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:
Propuesta de un manual de políticas de seguridad para el proceso de comunicación entre los dispositivos IoT, mediante métodos de encriptación
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:
Atiaja Jiménez Diego Aníbal
Tutor/a:
Mg. Renato Mauricio Toasa Guachi PhD. Maryory Urdaneta Herrera

Quito – Ecuador

2024

APROBACIÓN DEL TUTOR

Yo, **Renato Mauricio Toasa Guachi** con C.I: **1804724167** en mi calidad de Tutor del proyecto de investigación titulado: **Propuesta de un manual de políticas de seguridad para el proceso de comunicación entre los dispositivos IoT, mediante métodos de encriptación**.

Elaborado por: **Diego Aníbal Atiaja Jiménez**, de C.I: **1719153106**, estudiante de la Maestría: en 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 2024

Firmado electrónicamente por:
RENATO MAURICIO
TOASA GUACHI

_____

Mg. Toasa Guachi Renato Mauricio

ORCID: 0000-0002-2138-300X

APROBACIÓN DEL TUTOR

Yo, **Maryory Urdaneta Herrera** con C.I: **1759316126** en mi calidad de Tutor del proyecto de investigación titulado: **Propuesta de un manual de políticas de seguridad para el proceso de comunicación entre los dispositivos IoT, mediante métodos de encriptación.**

Elaborado por: **Diego Aníbal Atiaja Jiménez**, de C.I: **1719153106**, estudiante de la Maestría: en 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 2024

Firmado electrónicamente por:
MARYORY URDANETA HERRERA

_____

PhD. Urdaneta Herrera Marjory

ORCID: 0000-0001-8773-5349

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Universidad Israel

Yo, Diego Aníbal Atiaja Jiménez con C.I: 1719153106, autor del proyecto de titulación denominado: Propuesta de un manual de políticas de seguridad para el proceso de comunicación entre los dispositivos IoT, mediante métodos de encriptación. Previo a la obtención del título de Magister en 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 2024

Firma

Tabla de contenido

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

A continuación, una breve descripción del trabajo realizado.

Contextualización del tema

Con el progreso vertiginoso del internet de las cosas (IoT) las tareas cotidianas se han transformado, acoplando dispositivos desde los más básicos como electrodomésticos hasta sistemas complejos de seguridad vinculándose a la red, esta modernización también ha permitido divisar vulnerabilidades que los ciberdelincuentes aprovechan para causar estragos. (Ríos, 2023)

IoT desarrolla un ámbito inteligente vinculando dispositivos físicos al internet y dotando con la cualidad de recopilar y canjear datos en tiempo real (Rivadeneira, 2020).

La transformación de la tecnología y el perfeccionamiento del internet ha permitido que dispositivos comunes del hogar como es electrodomésticos, lunarias, televisores etc., se puedan conectar a la red y permiten ser programados que realicen sus tareas a determinada hora, o controlar por el usuario por medio de aplicaciones móviles o páginas web en tiempo real, facilitando las tareas cotidianas y optimizando el tiempo de los usuarios.

Al existir una gran cantidad de dispositivos conectados a la red, existe una sustancial cuantía de información en línea, ocasionando que subsistan vulnerabilidades entorno a la seguridad e intimidad (Kaspersky, 2024).

La tecnología IoT ayuda a hospitales, hogares, oficinas industrias y automóviles a obtener mayor productividad y eficiencia, estos equipos poseen riesgos propios de seguridad. Estas vulnerabilidades de seguridad dejan a los usuarios accesibles a diferentes tipos de ataques (Amos, 2023).

Los dispositivos inteligentes indefensos extienden las redes a los ataques y pueden disminuir la seguridad normal de Internet (ITSitio, 2020).

La tecnología IOT al convertirse en una extensión de red realiza principalmente la recopilación de información, transmisión y procesamiento de objetos a través de varias transmisiones existentes entre personas y cosas, la vulnerabilidad de datos maliciosos incrustados en una red, puede afectar traer muchos inconvenientes al usuario.(Patiño & Sánchez, 2021)

Los beneficios de los dispositivos IoT son diversos, pero con ello también se presentan en forma proporcional las vulnerabilidades para posibles ataques de delincuentes cibernéticos, siendo imperioso diseñar soluciones para la comunicación de los dispositivos IoT de manera encriptada, que permitirá disminuir vulnerabilidades y avalar la seguridad de la información de los usuarios.

La Unidad Educativa Particular PCEI "LÍDERES" es un referente en el servicio de educación virtual y autónoma en los subniveles de Educación Básica Superior y Bachillerato General Unificado en Ciencias, constituyéndose como una institución de carácter inclusivo e intercultural, con el fin de mejorar la calidad de vida de los estudiantes, para el desarrollo de nuestro país.(PCEI LÍDERES, 2024)

La institución LÍDERES al trabajar con entorno virtual y en su oficina contar con dispositivos IoT conectados a red, que le otorga beneficios en sus tareas cotidianas, estos equipos también presentan vulnerabilidades que deben ser mitigadas.

Problema de investigación

Los objetos IoT recogen datos automáticamente y los envían a otros objetos. Cada año, empresas, programadores y estudiosos crean y ejecutan nuevos usos y conexiones entre objetos hasta ahora inimaginables (González et al., 2020).

Debido a la gran cantidad de dispositivos IoT actualmente están en uso y a los usuarios conectados, es que empieza a tomar mucha relevancia la seguridad, debido que gran cantidad dispositivos carecen de protecciones integradas, con puntos de entrada para los ciberataques, comprometiendo los datos confidenciales y amenazando la seguridad del usuario, poniendo en peligro la intimidad y la seguridad de las personas.

Los usuarios por desconocimiento o economía, a menudo suelen utilizar dispositivos de la IoT que son fácilmente comprometidos en su seguridad, que forman redes de dispositivos conectados a Internet, dichos dispositivos se tornan vulnerables a que se infecten con software malicioso y sean utilizados con fines delictivos, por parte de los ciberdelincuentes.(Bermúdez, 2022)

La Institución Educativa Particular PCEI “Líderes”, se encuentra en desarrollo por lo que aún no tiene definido su departamento de Tics, sus activos informáticos son manejados por personal externos, adicional no poseen un manual de políticas de seguridad para los dispositivos IoT instalados en sus oficinas.

Objetivo general

Elaborar un manual de políticas para la seguridad de los dispositivos IoT, usando procesos de encriptación para la comunicación entre los medios, para reducir las vulnerabilidades ante posibles ciberataques.

Objetivos específicos

1. Contextualizar los fundamentos teóricos sobre políticas de seguridad y vulnerabilidades sobre los dispositivos IoT.
2. Diagnosticar el estado actual de la seguridad en dispositivos IOT referente a vulnerabilidades
3. Diseñar el manual de políticas de seguridad de los dispositivos IoT con base en criptografía para proteger la comunicación entre dispositivos.
4. Validar el manual propuesto mediante criterio de expertos.

Vinculación con la sociedad y beneficiarios directos:

Los beneficiarios directos de este proyecto de titulación será la comunidad educativa conformada por profesores, administrativos y estudiantes pertenecientes a La Unidad Educativa Particular PCEI “LÍDERES”, debido que al elaborar este documento se proporciona de un manual con una serie de políticas que facilitaran el manejo de la seguridad de los dispositivos IoT.

Adicionalmente, contribuirá a alcanzar el objetivo de desarrollo sostenible 4, de acuerdo con ONU Ecuador, (2024), es imperativo proporcionar una educación integral, igualitaria y de alta calidad, al tiempo que se promueven las posibilidades de aprendizaje permanente para todos.

Al presentar un manual de normativas de seguridad para los dispositivos IoT en la Unidad Educativa se garantiza una educación de calidad ya que la red estará protegida de ataques cibernéticos.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

En este capítulo se procura presentar al lector información relevante referente a los dispositivos IoT que encontramos a diario en los hogares ecuatorianos, políticas de seguridad existentes y sus vulnerabilidades.

1.1. Contextualización general del estado del arte

Ahora con la facilidad que los dispositivos cotidianos se puedan conectar al internet, facilita muchas tareas habituales, que pueden ser programadas con anterioridad o de forma remota, pero esto también implica que presentan vulnerabilidades, esos dispositivos se vuelven blancos de ataques para los delincuentes informáticos.

De acuerdo con (Villacis Miguel, 2023) en el estudio realizado investigación bibliográfica y descriptiva determina que, se puede concluir que la tendencia de universalidad y transformación digital de las cosas aporta numerosos y novedosos tipos de ataque y vulnerabilidad; Aun así, Se cree que también se están desarrollando métodos de mitigación para ellos.

Según Bermúdez (2022), en Costa rica se realizó un estudio por medio de varias encuestas referentes al conocimiento de los usuarios sobre dispositivos IoT, implementación y percepción de seguridades que debe tener el usuario en los hogares, determinando la necesidad de la elaboración de la Guía de Mejores Prácticas: Uno de los resultados de este esfuerzo es la seguridad en los servicios de Internet de las Cosas (IoT) en el hogar.

De acuerdo con Cuji y Araujo (2024), al realizar pruebas de penetración utilizando el método STRIDE, sobre dispositivos IoT comunes de hogares inteligentes. detectó varias amenazas latentes, este estudio determinó que, implementando medidas de seguridad dentro de la red, y utilización de herramientas de monitorización de tráfico de datos de la red, se muestra una mitigación de vulnerabilidades de un 64.052% en el sistema IoT, garantizando un entorno más seguro para los dispositivos IoT.

Para un adecuado manejo y protección de posibles ataques de delincuentes informáticos es necesario basarse en documentos o guías que tengan políticas o normativas que permitan el correcto manejo de la seguridad de los dispositivos IoT.

La importancia de la gestión de riesgos en la Internet de los objetos (IoT), dado su creciente impacto tanto en las empresas como en la vida cotidiana. Debido a la continua expansión de la Internet de los objetos, las empresas deben considerar formas de aminorar los posibles efectos que podrían

poner en peligro la privacidad y la ciberseguridad de los usuarios y comprometer la continuidad de la actividad. (Molina, 2019)

Las principales técnicas de criptografía que se pueden aplicar a la seguridad de los datos de los dispositivos IoT, debido a esta clase de componentes tienen pocos recursos, el cifrado de curva elíptica se considera el más calificado, se debe utilizar AES para priorizar la seguridad, estándar avalado por su eficacia en la seguridad de datos en IoT (Olivarez et al., 2023).

Para evitar ataques a nuestra red por medio de los dispositivos IoT, es necesario proteger de manera eficiente nuestra infraestructura IoT, la mejor arma es el conocimiento.

1.2. Proceso investigativo metodológico

Por medio de esta sección se procura mencionar el curso que se ha seguido para poder proponer el diseño del manual de políticas criptográficas para proteger la comunicación de los dispositivos IoT.

1.3. Investigación Bibliográfica o Documental

Para el presente trabajo se ha creado una lista de citas de varios documentos, entre ellos artículos, papers, blocks, páginas oficiales de universidades y empresas de tecnología, que facilitan la información necesaria para poder proyectar lo que se investiga en este trabajo.

De acuerdo con Universidad Veracruzana (2024) , este tipo de estudio se realiza con la ayuda de fuentes escritas, audiovisuales, sonoras, esto es en todo tipo de documentos libros artículos, revistas, periódicos, ensayos, monografías, etc., con respecto al tema estudiado.

El presente trabajo empleará la investigación explicativa, que permitirá ahondar en los conocimientos de las vulnerabilidades que pueden presentan los dispositivos IoT

La investigación explicativa tiene como objetivo profundizar el conocimiento ya existente sobre algo de lo que comprendemos poco, o nada. De esta manera, se enfoca en los detalles, permitiendo conocer más a fondo (López, 2020).

Adicionalmente se utilizará la investigación cuantitativa, que facilitará el proceso de análisis de datos retomados dentro de la elaboración del proyecto, mediante la utilización de la herramienta de encuesta.

Mediante la aplicación de técnicas de análisis estadístico y matemático, la investigación cuantitativa utiliza datos numéricos para describir, explicar y prever acontecimientos.

Un método de recopilación de datos son las encuestas, a menudo tienen como objetivo generalizar los resultados a una parte más amplia de la población. (Qualtrics, 2024)

1.4. Análisis de resultados

A continuación, se describen los resultados de la aplicación de la encuesta, por medio de análisis gráfico de las respuestas otorgadas.

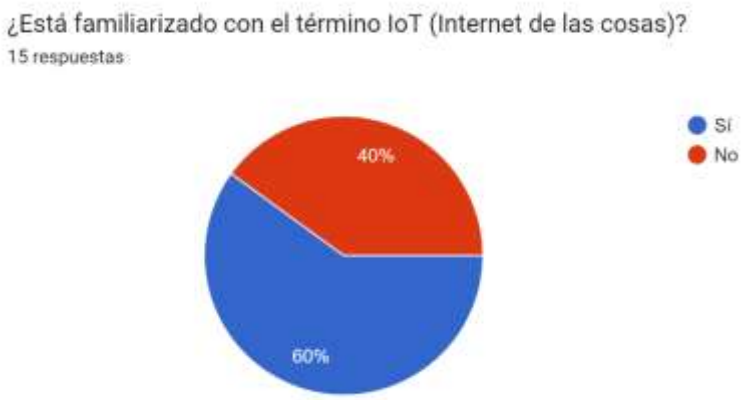
La encuesta está conformada por tres secciones fundamentales para recabar información relevante del presente trabajo.

Se realizará el análisis sobre las preguntas primordiales de para la investigación y de acuerdo a la sección.

Primera sección: Conocimiento General sobre dispositivos IoT

Figura 1

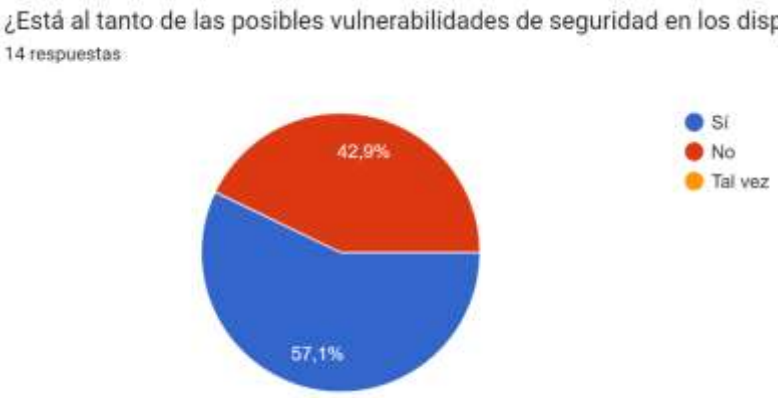
Conocimiento General sobre dispositivos IoT pregunta 1



En referencia a la respuesta a las preguntas de Figura 1, se puede determinar que el 60% de los encuestados han oído hablar del término Internet de las cosas, mientras que la proporción restante desconoce.

Figura 2

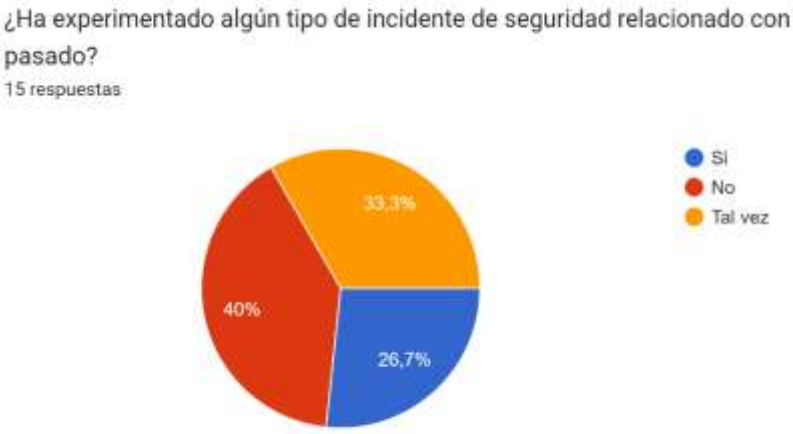
Conocimiento General sobre dispositivos IoT pregunta 2



Según la Figura 2 más del 50% de los encuestados conocen sobre posibles vulnerabilidades que pueden tener los dispositivos IoT

Figura 3

Conocimiento General sobre dispositivos IoT pregunta 3

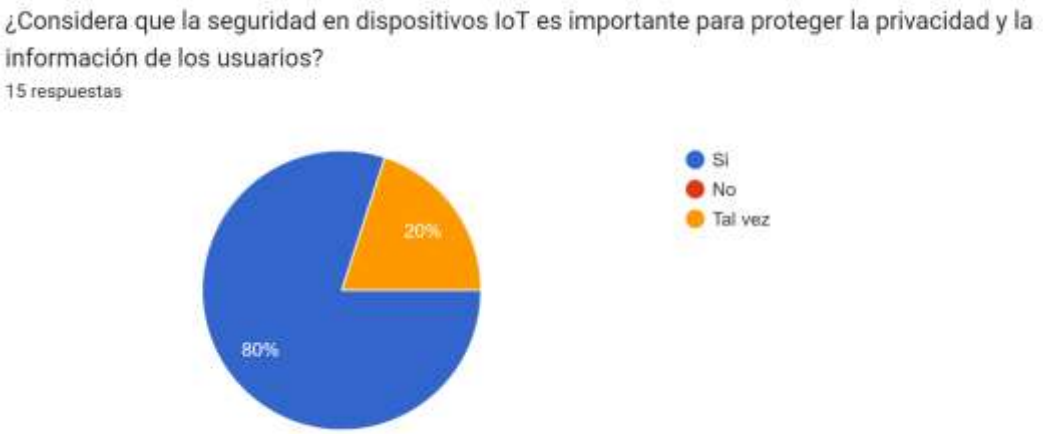


Se puede observar dentro de las respuestas en la Figura 3, que el 40 % de los encuestados afirman no haber experimentado algún tipo de incidente de seguridad relacionado con los dispositivos IoT, el 33.3% desconoce si experimento y el 26.7% confirma haber experimentado algún incidente de seguridad.

Segunda Sección: Importancia de la seguridad en los dispositivos IoT

Figura 4

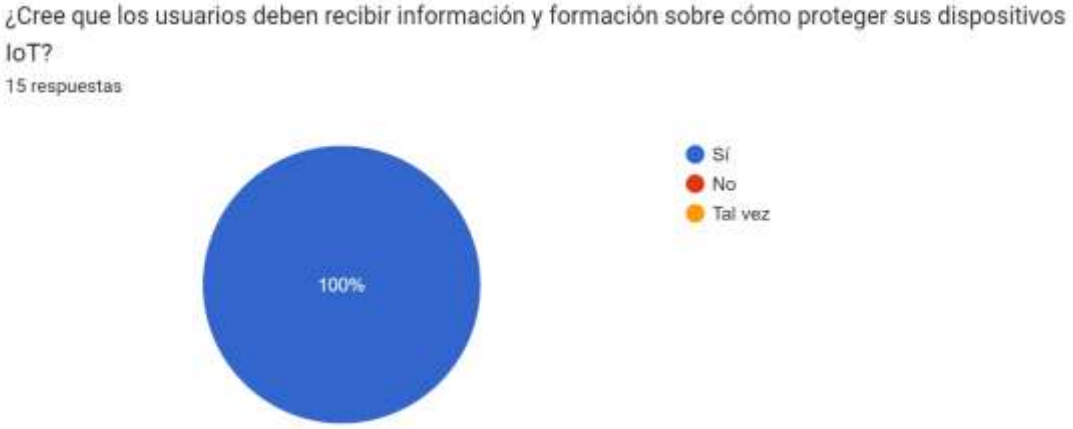
Importancia de la seguridad en los dispositivos IoT pregunta 1



El 80% de la población encuestada está de acuerdo en que la seguridad en los dispositivos IoT es importante para proteger los datos personales, mientras que el 20% divaga en referencia al tema.

Figura 5

Importancia de la seguridad en los dispositivos IoT pregunta 2

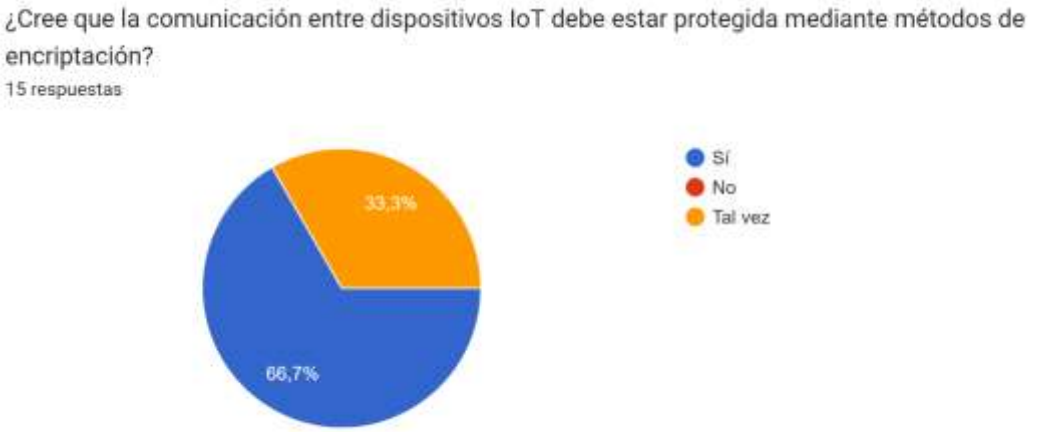


De acuerdo con el 100% de los encuestados se encuentra de acuerdo en que los usuarios deben recibir información y formación sobre cómo proteger sus dispositivos IoT.

Tercera Sección: Mejoras para seguridad de dispositivos IoT

Figura 6

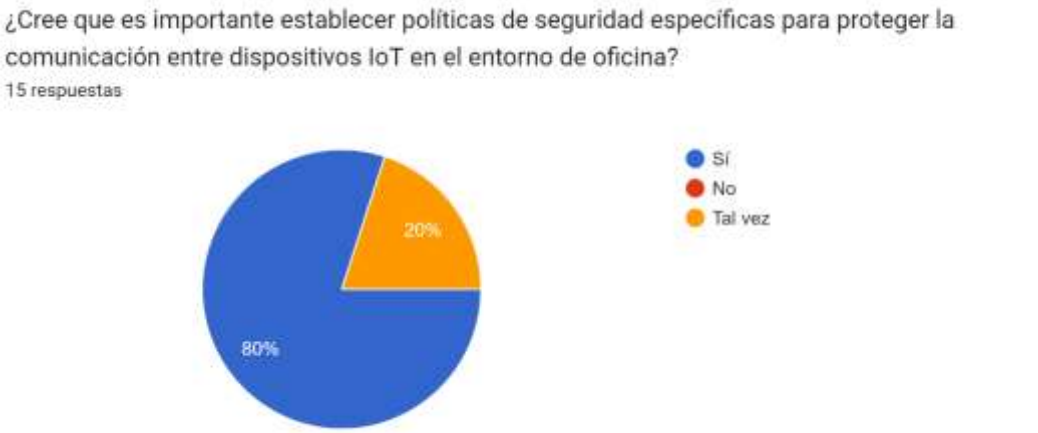
Mejoras para seguridad de dispositivos IoT pregunto 1



Según el 66.7% de la población encuestada está de acuerdo que la comunicación entre dispositivos IoT debe estar protegida por métodos de encriptación, el porcentaje restante piensa que tal vez debería estarlo.

Figura 7

Mejoras para seguridad de dispositivos IoT pregunto 2



De acuerdo con el análisis el 80% considera que es importante establecer políticas de seguridad para proteger la comunicación entre los dispositivos IoT, el porcentaje restante piensa que tal vez debería implementarse.

Figura 8

Mejoras para seguridad de dispositivos IoT pregunto 2

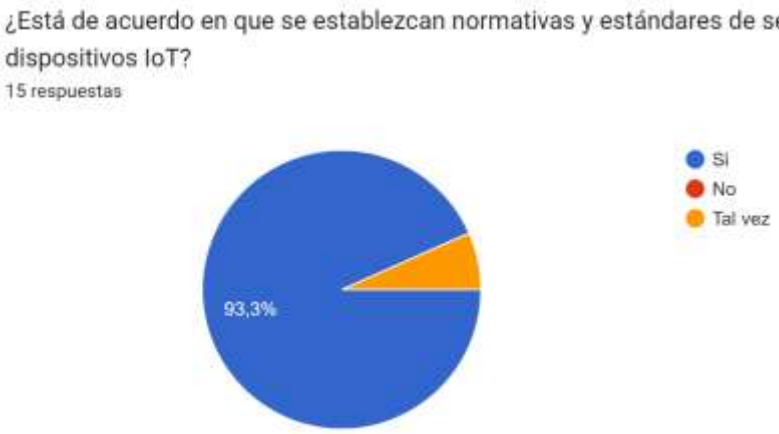


Figura 9

Mejoras para seguridad de dispositivos IoT pregunto 3

El 53.3% considera que la medida de encriptación de datos, es importante para la seguridad de los dispositivos IoT, el 46.7% indica que la medida de seguridad más importante seria la autenticación de los usuarios.

Figura 10

Mejoras para seguridad de dispositivos IoT pregunto 4

Dentro del análisis de la siguiente pregunta existe un empate del 40% como propuesta para Implementar normativas y estándares de seguridad obligatorios, y Establecer colaboración entre fabricantes, usuarios y autoridades, mientras que el 20% restante considera, mejorar la formación sobre seguridad en dispositivos IoT.

De las conclusiones podemos deducir que:

Más del 50% de la muestra tiene conocimientos generales en relación a la tecnología IoT.

Los resultados indican que la seguridad desempeña un papel fundamental a la hora de salvaguardar la información personal de los usuarios.

Los resultados de la encuesta determinan que es importante, la elaboración mediada de seguridad como estándares generales, políticas de encriptación para la comunicación entre dispositivos IoT, para proteger la exactitud de los datos de los usuarios.

CAPÍTULO II: PROPUESTA

En el presente capítulo se especificará la información teórica fundamental para la elaboración de la propuesta.

2.1. Fundamentos teóricos aplicados

En la siguiente sección se incluyen extractos de las definiciones de los términos a los que se refiere esta propuesta.

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

Según Fernández, (2024) el Internet de las cosas (IoT) es una idea innovadora que está transformando la forma en que interactúan los mundos físico y digital. En el corazón de IoT está conectar objetos y dispositivos cotidianos para que puedan comunicarse, recopilar datos y realizar acciones de manera inteligente. Esta conectividad está habilitada por sensores, software y tecnologías de conectividad que permiten que estos objetos se conviertan en componentes activos de una red global. Lo más importante es que no requieren interacción humana directa una vez que estén operativos.

La tecnología IoT entrega grandes ventajas en el proceso de automatización en las diferentes áreas donde se utilizan estos dispositivos, en este caso nos centraremos en el ámbito doméstico.

2.1.2. Arquitectura IoT

Existen varios tipos de arquitecturas de acuerdo al número de capas de tres, cuatro, cinco, seis etc. capas de acuerdo al enfoque que se le esté tomando, para el presente documento nos guiaremos en la arquitectura más común que es la de cuatro capas que son: Capturar los datos, Conectividad, Procesamiento de datos, Actuar a partir de los datos.

De acuerdo con Pérez (2020) se consideran las siguientes capas:

Tabla 1

Arquitectura de 4 capas

Capas	Descripción
Capturar los datos	Es la capa donde se encuentran los sensores son los que dan la capacidad de conectar el mundo real y el virtual, a por medio de la recopilación y procesamiento de información en tiempo real. De acuerdo al propósito de los sensores existen diferentes tipos como pueden ser para medir temperatura, calidad de aire, velocidad, humedad, presión, entre otros.
Conectividad o red	Esta capa es el vehículo de transporte para transmitir los datos generados por los sensores. Esto se puede hacer de manera confiable a través de una infraestructura cableada o inalámbrica. A diferencia de otras redes, IoT requiere el uso de sistemas que permitan que diferentes tecnologías y protocolos funcionen juntos debido a la mayor demanda de servicios de baja latencia, alta velocidad y ancho de banda.
Procesamiento de datos	Dentro de esta capa reside la gestión responsable de acceder, integrar y controlar la información para que la capa superior (capa de aplicación) pueda evitar procesar datos innecesarios. Se utilizan técnicas de filtrado como la anonimización, la consolidación y la sincronización para proporcionar sólo la información importante que las aplicaciones interoperables necesitan procesar.
Actuar a partir de los datos (aplicación)	Esta capa incluye los entornos en los que se aplica IoT, pasando de contextos "básicos" a contextos "inteligentes", como hogares, edificios, transporte, salud y energía. En esta capa puede o no ser necesaria la interacción de los usuarios dependiendo de la funcionalidad.

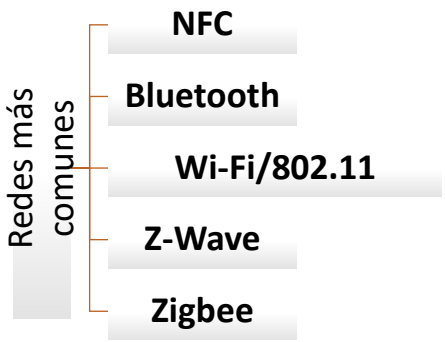
Nota: Información tomada de (Pérez, 2020)

2.1.3. Redes de corto alcance y bajo consumo

Las redes de baja potencia y corto alcance son apropiadas para hogares, oficinas y otros entornos de tamaño reducido. Comúnmente, requieren baterías pequeñas y su uso suele resultar económico(Azure, 2024).

Figura 11

Redes más comunes de corto alcance



Nota: referencia (Azure, 2024)

2.1.4. Vulnerabilidades IoT

Es la capacidad de recibir o asimilar negativamente acontecimientos externos, que tiene el potencial de convertirse en un ataque.

Hoy en día la creciente demanda ha aumentado la cantidad de aparatos conectados a Internet, la mayoría de las personas tienen un teléfono inteligente y otros dispositivos en casa o en el trabajo, esto ha alterado el modo de vida de las personas, facilitando la comunicación, logrando conectar a personas en diferentes partes del mundo. Además de optimizar procesos en las fábricas, cumpliendo con las tareas de todos cada vez es más complejo, pero a diferencia de una computadora, los dispositivos IoT no tienen antivirus, también tienen sensores incorporados, micrófonos, cámaras: todos ellos son capaces de monitorear nuestra vida diaria, recopilar datos y enviarlos a través de Internet.(Casarrubias et al., 2022)

De acuerdo con ITSitio (2020), los dispositivos IoT carecen de seguridad inherente para defenderse de los ataques, que es la razón fundamental por la que son vulnerables Además de los aspectos tecnológicos, el usuario aumenta la susceptibilidad del dispositivo a las amenazas.

Algunas de las razones por las que los aparatos inteligentes siguen siendo vulnerables son las siguientes:

Tabla 2

Vulnerabilidades dispositivos IoT

Vulnerabilidad	Descripción
Limitaciones de potencia informática y hardware	Ciertas características de estos dispositivos garantizan una capacidad de procesamiento restringida y ofrecen un espacio mínimo para medidas de seguridad y protección de datos.
Tecnologías de transmisión heterogéneas	Los dispositivos utilizan con frecuencia diferentes tecnologías de transmisión. Por ello, puede resultar difícil establecer procedimientos y protocolos de protección uniformes.
Componentes de los dispositivos son vulnerables	Millones de aparatos inteligentes desplegados se ven afectados por componentes fundamentales comprometidos.
Usuarios tienen poca conciencia de seguridad	Los usuarios que no son conscientes de la seguridad pueden dejar los dispositivos inteligentes expuestos a amenazas y vulnerabilidades.

Nota: Información tomada de (ITSitio, 2020).

2.1.5. Criptografía

El cifrado garantiza la integridad y el secreto de la información, de tal modo que, en el entorno local mediante el llamado cifrado tradicional, como en las comunicaciones constantes a través de Internet.

Criptografía ligera

En algunos entornos móviles y aquellos asociados al modelo de Internet de las cosas (IoT), no es posible utilizar los algoritmos de cifrado utilizados actualmente, como el RSA de 2048 bits, porque consumen demasiados recursos. La criptografía ligera se basa en el estudio de algoritmos específicos de estos entornos y, por supuesto, ofrece un compromiso entre seguridad, rendimiento y coste, sin aumentar la vulnerabilidad de los algoritmos actuales a ciertos ataques de fuerza bruta. (Navas, 2023)

2.2. Descripción de la propuesta

Se inicia con la recopilación de información referente a la posición actual de La Unidad Educativa Particular PECI "LÍDERES", en relación a políticas de seguridad para el manejo de dispositivos IoT, a continuación, se analiza la estructura de red donde se encuentran vinculados los dispositivos inteligentes. A la postre se utilizan herramientas de escaneo de la red que permiten el análisis de posibles vulnerabilidades como son Nmap, Nessus versión trial, Fing App.

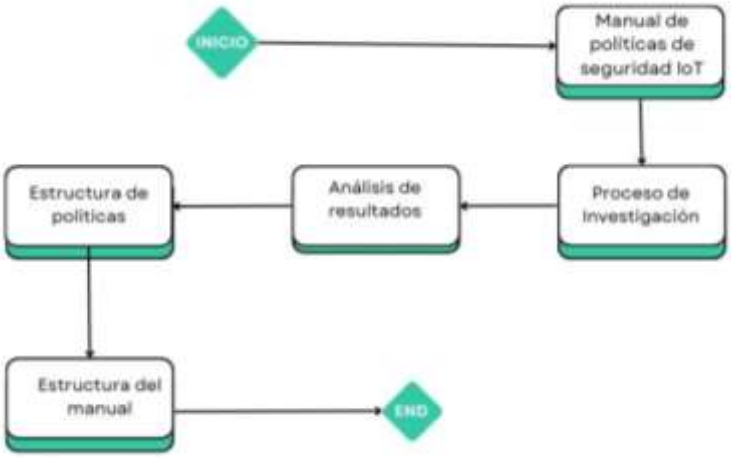
Con los frutos del análisis previo, se obtienen los parámetros fundamentales que serán partícipes para poder elaborar el análisis de políticas que se requieren para el proyecto. Se concreta el estudio de vulnerabilidades a los que se exponen teniendo dispositivos IoT home vinculados a la red de la institución.

a. Estructura general

En la Figura 12 se muestra el esquema general del manual de políticas de seguridad sugerido para el proceso de comunicación de dispositivos IoT.

Figura 12

Secuencia proyecto general



EL gráfico representado en la figura 13 muestra la estructura como se encuentra constituido el compendio de políticas de seguridad para el proceso de comunicación entre los dispositivos IoT, mediante métodos de encriptación

Figura 13

Proceso manual de políticas se seguridad dispositivos IoT

b. Explicación del aporte

Para la elaboración de la propuesta se ejecutaron diversos procesos, entre ellos la investigación bibliográfica, que establecieron los fundamentos teóricos del proyecto.

El siguiente proceso se basa en el escaneo de la red, que nos permitirá determinar las vulnerabilidades que se encuentran presentes y son fundamentales para estructuración de las políticas necesarias para el desarrollo de manual de políticas de seguridad de comunicación entre los dispositivos IoT.

c. Estrategias y/o técnicas

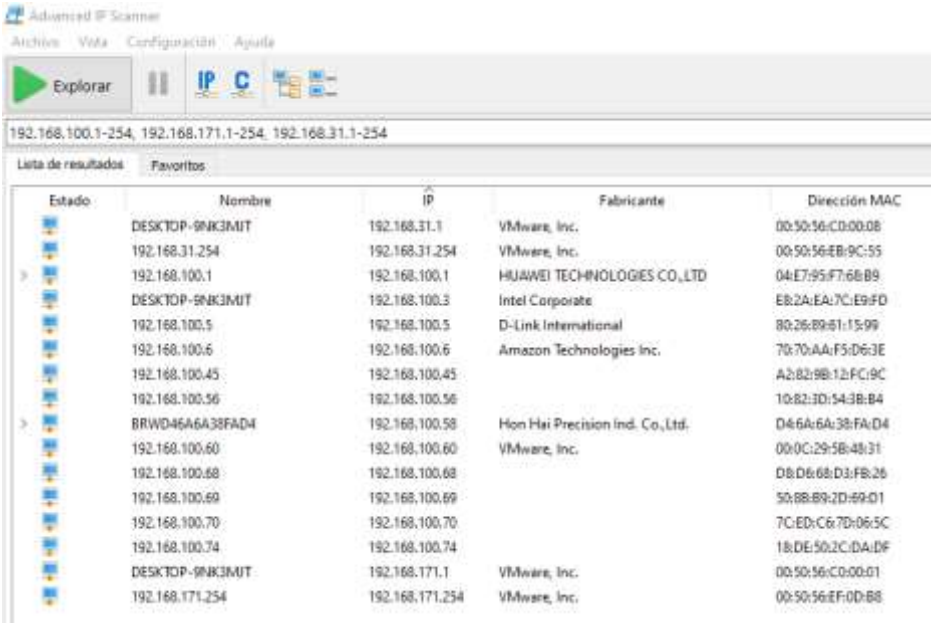
Utilizando diversas herramientas de escaneo como son de código abierto, Apps y trials.

Escaneo de la red y vulnerabilidades

Con la ayuda de herramientas de escaneo IP Scanner se pudo determinar la suma de dispositivos vinculados a la red de la oficina de la institución Líderes.

Figura 14

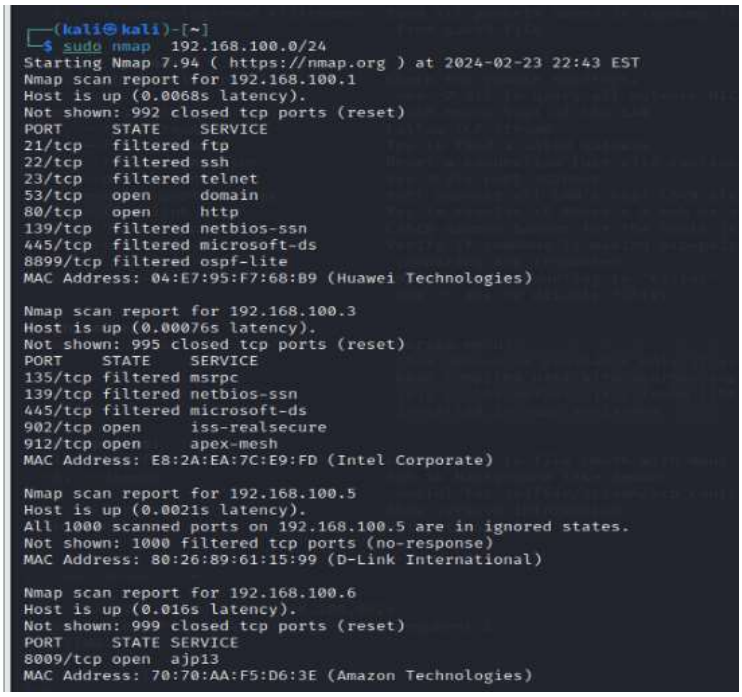
Red escaneado utilizando herramienta IP Scanner



Se escanea la red de manera individual para determinar los diferentes puertos que se encuentran abiertos utilizando la herramienta Nmap.

Figura 15

Escaneo punto por punto con herramienta Nmap



Detección de vulnerabilidades utilizando herramienta Nessus versión Trial

Figura 16

Escaneos red Líderes con herramienta Nessus

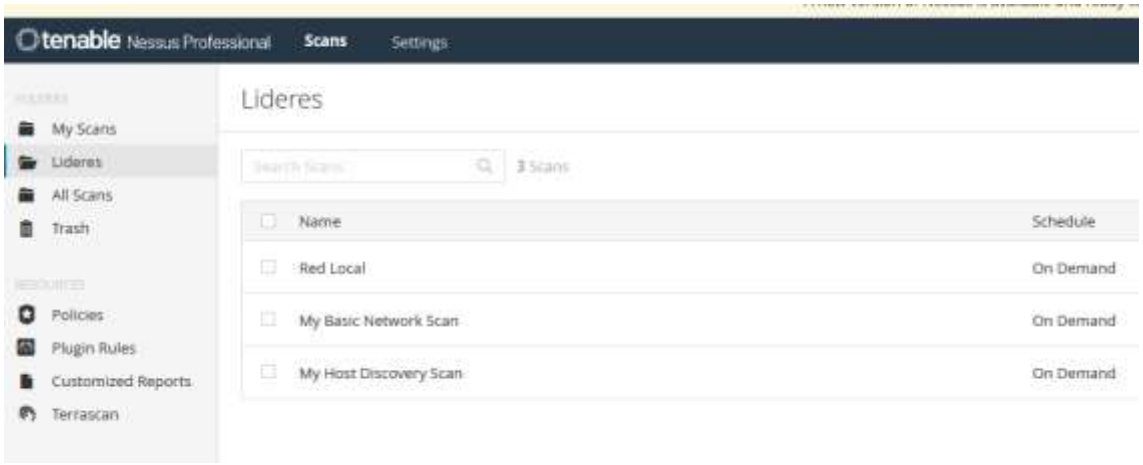


Figura 17

Dispositivos escaneados red Líderes

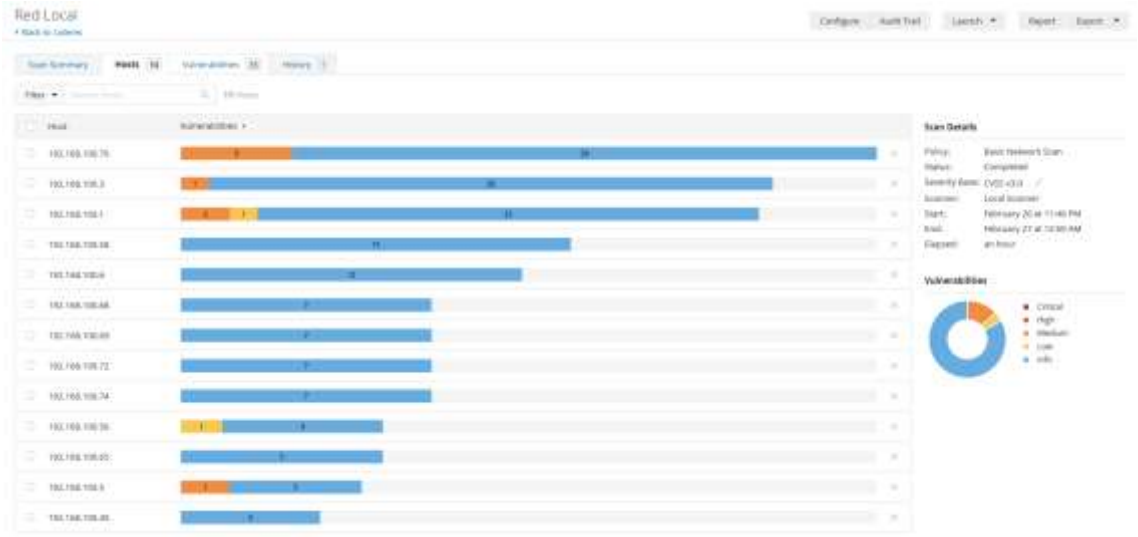
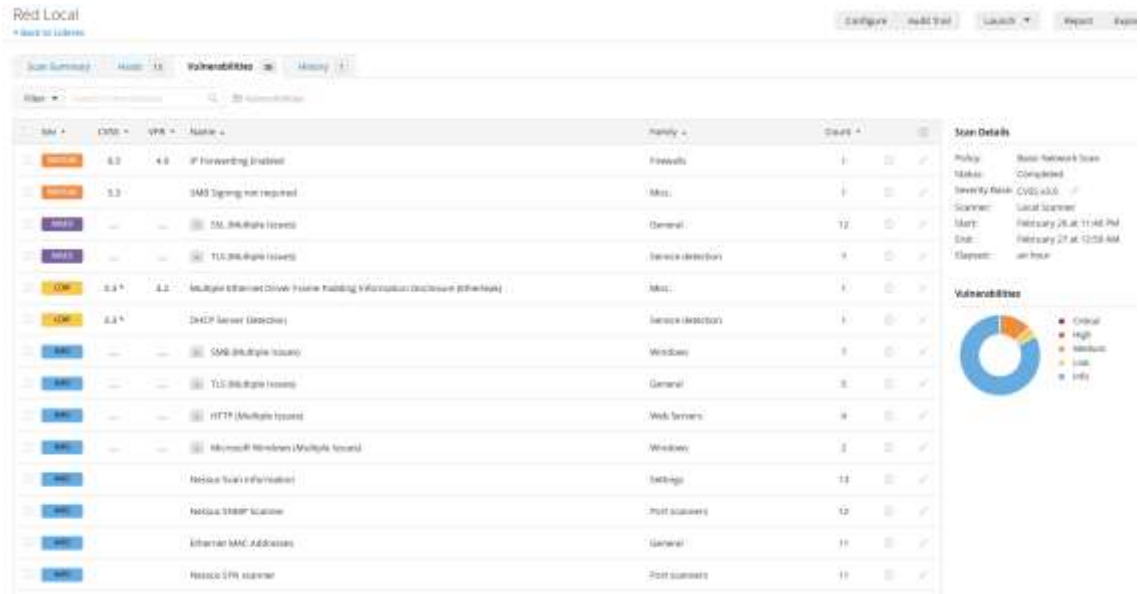


Figura 18

Vulnerabilidades encontradas en red Líderes



La herramienta Nessus muestra por dispositivo la cantidad y la criticidad de vulnerabilidades que se encontraron en el escaneo.

Escaner App Fing

Este escaneo nos permite visualizar la dirección ip, tipo de dispositivo, dirección mac y fabricante, por medio de un dispositivo Smart que se conecte a la red de la institución .

Figura 19

Escaneo herramienta App Fing

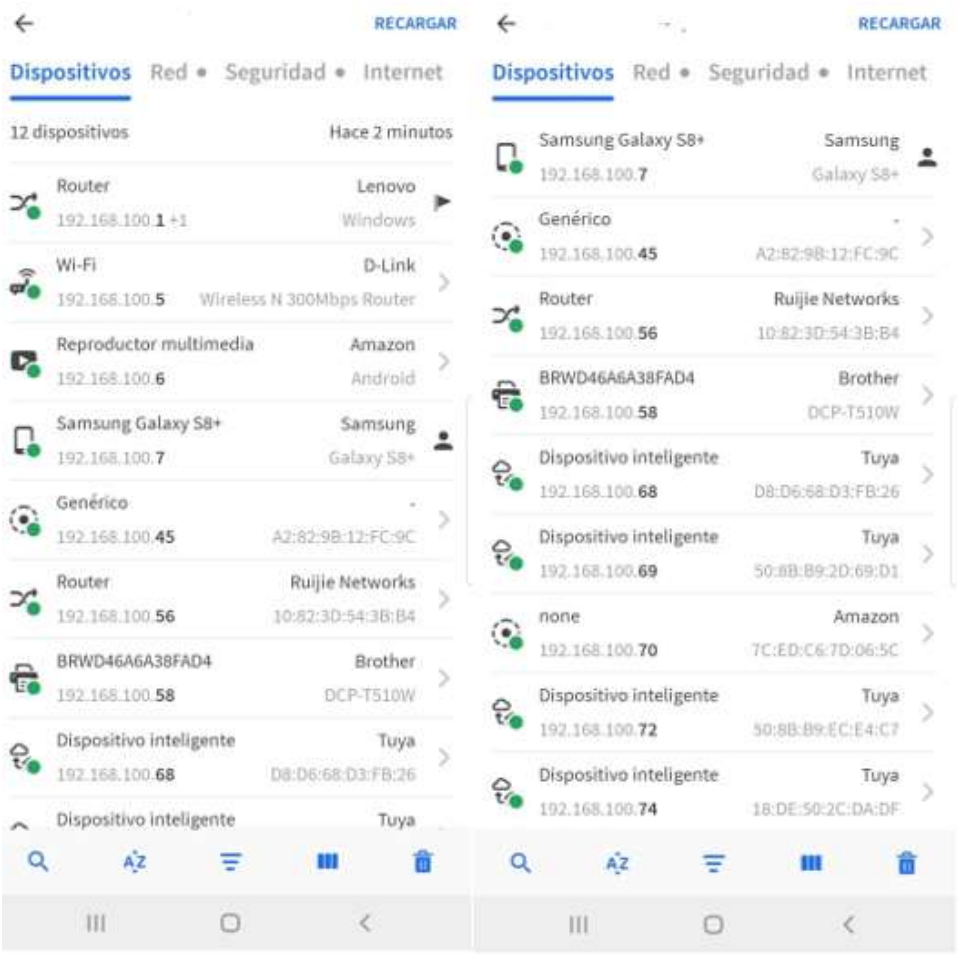


Figura 20

App Fing muestra fabricante del dispositivo

La aplicación Fing permite obtener datos de los fabricantes de dispositivos IoT que han sido escaneados.

Análisis de resultados

A partir del estudio realizado con las distintas herramientas de detección de vulnerabilidades, se pudo determinar que existen múltiples puertos filtrados y abiertos, y que cada puerto abierto conlleva un riesgo latente. Dado que los puertos abiertos constituyen una puerta de entrada para posibles ataques de ciberdelincuentes.

2.3. Validación de la propuesta

Especialistas con la experiencia y los conocimientos necesarios validará el plan, ofreciendo este estudio una aportación inestimable para la propuesta del manual de políticas de seguridad para el proceso de comunicación entre los dispositivos IoT, mediante métodos de encriptación.

Las respectivas validaciones de los directivos de la institución Educativa Líderes y de un experto externo se encuentran dentro del Anexo 7.

2.4. Matriz de articulación de la propuesta

La matriz que sigue ofrece una visión general de cómo se articula el manual de procedimientos sugerido, junto con los fundamentos teóricos y los enfoques metodológicos, tecnológicos y estratégicos empleados:

Tabla 3

Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Internet de las cosas IoT	Descripción de Internet de las cosas IoT (Internet of Things) (Fernández, 2024).	Gracias a los métodos de investigación bibliográfica, se pudo obtener las nociones intrincadas (Universidad Veracruzana, 2024).	Fuente bibliográfica	Respalda la información de fondo necesaria para comprender la idea.	Fuente bibliográfica
Vulnerabilidades	Teoría de las vulnerabilidades más comunes que enfrenta los dispositivos IoT	Gracias a los métodos de investigación bibliográfica, se pudo obtener las nociones intrincadas	Fuente bibliográfica	Respalda la información de fondo necesaria para comprender la idea.	Fuente bibliográfica

	(Casarrubias et al., 2022)	(Universidad Veracruzana, 2024).			
Criptografía	Definición de criptografía, criptografía ligera (Navas Damas, 2023)	Gracias a los métodos de investigación bibliográfica, se pudo obtener las nociones intrincadas (Universidad Veracruzana, 2024).	Fuente bibliográfica	Respalda la información de fondo necesaria para comprender la idea.	Fuente bibliográfica
Diseño y elaboración de manual de políticas	Definiciones relevantes consideradas en la estructura del manual propuesto (Bermúdez, 2022).	Enfoque cualitativo y cuantitativo. Alcance descriptivo y explicativo de los procedimientos. Tipo analítico y documental (Qualtrics, 2024).	Revisión de actuales políticas de seguridad para IoT, Elaboración de flujogramas de los procesos.	Elaboración de políticas de seguridad para el proceso de comunicación entre los dispositivos IoT, mediante métodos de encriptación, para la institución	Fuente bibliográfica, encuestas al personal, Herramientas de escaneo de vulnerabilidades.

Fuente: Elaboración propia

2.5. Análisis de resultados presentación y difusión

UNIDAD EDUCATIVA PARTICULAR PCEI
DISTANCIA -VIRTUAL
"LIDERES"
Resolución Nro. MINEDUC-SEDMQ-2023-00015-R
Correo iepceilideres@gmail.com

Manual de políticas de seguridad para el proceso de comunicación entre los dispositivos IoT, mediante métodos de encriptación

Unidad Educativa Particular PECI LÍDERES

2024

Tabla de contenido

Introducción

El Internet de las cosas (IoT) ha revolucionado la forma en que interactuamos con nuestros dispositivos y nuestro entorno. Los dispositivos IoT en el hogar, como termostatos inteligentes, cámaras de seguridad y cerraduras inteligentes, nos brindan comodidad y seguridad, pero también plantean riesgos de seguridad. Por lo tanto, para salvaguardar la comunicación entre los dispositivos IoT domésticos, deben establecerse fuertes medidas de seguridad.

En este manual, se proporcionarán pautas sobre cómo garantizar la seguridad en el proceso de comunicación entre electrodomésticos con Internet de las Cosas, mediante el uso de métodos de encriptación.

Misión

La Unidad Educativa Particular PCEI "LÍDERES", inspirada en el servicio a la comunidad, busca garantizar el acceso y a la continuidad de la educación básica superior y bachillerato de jóvenes y adultos con escolaridad inconclusa, mediante procesos virtuales innovadores, que garantice una educación integral con calidad y calidez, brindando las oportunidades para la inserción en los ámbitos laborales y de educación superior.

Visión

Para el 2025, La Unidad Educativa Particular PCEI "LÍDERES" será un referente en el servicio de educación virtual y autónoma en los subniveles de Educación Básica Superior y Bachillerato General Unificado en Ciencias, constituyéndose como una institución de carácter inclusivo e intercultural, con el fin de mejorar la calidad de vida de nuestros estudiantes, para el desarrollo de nuestro país.

Objetivo

Establecer políticas de seguridad que regulen el proceso de comunicación entre los dispositivos IoT de oficina, de La Unidad Educativa Particular PECI LÍDERES.

Alcance

Todos los empleados de la institución La Unidad Educativa Particular PECI LÍDERES, están obligados a cumplir las políticas establecidas en este manual y debe ser seguido por todos los que utilicen los dispositivos IoT de la institución para fines relacionados con el trabajo.

Definiciones

- **IoT (Internet Of Things)**

  La red de objetos físicos con sensores integrados, software y otras tecnologías que pueden comunicarse y compartir datos con otros sistemas y dispositivos a través de Internet se conoce como Internet de los objetos o IoT.

- **Encriptación**

  El proceso de convertir texto plano legible por el ser humano en texto cifrado, que es un texto incomprensible.

- **AES (Advanced Encryption Standard)**

  Uso de un cifrado simétrico por bloques para cifrar información privada.

- **RSA (Rivest-Shamir-Adleman)**

  El algoritmo más popular de este tipo, la factorización entera, se utiliza en un sistema criptográfico de clave pública.

- **Firmware**

  Se describe como un tipo de software que se instala en la memoria de lectura de un dispositivo y se encarga de dar instrucciones sobre cómo comportarse, así como de activar normalmente las funciones fundamentales del dispositivo.

- **Cortafuegos**

  Un cortafuegos es un componente de una red o sistema informático destinado a impedir el acceso no deseado y permitir al mismo tiempo la comunicación legítima.

Marco Normativo

El Marco normativo para el Manual de políticas de seguridad para el proceso de comunicación entre los dispositivos IoT mediante métodos de encriptación se sustenta en las siguientes regulaciones y estándares:

Ley Orgánica de Protección de Datos Personales (LOPDP): Esta ley regula el tratamiento de datos personales en Ecuador y establece las medidas de seguridad que deben implementarse para proteger la privacidad de los individuos.

GDPR (Reglamento General de Protección de Datos): Este reglamento de la Unión Europea establece las normas para la protección de los datos personales de los ciudadanos europeos y exige que se implementen medidas de seguridad adecuadas, como la encriptación de datos, para garantizar su protección.

ISO/IEC 27001: Esta norma internacional establece los requisitos para la implementación de un sistema de gestión de seguridad de la información y recomienda la utilización de métodos de encriptación para proteger los datos.

NIST (Instituto Nacional de Estándares y Tecnología): Las guías y estándares del NIST proporcionan recomendaciones para la seguridad de la información, incluyendo el uso de encriptación para proteger la comunicación entre dispositivos IoT.

OWASP (Open Web Application Security Project): Esta organización ofrece pautas y herramientas para mejorar la seguridad de las aplicaciones web y móviles, incluyendo la encriptación de datos para proteger la comunicación entre dispositivos IoT.

Estos marcos normativos y estándares proporcionan una base sólida para la elaboración de un manual de políticas de seguridad para el proceso de comunicación entre dispositivos IoT mediante métodos de encriptación, ayudando a garantizar la protección de los datos y la privacidad de los usuarios.

1. Descripción de las Políticas

A continuación, se establecen políticas de seguridad para el proceso de comunicación entre los dispositivos IoT, mediante métodos de encriptación, las mismas que deben en el momento de su implementación deben ser cumplidas por todos los servidores de la unidad educativa Líderes.

1.1. Política de encriptación

Objetivo: Establecer un marco de políticas claras y concisas que regulen la seguridad en el proceso de comunicación entre dispositivos IoT.

Lineamientos

a. Se debe establecer un conjunto de políticas de seguridad que regulen el proceso de comunicación entre los dispositivos IoT de oficina.
b. Las políticas deben incluir directrices claras sobre el uso de métodos de encriptación para proteger la comunicación.

Responsables:

- Jefe del departamento de TIC de la institución
- Coordinador de Servicios TIC

1.2. Selección de métodos de encriptación

Objetivo: Implementar métodos de encriptación robustos y actualizados para proteger la integridad y confidencialidad de la información transmitida entre los dispositivos.

Lineamientos

a. Se debe seleccionar un método de encriptación robusto y seguro para proteger la comunicación entre los dispositivos IoT de oficina.
b. Los métodos de encriptación recomendados incluyen AES (Advanced Encryption Standard) y RSA (Rivest-Shamir-Adleman).

1.2.1. Implementar encriptación de extremo a extremo

Asegurarse de que la comunicación entre los dispositivos IoT de hogar esté protegida con encriptación de extremo a extremo. Esto significa que la información se encripta en el dispositivo de origen y se desencripta en el dispositivo de destino, evitando así que los datos sean interceptados o manipulados.

1.2.2. Utilizar protocolos de encriptación seguros

Emplear protocolos de encriptación seguros, como TLS (Transport Layer Security) o HTTPS (Hypertext Transfer Protocol Secure), para proteger la comunicación entre los dispositivos IoT. Estos protocolos garantizan la validez, confidencialidad e integridad de los datos transferidos.

1.2.3. Actualizar regularmente los algoritmos de encriptación

Mantenerse al día con los avances en la tecnología de encriptación y actualizar los algoritmos de encriptación utilizados en los dispositivos IoT de hogar. Esto ayudará a proteger la comunicación contra posibles vulnerabilidades y ataques.

Responsables:

- Jefe del departamento de TIC de la institución
- Coordinador de Servicios TIC

1.3. Gestión de claves

Objetivo: Definir roles y responsabilidades claras para el personal encargado de la implementación y mantenimiento de las medidas de seguridad en el proceso de comunicación de los dispositivos IoT.

Lineamientos

1.3.1. Generar claves fuertes

Utilizar algoritmos de generación de claves seguros para crear claves de encriptación sólidas. Las claves deben tener una longitud adecuada y ser generadas de forma aleatoria para garantizar su seguridad.

1.3.2. Almacenar las claves de forma segura

Proteger las claves de encriptación almacenándose en un lugar seguro y accesible solo para usuarios autorizados. Evitar almacenar las claves en dispositivos vulnerables o en lugares fácilmente accesibles.

1.3.3. Rotar las claves periódicamente

Establecer un programa de rotación de claves para cambiar las claves de encriptación de forma regular. Estas rotaciones ayudarán a prevenir posibles compromisos de seguridad y garantizarán la confidencialidad de la comunicación.

1.3.4. Gestión de claves de encriptación

a. Se debe establecer un sistema de gestión de claves de encriptación para garantizar la seguridad de las claves utilizadas en el proceso de comunicación.
b. Las claves de encriptación deben ser almacenadas de forma segura y protegidas contra accesos no autorizados.

Responsables:

- Jefe del departamento de TIC de la institución
- Coordinador de Servicios TIC

1.4. Seguridad del sistema

Objetivo: Establecer procedimientos de respuesta a incidentes de seguridad para actuar de manera rápida y eficiente en caso de detectarse una amenaza o vulnerabilidad en el proceso de comunicación entre dispositivos IoT.

Lineamientos

1.4.1. Actualizar el firmware de los dispositivos

Mantener actualizado el firmware de los dispositivos IoT de hogar para protegerlos contra posibles vulnerabilidades de seguridad. Instalar regularmente las actualizaciones de seguridad proporcionadas por los fabricantes.

1.4.2. Implementar cortafuegos y medidas de seguridad de red

Configurar cortafuegos y otras medidas de seguridad de red para proteger los dispositivos IoT de hogar de posibles ataques externos. Establecer políticas de seguridad para controlar el tráfico de red y limitar el acceso no autorizado.

1.4.3. Monitorear y auditar la seguridad

Implementar sistemas de monitoreo y auditoría para vigilar la seguridad de los dispositivos IoT domésticos y detectar posibles anomalías o ataques. Analizar regularmente los registros de seguridad y responder de manera proactiva a cualquier incidente de seguridad.

Responsables:

- Jefe del departamento de TIC de la institución
- Coordinador de Servicios TIC

1.5. Implementación de la encriptación

Objetivo: Establecer lineamientos para la adecuada gestión implementación de las políticas a todos los dispositivos IoT, estableciendo claves seguras

Lineamientos

a. La encriptación debe implementarse en todos los dispositivos IoT de oficina que participan en el proceso de comunicación.
b. Se deben establecer claves de encriptación seguras y únicas para cada dispositivo y canal de comunicación.

Responsables:

- Equipo de tecnología de la información (TI)

- Jefe del departamento de TIC de la institución
- Coordinador de Servicios TIC

1.6. Actualización y mantenimiento

Objetivo: Mantener actualizados los procedimientos de seguridad y las medidas de protección para garantizar la integridad, confidencialidad y disponibilidad de los dispositivos IoT y datos conectados a la red.

Lineamientos

a. Se debe realizar una revisión periódica de las políticas de seguridad y los métodos de encriptación utilizados en el proceso de comunicación.
b. Se deben aplicar actualizaciones y parches de seguridad de forma regular para garantizar la protección de la comunicación.

Responsables:

- Equipo de tecnología de la información (TI)
- Jefe del departamento de TIC de la institución
- Coordinador de Servicios TIC
- Junta directiva de la Institución

1.7. Auditoría y monitorización

Objetivo: Realizar auditorías periódicas para evaluar la efectividad de las políticas de seguridad y detectar posibles vulnerabilidades en el proceso de comunicación entre dispositivos IoT.

Lineamientos

a. Se debe realizar una auditoría regular del proceso de comunicación entre los dispositivos IoT de oficina para garantizar el cumplimiento de las directrices de seguridad.
b. Se debe implementar un sistema de monitorización para detectar posibles amenazas y actividades maliciosas en la red

Responsables

- Jefe del departamento de TIC de la institución
- Coordinador de Servicios TIC

2. Sensibilización y Comunicación

La Unidad Educativa particular PCEI Líderes, por medio de su departamento de TI y alta gerencia, realizará capacitaciones e inducciones de las políticas de seguridad para el proceso de comunicación entre los dispositivos IoT, mediante métodos de encriptación, con el objetivo de que los colaboradores de la entidad tengan pleno conocimiento de las políticas de seguridad de seguridad que se implementarían en la oficial de la institución.

3. Mejoras

3.1. Mejora continua

Para realizar acciones de mejora continua sobre la efectividad del Manual de políticas de seguridad para el proceso de comunicación entre los dispositivos IoT, mediante métodos de encriptación.

- Establecer un proceso de revisión periódica del manual de políticas de seguridad para mantenerlo actualizado con las últimas tecnologías y mejores prácticas en encriptación.
- Definir claramente los algoritmos de encriptación que se utilizarán para proteger la comunicación entre los dispositivos IoT, asegurándose de que sean robustos y seguros.
- Implementar mecanismos de autenticación fuertes, como el uso de certificados digitales, para garantizar la identidad de los dispositivos que se comunican entre sí.
- Establecer políticas de gestión de claves para asegurar que las claves de encriptación se generen, almacenen y compartan de forma segura.
- Capacitar al personal involucrado en el proceso de comunicación entre dispositivos IoT en buenas prácticas de seguridad, como el uso de contraseñas seguras y la protección de la información confidencial.
- Realizar pruebas de penetración de forma regular para detectar posibles vulnerabilidades en el sistema de comunicación y tomar medidas correctivas de forma oportuna.

- Establecer un proceso de respuesta a incidentes de seguridad que permita actuar rápidamente en caso de una brecha de seguridad en la comunicación entre dispositivos IoT.

Al implementar estas recomendaciones, se mejorará la seguridad del proceso de comunicación entre dispositivos IoT mediante métodos de encriptación, protegiendo la información sensible y garantizando la confidencialidad e integridad de los datos transmitidos.

3.2. Manejo de Excepciones

a. **Excepción por incompatibilidad de dispositivos:** Si un dispositivo IoT no es compatible con los métodos de encriptación establecidos en el manual de políticas de seguridad, se podrá conceder una excepción temporal siempre y cuando se implementen medidas alternativas de seguridad para proteger la comunicación.
b. **Excepción por necesidades operativas:** En situaciones en las que la encriptación afecte la operatividad de los dispositivos IoT y sea necesario deshabilitar temporalmente los métodos de encriptación, se podrá conceder una excepción siempre y cuando se notifique de inmediato al responsable de seguridad de la unidad educativa y se tomen medidas adicionales para minimizar los riesgos de seguridad.
c. **Excepción por problemas de rendimiento:** Si la implementación de métodos de encriptación afecta significativamente el rendimiento de los dispositivos IoT y se demuestra que no es factible mantenerlos activos, se podrá conceder una excepción temporal sujeta a revisión periódica para evaluar la situación.
d. **Excepción por actualización de tecnología:** En caso de que surjan nuevas tecnologías de encriptación que superen las utilizadas en el manual de políticas de seguridad, se podrá conceder una excepción para la implementación de estas nuevas tecnologías siempre y cuando se realice una evaluación de riesgos y se garantice una transición segura y efectiva.

Es importante tener en cuenta que las excepciones deben ser autorizadas por el responsable de seguridad de la unidad educativa y deben estar debidamente justificadas y documentadas para garantizar la integridad y confidencialidad de la comunicación entre los dispositivos IoT.

Control de Modificaciones

Control de Modificaciones		
Versión	Fecha Modificación	Naturaleza del cambio
01		

Registro de Aprobación

Registro de Aprobación					
Elaborado		**Revisado**		**Aprobado**	
Nombre:	Diego Atiaja	**Nombre:**	Lucia Collaguazo	**Nombre:**	Alejandro Caisatoa
Cargo:	Ingeniero en Sistemas	**Cargo:**	Secretaria Estudiantil	**Cargo:**	Rector de la Institución

CONCLUSIONES

En relación a la investigación realizada se determina a continuación las siguientes conclusiones:

Es necesario contar con conocimientos sólidos de los fundamentos teóricos detrás de las políticas de seguridad en el Internet de las Cosas (IoT) para poder tratar de manera efectiva las vulnerabilidades presentes en los dispositivos IoT. La información privada y personal de los usuarios debe protegerse constantemente, y estas medidas de seguridad deben ser contextuales y adaptarse a las características únicas de cada dispositivo y entorno en el que se utilizan.

Actualmente existen una serie de vulnerabilidades en la seguridad de los dispositivos IoT que pueden ser utilizados por los ciberdelincuentes para obtener datos privados o tomar el control de los dispositivos. Unas contraseñas débiles, una seguridad de red insuficiente o la falta de actualizaciones de seguridad pueden dar paso a estas vulnerabilidades. Para garantizar la seguridad de los dispositivos IoT, deben aplicarse medidas preventivas, es fundamental educar a los usuarios sobre el valor de proteger sus dispositivos y mantenerse actualizados de las amenazas cibernéticas más recientes.

Es fundamental diseñar un manual de políticas de seguridad para el proceso de comunicación entre los dispositivos IoT, mediante métodos de encriptación. La realización de medidas de seguridad basadas en criptografía que sea sólidas es necesario para garantizar la integridad y confidencialidad de los datos transmitidos a través de la red de dispositivos IoT. Es fundamental mantenerse actualizado con las últimas tecnologías y enfoques en seguridad para garantizar la protección efectiva de la red de dispositivos IoT.

La validación del manual propuesto mediante criterio de expertos es un paso importante en el proceso de desarrollo, ya que genera una perspectiva externa y especializada que contribuye a mejorar la calidad y efectividad del manual.

RECOMENDACIONES

En base al análisis realizado y resultados obtenidos a la Unidad Educativa Particular PECI LÍDERES, se plantea las siguientes recomendaciones:

Se recomienda implementar el Manual de políticas de seguridad para el proceso de comunicación entre los dispositivos IoT propuesto, que permite controlar los dispositivos IoT.

Se recomienda desarrollar un protocolo de seguridad que incluya la autenticación del dispositivo con el fin de impedir accesos no deseados a la red.

Se recomienda capacitar al personal de la institución encargado de la seguridad de los dispositivos IoT en el uso adecuado de los métodos de encriptación, así como en la detección y respuesta ante posibles vulnerabilidades.

Se recomienda realizar auditorías de seguridad periódicas que evalúen la eficacia de las medidas de protección implementadas y realizar las actualizaciones para preservar la seguridad de las redes de dispositivos IoT.

BIBLIOGRAFÍA

Amos, Z. (2023, March 23). *Abordando las vulnerabilidades de ciberseguridad en los dispositivos IoT | Ridge Security*. https://ridgesecurity.ai/es/blog/abordando-las-vulnerabilidades-de-ciberseguridad-en-los-dispositivos-iot/

AWS Amazon. (2023). *¿Qué es la criptografía?* https://aws.amazon.com/es/what-is/cryptography/

Azure. (2024). *Protocolos y tecnologías de IoT | Microsoft Azure*. https://azure.microsoft.com/es-mx/solutions/iot/iot-technology-protocols

Bermúdez, A. (2022). *Ciberseguridad en los servicios que usan dispositivos IoT para los usuarios del sector residencial | Enhanced Reader* [UNIVERSIDAD LATINA DE COSTA RICA]. https://repositorio.ulatina.ac.cr/bitstream/20.500.12411/1697/1/TFG_Ulatina_Aurora_Bermudez_Lopez_200403009921.pdf

Casarrubias, E., Castro, J., Hernández, R., & Galarce Jorge. (2022). *Vista de VULNERABILIDADES DE LAS REDES IoT*. https://www.innovaingenieria.uagro.mx/innova/index.php/innova/article/view/78/39

Cuji, J., & Araujo, M. (2024). *Soluciones de seguridad en sistemas iot de hogares inteligentes para mitigar riesgos y vulnerabilidades mediante la realización de pruebas de penetración*. https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/40766

Fernández, J. (2024). *Implementación de IoT Honeypot y análisis de resultados*. *01*.

González, L., Sofía, O., Laguía, D., Gesto, E., & Hallar, K. (2020). *Internet Del Futuro Estudio De Tecnologias IoT*. https://doi.org/10.22305/ict-unpa.v12.n3.744

ITSitio. (2020, June 23). *Vulnerabilidades de los dispositivos IoT - ITSitio*. https://www.itsitio.com/seguridad/vulnerabilidades-los-dispositivos-iot/

Kaspersky. (2024). *¿Qué es la Internet de las cosas (IoT) y qué son los dispositivos de IoT?* https://latam.kaspersky.com/resource-center/definitions/what-is-iot

López, J. (2020, November 1). *Investigación explicativa - Qué es, definición y concepto*. https://economipedia.com/definiciones/investigacion-explicativa.html

Molina, J. (2019). *LA IMPORTANCIA DE LA GESTIÓN DE RIESGOS Y SEGURIDAD EN EL INTERNET DE LAS COSAS (IOT)* .

Navas Damas, M. (2023). *Criptografía simétrica y asimétrica*. http://crea.ujaen.es/jspui/handle/10953.1/19494

Olivarez, G., Dionicio, P. ;, Gil, L., José, A., De, M., Santos, L., Carlos, A., Olivarez, P., Dionicio, G., Nacional De Trujillo, U., Universidad, T., & Nacional, A. (2023). Principales técnicas criptográficas aplicadas a la seguridad de la información en IoT: una revisión sistemática. *Periodicidad: Frecuencia Continua*, *5*, 2023.

ONU Ecuador. (2024). *Sustainable Development Goal 4: Educación de calidad | Naciones Unidas en Ecuador*. https://ecuador.un.org/es/sdgs/4

Patiño, R., & Sánchez, E. (2021). *Las amenazas de seguridad a las que se enfrenta IoT y las soluciones en desarrollo*.

PCEI "LÍDERES." (2024). *Institucion Educativa IEPCEI "LÍDERES."* http://www.iepceilideres.com/

Pérez, K. A. (2020). *Tendencias en educación utilizando dispositivos IOT*. 6–7. http://dspace.udla.edu.ec/handle/33000/13092

Qualtrics. (2024). *Investigación cuantitativa: definición y procedimiento | Qualtrics*. https://www.qualtrics.com/es/gestion-de-la-experciencia/investigacion/investigacion-cuantitativa/

Ríos, J. (2023, September 30). *Cuáles son los ciberataques más comunes a lavadoras, televisores y más dispositivos IoT - Infobae*. https://www.infobae.com/tecno/2023/09/30/cuales-son-los-ciberataques-mas-comunes-a-lavadoras-televisores-y-mas-dispositivos-iot/

Rivadeneira, C. (2020). *Evaluación de rendimiento entre el estándar de mensajería MQTT y la plataforma Firebase a través de un prototipo, modelo de comunicación IoT*. http://repositorio.uisrael.edu.ec/handle/47000/2751

Universidad Veracruzana. (2024). *Introducción a la Investigación: guía interactiva*. https://www.uv.mx/apps/bdh/investigacion/unidad1/investigacion-tipos.html

Villacis Miguel. (2023). *ANÁLISIS DE BRECHAS DE SEGURIDAD EN REDES LPWAN: SIGFOX Y LORAWAN EN BASE A LA NORMA ISO 27001:2013*. http://repositorio.uisrael.edu.ec/handle/47000/3564

ANEXOS

ANEXO 1

TABLAS DE CAPAS DE ARQUITECTURA IOT

Tabla 4

Capas de la arquitectura IoT

Capa	Acción	Ejemplo
Capturar los datos	Por medio de los sensores el dispositivo captura los datos desde su entorno para un propósito práctico.	Coordenadas GPS Temperatura
Conectividad	Por medio de conexión a la red. Los dispositivos IoT, envían la información a la nube. La aplicación IoT determinará qué opción de conectividad le conviene más.	Conexión Wi-Fi, Bluetooth, satélite Redes de baja potencia y área amplia (LPWAN, por sus siglas en inglés) Conexión directa a Internet vía Ethernet.
Procesamiento de datos	Tras procesar los datos, el software decide si debe o no realizar una determinada acción.	Envió de alertas Ajustes automáticos de sensores Interacción usuario
Actuar a partir de los datos	Se examinan los datos totales de una red IoT recopilados de todos sus dispositivos. Esto ofrece datos estratégicos sólidos para respaldar decisiones y acciones corporativas fiables, si la intervención del usuario es necesaria o requiere controlar el sistema, para toma de decisiones	

Nota: información tomada de (Kaspersky, 2024)

ANEXO 2

TABLAS DE VULNERABILIDADES IOT

Tabla 5

Vulnerabilidades IoT

Vulnerabilidad	Descripción
Credenciales débiles	Usuario no cambia contraseñas que trae el dispositivo por defecto o a su vez designa credenciales muy sencillas.
Protocolos de cifrado inseguros	Al existir múltiples empresas que elaboran los dispositivos IoT desarrollan sus propios protocolos, utilizan protocolos de cifrados inseguros
Inexistencia de Cifrado	No poseen cifrados para el proceso de comunicación o si existen son inseguros
Características de seguridad que no pueden modificarse	Presentan configuraciones de seguridad predeterminadas, que no ser modificadas
Falta de actualizaciones	En determinados casos no existen actualizaciones para corrección de fallos
Puertas traseras existen de fabrica	Existen dispositivos IoT que poseen backdoors instaladas de fabrica

Nota: Información tomada de (Casarrubias et al., 2022)

ANEXO 3

ATAQUES FRECUENTES A DISPOSITIVOS IOT

Figura 21

Ataques frecuentes a dispositivos IoT

Nota: Información tomada de (Casarrubias et al., 2022)

ANEXO 4

OBJETIVOS DE LA CRIPTOGRAFÍA

Figura 22

Objetivos de la criptografía

Nota: Información tomada de (AWS Amazon, 2023)

ANEXO 5

CAPTURAS DE ESCANEOS CON HERRAMIENTAS

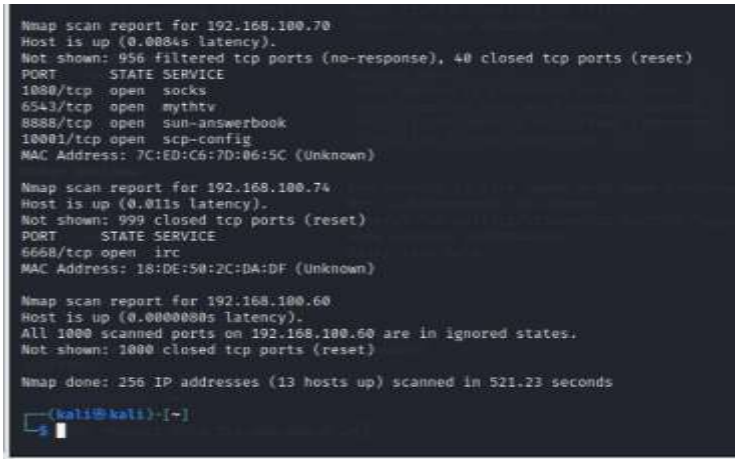
Figura 23

Escaneo punto por punto 2

En las figuras se puede observar la información de cada dispositivo , como es la dirección IP, en especial los puertos que se encuentran abiertos

Figura 24

Escaneo punto por punto 3



ANEXO 6

FORMATO DE ENCUESTA

Sección 1 de 4

Encuesta referente a la seguridad de los dispositivos IoT (Internet de las cosas)

La presente encuesta tiene como finalidad recabar información, referente al conocimiento de los usuarios de la institución, sobre IoT vulnerabilidades y Políticas de seguridad

Sección 2 de 4

Conocimiento General sobre dispositivos IoT

¿Está familiarizado con el término IoT (Internet de las cosas)?

- Si
- No

¿Utiliza dispositivos IoT en su entorno de oficina?

- Si
- No
- Tal vez

¿Está al tanto de las posibles vulnerabilidades de seguridad en los dispositivos IoT?

- Si
- No
- Tal vez

¿Ha experimentado algún tipo de incidente de seguridad relacionado con tus dispositivos IoT en el pasado?

- Si
- No
- Tal vez

Sección 3 de 4

Importancia de la seguridad en los dispositivos IoT

¿Considera que la formación y concienciación del personal es fundamental para garantizar la seguridad en la comunicación entre dispositivos IoT de oficina?

- Si
- No
- Tal vez

¿Ha experimentado alguna vez algún incidente de seguridad relacionado con dispositivos IoT en su entorno de oficina?

- Si
- No
- Tal vez

¿Considera que la seguridad en dispositivos IoT es importante para proteger la privacidad y la información de los usuarios?

- Si
- No
- Tal vez

¿Cree que los usuarios deben recibir información y formación sobre cómo proteger sus dispositivos IoT?

- Si
- No
- Tal vez

¿Está dispuesto a pagar un precio más alto por un dispositivo IoT con mejores medidas de seguridad?

- Si
- No
- Tal vez

¿Considera que la colaboración entre fabricantes, usuarios y autoridades es clave para garantizar la seguridad en los dispositivos IoT?

- Si
- No
- Tal vez

¿Cree que las empresas fabricantes de dispositivos IoT deben realizar pruebas de seguridad antes de lanzar un producto al mercado?

- Si
- No
- Tal vez

Sección 4 de 4

Mejoras para seguridad de dispositivos IoT

¿Cree que la comunicación entre dispositivos IoT debe estar protegida mediante métodos de encriptación?

- Si
- No
- Tal vez

¿Cree que es importante establecer políticas de seguridad específicas para proteger la comunicación entre dispositivos IoT en el entorno de oficina?

- Si
- No
- Tal vez

¿Está de acuerdo en que se establezcan normativas y estándares de seguridad para los dispositivos IoT?

- Si
- No
- Tal vez

¿Qué medidas de seguridad considera más importantes para los dispositivos IoT?

- Encriptación de datos
- Autenticación de usuarios
- Actualizaciones periódicas de software

¿Qué propuestas o sugerencias tiene para mejorar la seguridad en los dispositivos IoT?

- Establecer colaboración entre fabricantes, usuarios y autoridades
- Implementar normativas y estándares de seguridad obligatorios
- Mejorar la formación sobre seguridad en dispositivos IoT

¿Cree que se necesita una regulación más estricta para garantizar la seguridad de los dispositivos IoT?

- Si
- No
- Tal vez

ANEXO 7

VALIDACIÓN DE LA PROPUESTA

Figura 25

Validación Interna 1

INSTRUMENTO DE VALIDACIÓN

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 siguiente propuesta del proyecto de titulación: Propuesta de un manual de políticas de seguridad para el proceso de comunicación entre los dispositivos IoT, mediante métodos de encriptación

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos
Validado por: Lucia Collaguazo
Licenciada en Ciencias de la Educación mención Administración Educativa
Título obtenido
1716270614
Cédula de Identidad
Lucygkd@gmail.com
E- mail
UNIDAD EDUCATIVA PARTICULAR PCEI "LÍDERES"
Institución de Trabajo
SECRETARIA ACADÉMICA
Cargo
22 AÑOS
Años de experiencia en el área

1

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- 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: Propuesta de un manual de políticas de seguridad para el proceso de comunicación entre los dispositivos IoT, mediante métodos de encriptación.

Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	X				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*	X				
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	X				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	X				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	X				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	X				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	X				
Total		35				

Observaciones:

_____

_____

Recomendaciones

_____

_____

Lugar, fecha de validación: 07/03/2024

_____

Firma del especialista

2

Figura 26

Validación Externa

INSTRUMENTO DE VALIDACIÓN

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 siguiente propuesta del proyecto de titulación: Propuesta de un manual de políticas de seguridad para el proceso de comunicación entre los dispositivos IoT, mediante métodos de encriptación

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: JOSE LUIS RODRIGUEZ ABRIL

Título obtenido
MASTER UNIVERSITARIO EN DIRECCION E INGENIERIA EN SITIOS WEB
Cédula de Identidad
1709769663
E- mail
jlra201602@gmail.com
Institución de Trabajo
TOPAZ
Cargo
Developer Analyst
Años de experiencia en el área
2

1

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- 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: Propuesta de un manual de políticas de seguridad para el proceso de comunicación entre los dispositivos IoT, mediante métodos de encriptación.

Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	X				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*	X				
–Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	X				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	X				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	X				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	X				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	X				
Total		*35*				

Observaciones:

_____

_____

Recomendaciones

_____

_____

Lugar, fecha de validación: Quito, 7 de marzo del 2024

_____

Firma del especialista

2

esta lento el ambiente