstico, pueden ser manipulados por los ciberdelincuentes para el robo de datos o posesión del control de los dispositivos, en pro de asegurar la seguridad en los dispositivos IoT deben aplicarse estrategias anticipadas que mitiguen las vulnerabilidades, es muy importante que los usuarios conozcan las amenazas que puede afectar en su hogar.
- Es muy importante diseñar una guía de estrategias de mitigación basadas en aprendizaje automático para que los usuarios hagan un buen uso de dispositivos IoT de tipo doméstico, estas estrategias garantizan la integridad y confiabilidad de los datos que transmitan los dispositivos IoT, adicional es de suma importancia estar actualizado con las nuevas tecnologías y seguridad que cuentan los dispositivos IoT.
- El criterio de los especialistas fue un factor decisivo importante para la realización de la propuesta, su experiencia permitió el identificar posibles riesgos en los dispositivos IoT de tipo hogar. Estas sugerencias incorporar en la guía garantiza las mejores prácticas de seguridad.

Recomendaciones

- Se recomienda la implementación de una guía para el uso de dispositivos IoT de tipo doméstico y estrategias de mitigación basadas en aprendizaje automático.
- Se sugiere técnicas avanzadas de aprendizaje automático para la recopilación de los datos de los dispositivos IoT y poder generar estrategias para mitigar el riesgo en los dispositivos IoT de tipo doméstico.
- Se recomienda para una siguiente etapa en la investigación, la guía se socialice de manera general hacia los sectores empresariales, educativos, industriales y financieros, campos donde están presentes los dispositivos IoT.
- Se recomienda crear una red exclusiva para la conexión de los dispositivos IoT de tipo hogar al internet todo esto avalado por especialistas en Seguridad Informática.

6. Glosario

IoT: Internet de las Cosas

Aprendizaje Automático: Técnica de IA que permite a los sistemas aprender de los datos para hacer predicciones.

Anomalía: Comportamiento inusual que puede indicar un ataque o fallo de seguridad.

7. Índice de tablas

8. Índice de figuras

9. Referencias Bibliográficas

Arar, M., Jung, C., Awad, Y., & Chohan, A. (5 de Noviembre de 2021). *designs*. Obtenido de Analysis of Smart Home Technology Acceptance and Preference for Elderly in Dubai, UAE: https://doi.org/10.3390/designs5040070

Arif, R. (19 de Diciembre de 2023). *Rise Up Labs*. Obtenido de Google Cloud IoT Solutions Guide: https://riseuplabs.com/google-cloud-iot-solutions-guide/

Cloud Ausum. (2025). *¿Qué es la plataforma AWS IoT Core?* Obtenido de ausum cloud: https://ausum.cloud/aws-iot-core/

Dsouza, R. (18 de Febrero de 2025). *Bacancy*. Obtenido de Azure IoT Hub: su puerta de entrada a soluciones de IoT más inteligentes: https://www.bacancytechnology.com/blog/what-is-azure-iot-hub

García, K., & Apolinario, O. (21 de Agosto de 2024). *Minerva Journal*. doi:https://doi.org/10.47460/minerva.v5i15.171