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 MAGÍSTER

Título del proyecto:
ANÁLISIS DE BRECHAS DE SEGURIDAD EN REDES LPWAN: SIGFOX Y LORAWAN EN BASE A LA NORMA ISO 27001:2013
Línea de Investigación:
SEGURIDAD INFORMÁTICA
Campo amplio de conocimiento:
TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
Autor:
ING. MIGUEL LEOPOLDO VILLACIS ESPINOSA
Tutor:
ING. PABLO MARCEL RECALDE VARELA MSc.

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, MSc. Pablo Marcel Recalde Varela con C.I:1711685055 en mi calidad de Tutor del proyecto de investigación titulado: ANÁLISIS DE BRECHAS DE SEGURIDAD EN REDES «LPWAN» - «SIGFOX» Y LORAWAN EN BASE A LA NORMA ISO 27001:2013.

Elaborado por: Miguel Leopoldo Villacís Espinosa, de C.I: 1716282510, estudiante de la Maestría: en SEGURIDAD INFORMÁTICA, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL,** 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 2023

PABLO MARCEL RECALDE VARELA

_____

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Universidad Israel

Yo, Miguel Leopoldo Villacís Espinosa con C.I: 1716282510, autor del proyecto de titulación denominado: ANÁLISIS DE BRECHAS DE SEGURIDAD EN REDES «LPWAN» - «SIGFOX» Y LORAWAN EN BASE A LA NORMA ISO 27001:2013. 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 2023

_____

Firma

https://orcid.org/0000-0003-4442-6938

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

Desde hace varios años atrás, el denominado «*internet de las cosas (IoT, por sus siglas en inglés)*» se ha venido incorporando a la economía mundial de forma progresiva y exponencial, generando diversos mercados de soluciones y comodidades tanto para la industria como para el hogar. Las aplicaciones de *«IoT»* se pueden usar para monitoreo en general por medio de sensores electrónicos como son sensores de humedad, de presión, de proximidad, de temperatura, etc; así como se los puede usar para hogares inteligentes, medición inteligente, monitoreo de fábricas, agricultura, edificios inteligentes, etc. Las tecnologías inalámbricas de corto alcance o también conocidas como redes de área personal de sus siglas en inglés (Redes PAN) como son Bluetooth, WiFi, ZigBee, etc., solían cumplir con los requisitos de comunicación para el *«IoT»*; sin embargo, debido a que son tecnologías de conectividad para corto alcance, limitaban la funcionalidad de los dispositivos de *«IoT»*. (Hernádez, 2019)

Es por ello que para superar las limitaciones de los protocolos de comunicaciones inalámbricas de corto alcance se introducen las denominadas redes de área amplia de baja potencia (*«*LPWAN» de sus siglas en inglés), ofreciendo una conectividad de largo alcance en el orden de kilómetros. Las redes «LPWAN» permiten que los dispositivos *«IoT»* intercambien pequeños mensajes a largas distancias con un nivel de consumo muy bajo de potencia, logrando que los dispositivos de *«IoT»* tenga una eficiencia en su consumo y tiempo de vida útil de varios años con baterías pequeñas, lo que ha llevado a evidenciar que por estas características se convierte en una solución muy bien aceptada en el ámbito industrial por sus múltiples usos. (Hernádez, 2019)

En tal virtud se plantea la contextualización del tema como analizar a estas tecnologías de comunicaciones en el ámbito de la seguridad de la Información por medio de la *«Norma Internacional ISO 27001:2013»,* procurando levantar un conjunto de posibles amenazas y vulnerabilidades, indicar las brechas de cada una y procurar mitigar sus afectaciones con la ejecución y asignación de Técnicas de Control y Controles de la Norma una vez realizado el análisis de riesgos de dichas amenazas o vulnerabilidades. (Pérez, 2018)

Problema de investigación

Una vez mencionadas estas tecnologías que son muy aceptadas por las personas y en el orden empresarial, cabe realizarse la pregunta ¿qué tan seguras son?, ¿qué se debe y que no se debe transmitir?, ¿qué se debe y que no se debe exponer de la información personal o empresarial sobre este tipo de redes y componentes?

Para ello se plantea realizar una investigación comparativa entre las dos tecnologías más utilizadas comercialmente las que son «Sigfox» y Lora Wan, toda vez que cada una difiere en sus características técnicas será una muy buena oportunidad de verificación de cual es más susceptible a ataques de seguridad de la información, en base a la *«Norma Internacional ISO 27001:2013»*, una vez levantado el conjunto de posibles vulnerabilidades y amenazas se realizará un análisis de riesgos y para su tratamiento se lo realizará con los Técnicas de Control y Controles de la mencionada norma. (Hernádez, 2019)

Es importante mencionar que este tipo de redes son relativamente nuevas y se podría indicar que se encuentran aún en desarrollo, y al ser una más comercial que la otra, existe muy poca bibliografía sobre redes Lorawan; sim embargo llama la atención sus características técnicas por lo que se encuentra siendo mucho más desplegada y utilizada. (Hernádez, 2019)

¿Qué se debe y que no se debe transmitir?

Objetivo general

Realizar el análisis de brechas de seguridad informática en las comunicaciones inalámbricas «Sigfox» y Lorawan, bajo la *«Norma Internacional ISO 27001:2013»* aplicado a los dispositivos de *«IoT».*

Objetivos específicos

1. Contextualizar los fundamentos teóricos de la seguridad informática en el ámbito de las tecnologías de *«IoT»* fundamentándose en el marco de referencia de *la «Norma Internacional ISO 27001:2013».*

2. Calcular las matrices de brechas de seguridad, gestión de riesgos, aplicación de Técnicas de Control y Controles sobre las tecnologías de «LPWAN» escogidas bajo la *«Norma Internacional ISO 27001:2013»*

3. Determinar la existencia o no de las brechas de seguridad informática en las redes de área extendida de baja potencia «LPWAN» como son «Sigfox» y Lorawan, en base a la *«Norma Internacional ISO 27001:2013».*

4. Validar si la aplicación de las técnicas de control y controles, establecidos en la *«Norma Internacional ISO 27001:2013»* son eficaces para solventar o disminuir el impacto de las vulnerabilidades en las tecnologías escogidas.

Vinculación con la sociedad y beneficiarios directos:

Este trabajo de investigación coadyuvará a la sociedad y se integrará con la vinculación de la colectividad cuando el lector puede tener claro que son cada una de las tecnologías escogidas al no ser necesariamente un técnico en redes o telecomunicaciones; de igual manera cuando pueda entender o conocer el tipo de vulnerabilidades o amenazas sobre la seguridad de la Información se puede manejar en este tipo de dispositivos, de esta manera estará en la capacidad de decidir el uso o no de esta tecnología para sus dispositivos personales o a nivel industrial o empresarial.

El aporte a la sociedad será un documento de fácil entendimiento con análisis de riesgos y su debido tratamiento por medio de los Técnicas de Control y Controles de la «*Norma Internacional ISO 27001:2013»*, ayudando así a entender la Norma con un ejemplo de aplicación al escoger algunos Técnicas de Control y Controles para mitigar las posibles vulnerabilidades y amenazas encontradas en las redes LoraWan utilizadas para la tecnología de *«IoT».*

Con respecto a los Objetivos de Desarrollo Sostenible, este trabajo de investigación se enfoca en el objetivo número «nueve» que se denomina «Industria Innovación e Infraestructura», en virtud de que la «IoT» ha demostrado ser una tecnología innovadora de bajo costo y ahora con el desarrollo de estas redes de área amplia de baja potencia ayudan al medio ambiente con la disminución del consumo de energía almacenada como por ejemplo en el uso de baterías. De igual manera como es de conocimiento que la «IoT» ya se encuentra desarrollándose incluso para la industria, es importante mencionar que ayuda en los procesos de innovación, control y monitoreo lo que también decanta en una mejora considerable de la eficiencia energética al procurar ser amigable y de bajo consumo con el mismo.

Cabe también mencionar que este tipo de tecnologías se encuentran en franco desarrollo y evolución, por lo que este será un documento base que permitirá seguirlo alimentando hasta tener un compendio de las mejores prácticas para evitar posibles vulnerabilidades y amenazas en la seguridad del «IoT» y en la utilización de redes de área extendida de baja potencia.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

En este capítulo se pretende dar a conocer al lector una pequeña reseña histórica del desarrollo de la Seguridad Informática, la *«Norma Internacional ISO 27001:2013»*, de la evolución de la *«IoT»,* y de las tecnologías inalámbricas que se están desarrollando para que estos dispositivos tengan un mayor alcance.

1.1 Contextualización general del estado del arte

1.1.1 Seguridad de la Información

Esta definición llama a colación a cualquier técnica utilizada para proteger datos almacenados en los diferentes dispositivos de procesamiento, cómputo o de almacenamiento contra el acceso de personas o dispositivos no autorizados. Siendo esto posible por medio de la no alteración de la Confidencialidad, Integridad, y Disponibilidad de la información, así como de los sistemas implicados en su proceso, a nivel personal, dentro de una empresa o industria. (ISO 27001, 2021)

Norma ISO 27001

La Norma Internacional ISO proviene de la constitución de una familia de estándares, desarrollados por la Organización Internacional de Estandarización de sus siglas en inglés (ISO) y por Comisión Electrotécnica Internacional de sus siglas en inglés, (IEC) que son generalmente conocidas como las normas ISO 27000.

Esta familia de estándares fue desarrollada y publicada conforme la necesidad de contar con un procedimiento o proceso que permita establecer, implementar, controlar, mantener, e innovar u Sistema de Gestión de la Seguridad. (ISO 27001, 2021)

1.1.2 Internet de las Cosas

De la investigación realizada y la bibliografía consultada para la definición del estado del arte de este documento se puede evidenciar que las definiciones del *«IoT»* son muchas y muy similares en su idea fundamental es así que, se considera como la mejor definición que abarca el tema en análisis la siguiente:

«El Internet de las Cosas es la interconexión a través del Internet de dispositivos informáticos o electrónicos integrados en objetos cotidianos, lo que los permite enviar y recibir datos.» (Uribe Castro, 2021)

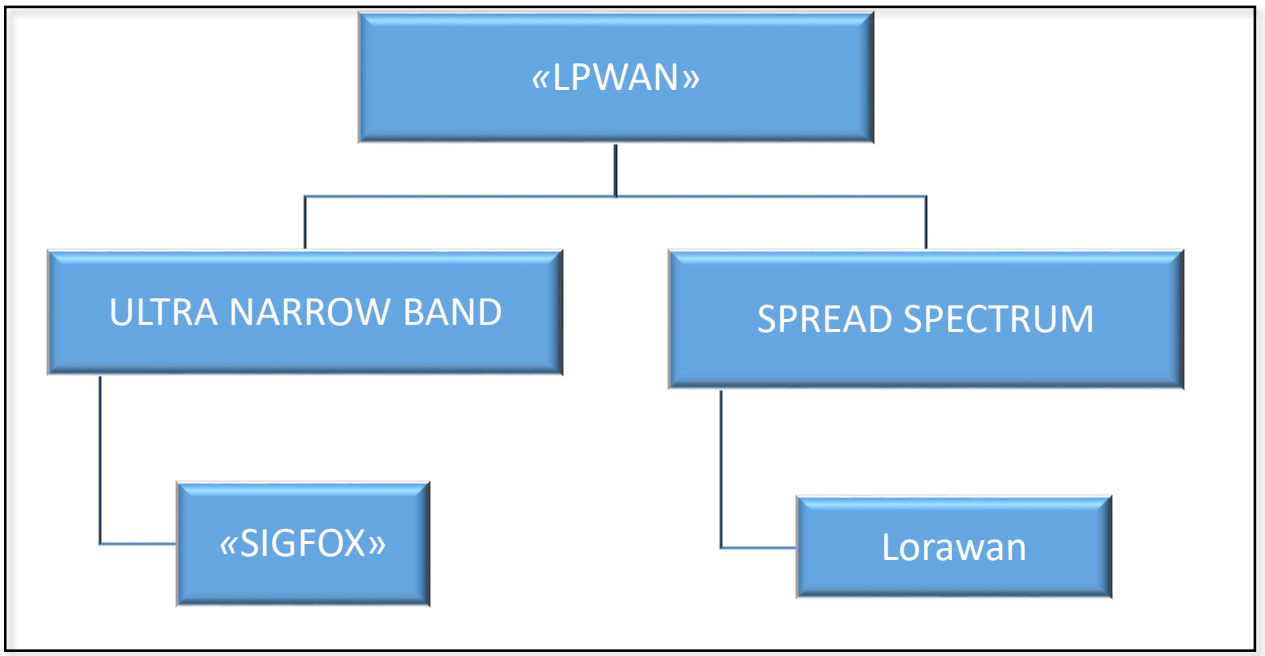
Tecnología «LPWAN»

Representa una clara evolución de las redes de comunicación orientadas hacia los dispositivos *«IoT».* Estas redes fueron diseñadas para interconectar una gran cantidad de

dispositivos, con un alcance superior a las tecnologías convencionales denominadas redes de área personal como Zigbee, bluetooth, wifi; usando la menor cantidad de recursos, pero sacrificando la velocidad de transmisión, lo que las hacia ideales para nueva tendencia de interconectar sensores y dispositivos de baja velocidad separados a distancias de área extendida, pero ineficaces para transmisión de voz, audio y video. (Eterovic, 2018)

Figura 1.

Redes de Área Extendida de Baja Potencia



Fuente: Elaboración propia (2023)

Para el desarrollo de este documento se ha evidenciado que si existen varios trabajos relacionados al tema desde el año 2018 en adelante; es así que se ha tomado como referencia bibliográfica 15 autores que entre artículos publicados y tesis de pregrado y posgrado nos indican que se puede apreciar claramente el desarrollo de estas tecnologías en el campo personal y de la industria y que lógicamente son susceptibles a ser analizadas en sus características técnicas, de desarrollo, de costo, de alcance, de eficiencia, de seguridad entre otras para poder ser puestas en el mercado como la mejor opción:

Dentro de la bibliografía investigada que demuestra los trabajos previos y que se podría ejemplarizar para la base de un Estado del Arte del tema se tiene la siguiente tabla.

Tabla 1.

Trabajos Previos

Nombre del trabajo	Año de Publicación
Redes LoRaWAN. Revisión de componentes funcionales en aplicaciones «IoT».	2019
Análisis de Seguridad en redes «LPWAN»	2018
Modelo de Seguridad «IoT»	2019
Análisis del Nivel de Seguridad presente en los dispositivos que componen el «IoT»	2019
Risk Management «IoT»_LGAH	2021
Estudio y Análisis de Protección y amenazas de seguridad en redes de comunicación	2020
Lorawan para control de incendio forestales	2018
Esquema de seguridad de datos entre los nodos y el gateway en una red lorawan	2020
Seguridad «IoT» principales amenazas en una taxonomía de activos	2020

Fuente: Elaboración Propia (2023)

1.2 Proceso investigativo metodológico

En este apartado se pretende indicar el proceso que se ha seguido para llegar a plantear los Técnicas de Control y Controles que la Norma ISO 27001:2013 brinda para mitigar las posibles amenazas y ataques en el campo de la seguridad de la información en *«IoT».*

1.3 Investigación Bibliográfica

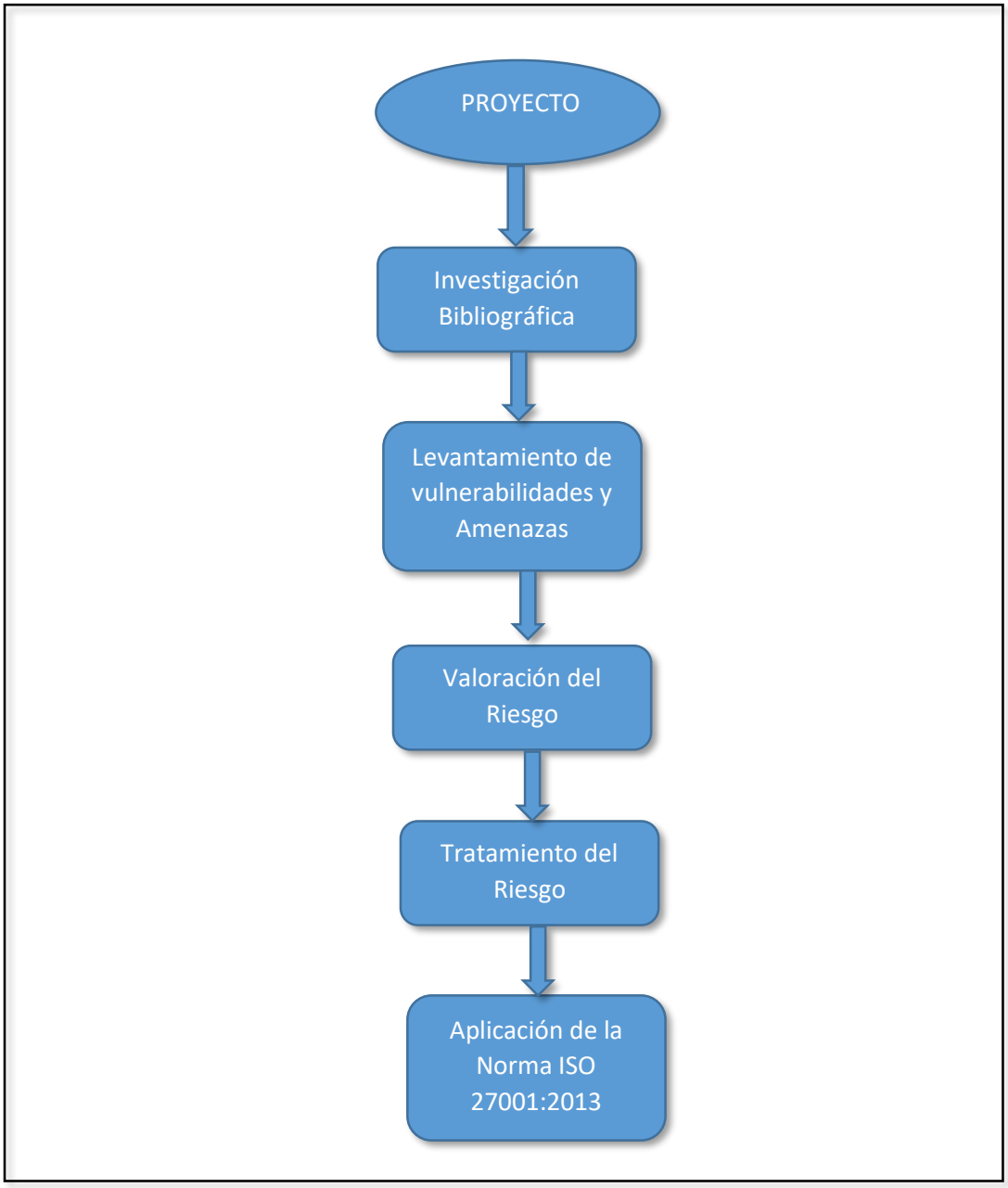
Como se mencionó en la Tabla 1., se ha levantado una bibliografía de algunos documentos como papers, tesis y artículos que permitan poder tener el recurso suficiente para poder plantear lo que se busca en este documento; tomando en cuenta que una investigación bibliográfica puede definirse como «*cualquier investigación que requiera la recopilación de información a partir de materiales publicados*». (Arteaga, 2020)

En tal virtud con la bibliografía disponible y previamente enunciada se ha procedido a levantar definiciones iniciales, y un conjunto de posibles amenazas o vulnerabilidades sobre las tecnologías de Lorawan, de esta manera se empieza con el análisis de las mismas por medio de la Norma ISO 27001:2013, se valora su riesgo y tomando en cuenta esos valores se procede a darles tratamiento aplicando los Técnicas de Control y Controles para mitigar al máximo las posibles afectaciones.

Para todo este trabajo se utilizará la investigación descriptiva misma que se enfoca en el análisis frecuente de los datos que se han recolectado por medio de la aplicación de varios instrumentos investigativos, al igual que la aplicación de herramientas completamente

necesarias para el análisis de la información, se utilizarán también herramientas como matrices que ayudarán al mejor entendimiento y aplicabilidad de la propuesta. (Taylor & Bogdan, 2012)

Figura 2.
Esquema del desarrollo del trabajo



Fuente: Elaboración propia (2023)

1.4 Análisis de resultados

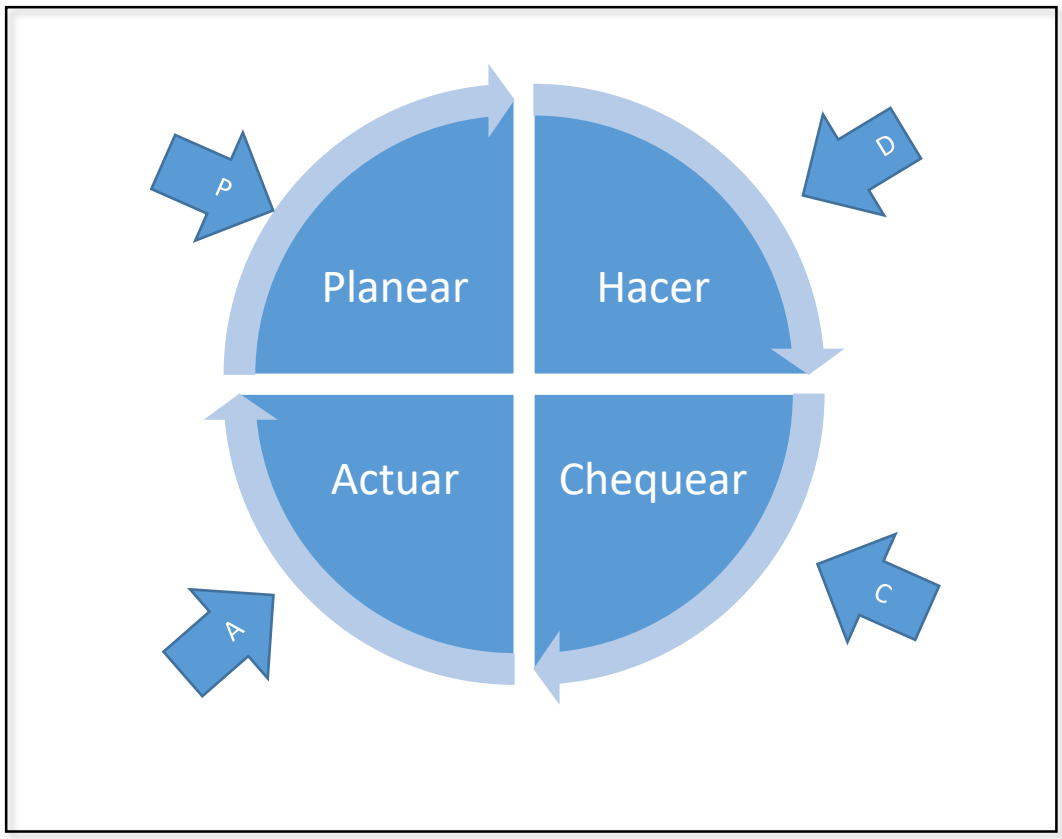
Siguiendo el procedimiento establecido en la Figura 2. Se pretende obtener un conjunto de las posibles vulnerabilidades que pueden afectar la seguridad de la información en los dispositivos de *«IoT»* que trabajen o utilicen las redes Lorawan.

Una vez con esos datos se los debe valorar y para ello se ha escogido el método de la valoración del riesgo en el sentido de que el riesgo es el producto lineal entre la probabilidad y el impacto, que a su vez se puede definir como el producto entre el nivel de riesgo y el costo, una vez obtenida esa valoración se procederá con el respectivo tratamiento a los riesgos sobre la premisa de aceptar, mitigar, transferir, evitar el riesgo; por lo que la *«Norma Internacional ISO 27001:2013»* nos dirá que objetivo de control y controles nos permitirá tratarlos. (Uribe Castro, 2021)

Con todo lo indicado en los numerales anteriores, es importante manifestar que el procedimiento a ser realizado y los posibles resultados que se desean obtener se basa en el Ciclo de Deming el cual nos indica que a un proyecto como el presente se lo puede absorber de una manera cíclica siguiendo cada uno de los siguientes procesos. (Marínez Pérez, 2021)

Figura 3.

Ciclo de Deming



Fuente: Elaboración propia (2023)

CAPÍTULO II: PROPUESTA

En este capítulo se enunciará el componente teórico que será la base para el desarrollo como tal de la propuesta y se trabajará con las matrices de análisis de riesgos y de Técnicas de Control y Controles de la Norma ISO 27001:2013 que serán parte de los apéndices de este documento, obteniendo así tablas que nos indicarán que hacer en caso de encontrarnos con cierto tipo de vulnerabilidad o amenaza en las tecnologías de *«IoT»* que utilizan las redes Lorawan

2.1 Fundamentos teóricos aplicados

En este apartado se presenta un resumen de las definiciones de Seguridad de la Información, generalidades del Internet de las cosas, redes de área amplia de baja potencia, análisis de riesgos y su tratamiento; así como la aplicación de Técnicas de Control y Controles de la Norma ISO 27001:2013.

2.1.1 Definición y necesidad de la seguridad de la información.

La información en la actualidad puede presentarse en varias formas y formatos a nivel empresarial o industrial es así que después del personal humano es el mayor de los activos; por consiguiente, esta definición llama a colación a cualquier técnica utilizada para proteger datos almacenados en los diferentes dispositivos de procesamiento, cómputo o de almacenamiento contra el acceso de personas o dispositivos no autorizados. Siendo esto posible por medio de la no alteración de la Confidencialidad, Integridad, y Disponibilidad de la información, así como de los sistemas implicados en su proceso, a nivel personal, dentro de una empresa o industria. (ISO 27001, 2021)

Es preciso mencionar que la seguridad «TOTAL» no existe, en virtud del constante crecimiento y aparecimiento de nuevas maneras de amenazas, riesgos, y vulnerabilidades por lo que se busca a toda costa es reducir todos estos riesgos y amenazas a un nivel «ACEPTABLE»; haciendo de estas técnicas un proceso que debe ser mejorado continuamente. (ISO 27001, 2020).

Retos de la seguridad.

Según (ISO 27001, 2021), se tienen entre los siguientes a los retos de la seguridad.

2.1.2 Confidencialidad.

Resguardo de la debida confidencialidad de los datos o paquetes de datos, para garantizar la confidencialidad de la información nadie no autorizado deberá tener acceso a la misma.

2.1.3 Integridad.

Garantizar que nadie podrá modificar el paquete de datos o datos a ser transmitidos o almacenados consiste en garantizar la integridad de la información.

2.1.4 Disponibilidad.

Garantizar el acceso universal de los datos a las personas o entidades autorizadas se define como cumplir con la disponibilidad de la información.

2.1.5 Autenticación.

La posibilidad de determinar la procedencia de un dato o conjunto de datos hará que se cumpla con la autenticación de la información.

2.1.6 No repudio.

Garantizar que entre emisor y receptor existe la transmisión de un mensaje indicará el no repudio a la misma.

2.2 Vulnerabilidad, amenaza, riesgo y ataques.

2.2.1 Vulnerabilidad.

Es la capacidad de aceptar o absorber incidencias externas de manera negativa pudiéndose transformar en un ataque potencial.

2.2.2 Amenaza.

Es una acción del tipo maligno que puede nacer a nivel interno o externo de una entidad pudiendo cualquiera de las dos ser fatales para garantizar la seguridad de la información, para definir una amenaza es necesario conocer ¿cuáles son sus objetivos?, ¿cuáles son sus agentes? y ¿qué tipo de evento puede ocasionar o producir?

2.2.3 Riesgo.

El riesgo se lo define como el producto de la probabilidad de ocurrencia por el impacto que puede ocasionarse, también tomando en cuenta que el producto anterior se lo conoce como Nivel de Riesgo; se puede decir que el riesgo se define como el producto del nivel del riesgo por el costo del daño.

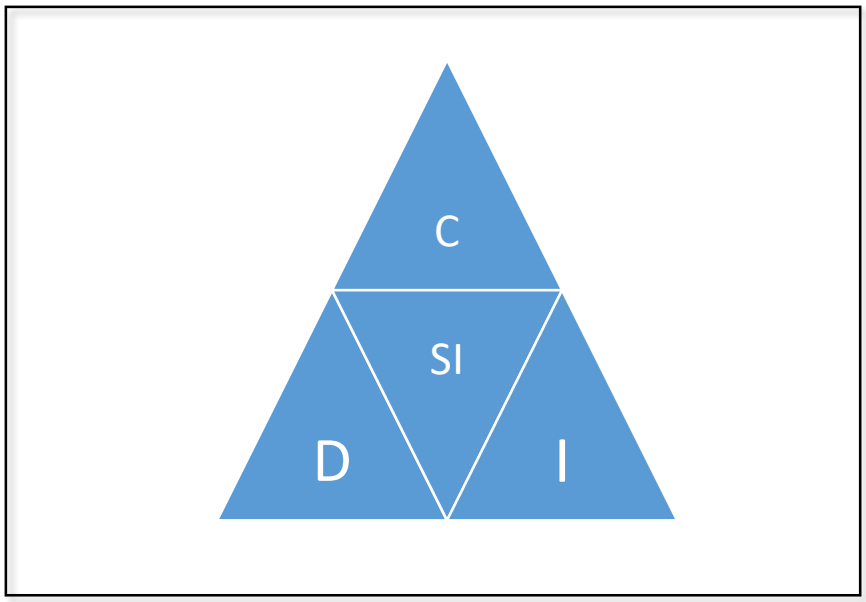
2.2.4 Ataque.

Es definido como la culminación de la ejecución de varias amenazas y vulnerabilidades efectuadas sobre un sistema informático, industrial o una red industrial o empresarial.

Es necesario mencionar que los atacantes lo que desean es hacer daño, acceder a información relevante o importante, y de alguna manera tratar de lucrar de ella para convertir este tipo de ataques en un medio de vida por cobrar al recuperar la información o subsanar un ataque.

Figura 4.

La Triada CID



Fuente: Elaboración propia (2023)

2.3 Norma Internacional ISO 2700

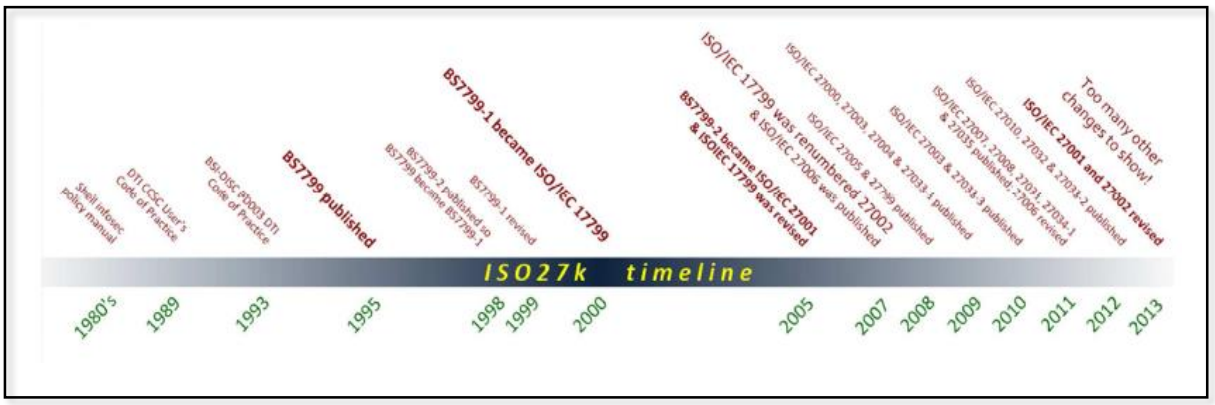
La Norma Internacional ISO proviene de la constitución de una familia de estándares, desarrollados por la Organización Internacional de Estandarización de sus siglas en inglés (ISO) y por Comisión Electrotécnica Internacional de sus siglas en inglés, (IEC) que son generalmente conocidas como las normas ISO 27000.

Esta familia de estándares fue desarrollada y publicada conforme la necesidad de contar con un procedimiento o proceso que permita establecer, implementar, controlar, mantener, e innovar u Sistema de Gestión de la Seguridad. (ISO 27001, 2021)

2.3.1 Evolución de la norma ISO 27000.

Las normas ISO tienen una constante evolución con el transcurso del tiempo para ello en la figura 5. se hace referencia a este proceso evolutivo, donde se puede apreciar que la norma tiene sus inicios en los años 80 donde toma el nombre de BS7799 y para el año 2005 es cuando empieza a ser denominada como la norma ISO 27001:2005, y finalmente en la actualidad se encuentra vigente le versión 2013; sin embargo, existe ya una norma más actualizada la cual se enfoca a controles sobre la nube la cual es la versión 27001:2022.

Figura 5.
Evolución de la Norma ISO 27001



Fuente: (martínez - Santander, 2018)

2.4 Generalidades del Internet de las cosas.

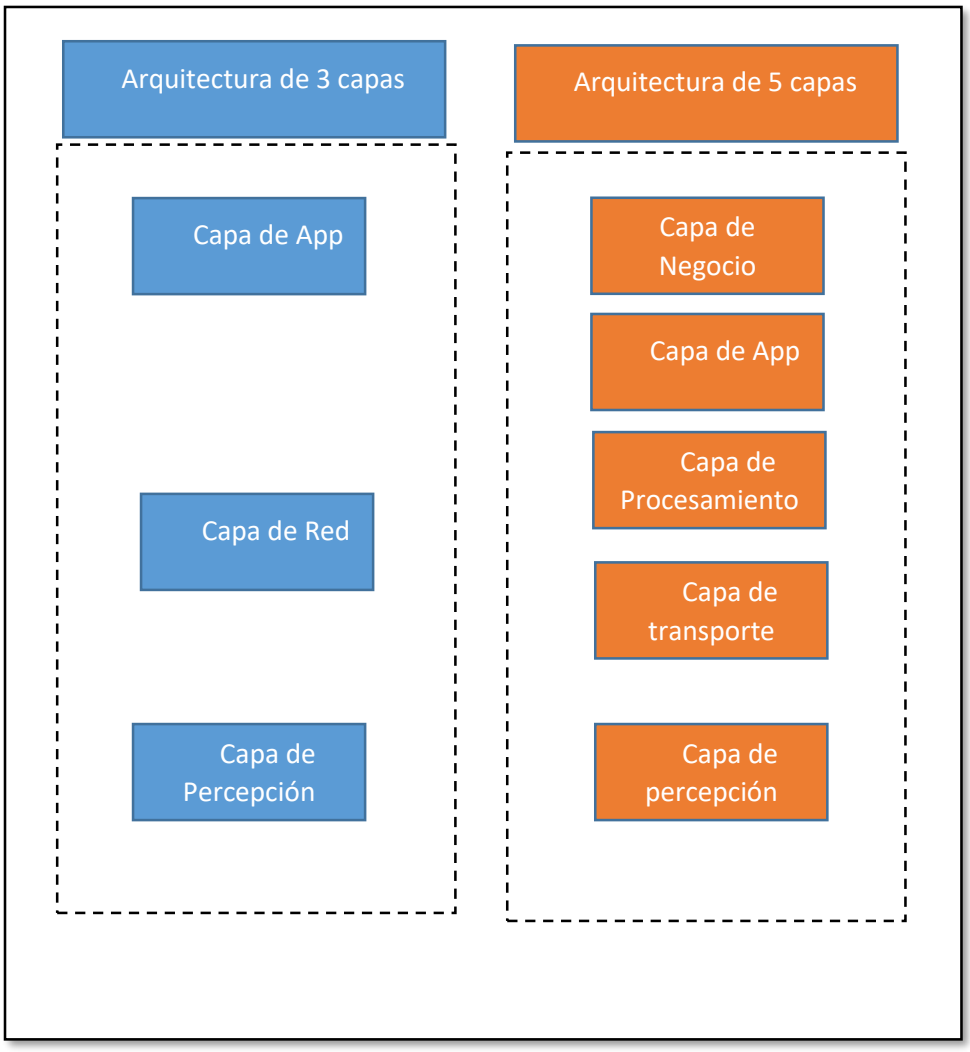
Hoy en día el uso del Internet es indispensable en cualquier campo de la vida, es decir es esencial para el día a día cotidiano; así como el día de producción de una planta industrial, el levantamiento de mediciones a distancia por medio de sensores, la comunicación esencial (niveles de estados), etc. Esto conlleva a pensar que la <<Internet está en todo»; por lo que al ser esto una verdad se da origen a la definición del Internet de las cosas como: «El Internet de las Cosas es la interconexión a través del Internet de dispositivos informáticos o electrónicos integrados en objetos cotidianos, lo que los permite enviar y recibir datos.», de igual manera se puede describir que es todo dispositivo al que se le puede asignar una dirección IP. (Uribe Castro, 2021)

En consecuencia, el uso de la *«IoT»* es una realidad, sin embargo, en unos años se cree que la conexión de estos dispositivos se dé a través de cualquier objeto que una persona se imagine desde los más cotidianos o de uso doméstico hasta autos o las llamadas casa artificiales que, aunque el día de hoy ya existen pueden ser mejoradas y desarrolladas a puntos inimaginables pues el objetivo es generar una conexión llamada machine to machine (M2M) o dispositivos M2M. Las proyecciones del impacto de la *«IoT»* sobre Internet y la economía son impresionantes, donde se pronostica que hasta en el año 2025 habrá hasta cien mil millones de dispositivos conectados a la *«IoT».* (Uribe Castro, 2021)

El *«IoT»* es aún un paradigma que está en constante evolución, en la actualidad no existe una arquitectura definida para *«IoT»,* ya que su estructura depende exclusivamente de la

aplicación en la que se quiere implementar. Sin embargo, existen varias recomendaciones de su Arquitectura, *«IoT»* cual se aprecia en la figura siguiente:

Figura 6.
Arquitectura de «IoT»



Fuente elaboración propia (2023)

2.4.1 Aplicaciones de «IoT».

Son varias las aplicaciones que pueden resultar difícil identificar a todas, sin embargo, se colocará algunos ejemplos que permitirán visualizar como estas se han incluido en el diario vivir de las personas sobre todo en su cotidianidad, en lo laboral, financiero, y también en la vida empresarial o industrial.

Tabla 2.
Aplicaciones de **«**IOT»

Área	Aplicaciones
Agricultura y Ganadería	Sensores de temperatura, humedad, toxicidad para siembras, cosechas, ordeño, o fertilizaciones.
Domótica	Casas y edificios inteligentes, conexiones a dispositivos como «Alexa»
Inteligencia Artificial	Sensores que permiten reproducir un patrón una vez aprendido por la máquina
Big Data	Procesos automatizados continuos de ETL
Control y Monitoreo	Sensores electrónicos de diferente tipo que permiten validar varios parámetros
Ciudades Inteligentes	Transito inteligente, sensores de redes de dispositivos (pozos)

Fuente: Elaboración propia (2023)

2.5 Tecnologías o Redes de «IOT».

2.5.1 Redes de corto alcance y bajo consumo.

Las tecnologías inalámbricas hoy en día son muy usadas en varias actividades de nuestra cotidianidad, es por ello que se han definido y diseñado varias redes de corto alcance y baja potencia y que suelen ser más utilizadas en hogares, oficinas o en lugares pequeños y cerrados debido a que su consumo es mucho más económico y el ancho de su banda de igual forma se ajusta a estos espacios, varias de estas tecnologías suelen necesitar baterías o cables que los recarguen, a continuación, se detallan alguna de ellas: (Manrique, Buitrago, Hernández, 2019).

Tabla 3

Tecnologías inalámbricas de corto alcance

Tecnología
Bluetooth
Zigbee
NFC
Wifi / 802.11 a,b,g,e
Wabe

Fuente: Elaboración propia (2023)

2.5.2 Redes de área extensa de bajo consumo («LPWAN»)

Representa una clara evolución de las redes de comunicación orientadas hacia los dispositivos *«IoT»*. Estas redes fueron diseñadas para interconectar una gran cantidad de dispositivos, con un alcance superior a las tecnologías convencionales denominadas redes de área personal que fueron mencionadas en el numeral anterior, usando la menor cantidad de recursos, pero sacrificando la velocidad de transmisión, lo que las hacia ideales para nueva tendencia de interconectar sensores y dispositivos de baja velocidad separados a distancias de área extendida, pero ineficaces para transmisión de voz, audio y video. (Rivera Vera, 2021)

Entre las redes *«LPWAN»* se tienen las siguientes que se detallan en la tabla 4.; sin embargo, se dará énfasis solamente aquellas que son parte de este estudio y que son realmente definidas para el desarrollo y aplicación de *«IoT»*. (Rivera Vera, 2021)

Tabla 4.

Tecnologías «LPWAN»

Tecnología «LPWAN»
GSM
LTE para «IoT»
5G para «IoT»
Cat-0
Cat-1
LoraWan
LTE Cat-M1
Banda Estrecha o NB – «IoT» / CAT-M2
«Sigfox»

Fuente: Elaboración propia (2023)

2.5.2.1 «Sigfox»

«Sigfox» ofrece redes inalámbricas que emiten datos continuamente de una forma más dinámica y la exponen amigablemente al usuario, «Sigfox» es una tecnología propietaria de la empresa que lleva su propio nombre y está basada en una modulación diferencial DBPSK para subida hacia la plataforma y una modulación GFSK para la descarga de datos. En ambas direcciones trabaja sobre la tecnología de comunicación «Ultra Narrow Band» (UNB) transmitiendo sobre las bandas de frecuencias de sub-GHz libres. (Hernádez, 2019)

Los paquetes que transmite son de un tamaño reducido, componiéndose por una parte fija de 12 bytes que incluye un preámbulo, un identificador del dispositivo y otros metadatos, y por la

parte variable formada por la información, siendo esta de hasta 12 bytes; por lo que el el paquete a trasmitirse puede variar entre 12 y 24 bytes más unos bytes extras usados para autenticación.

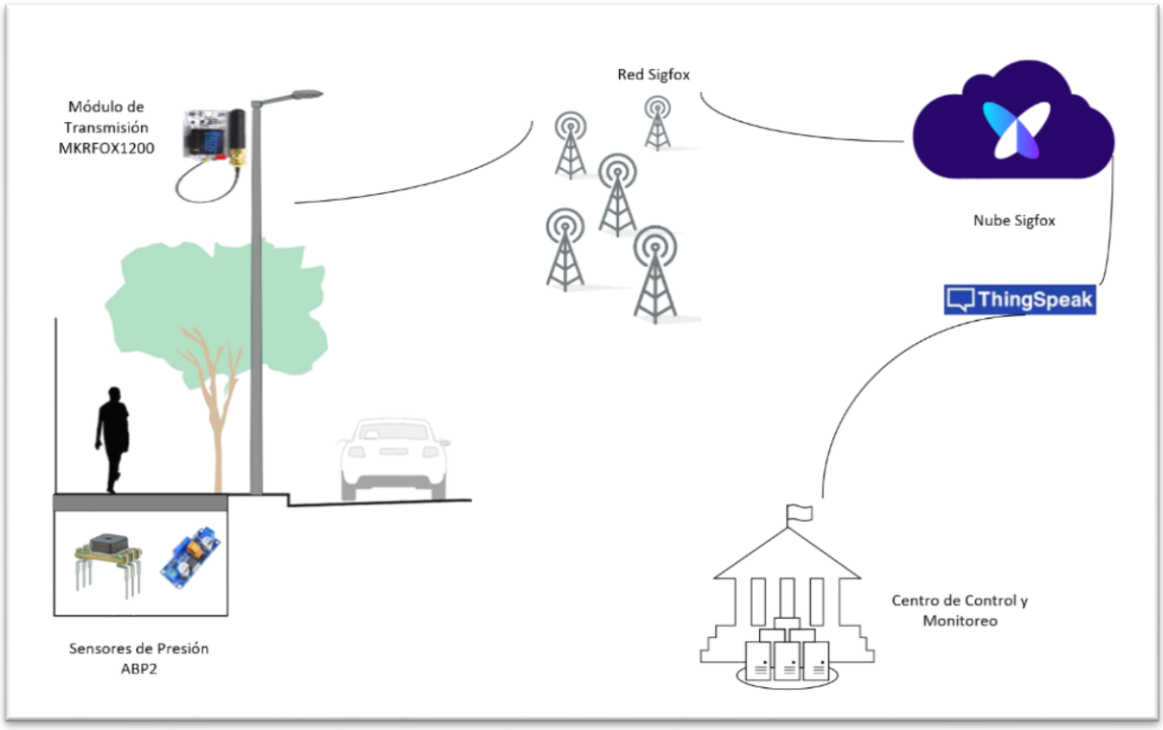
«Sigfox» funciona a partir de dispositivos «IoT» fabricados con chips específicos admitidos por la red, estos envían la información por medio de estaciones base (BTS), en esta plataforma se puede configurar diferentes servicios de mensajería en sistemas cloud como: AWS «IoT», IBM Watson y Microsoft Azure. (Uribe Castro, 2021)

Una característica a tener en cuenta es que «Sigfox» es eficaz para las comunicaciones desde los puntos finales a las estaciones base, con una velocidad de 100 bps, pero no es particularmente eficaz en transmisiones desde las estaciones base hasta los puntos finales. Las descargas son más lentas que la subida de información. (Uribe Castro, 2021)

«Sigfox», tiene un alcance de 1 a 5 km en zonas urbanas y en zonas rurales puede alcanzar de 10 a 40 km debido a que el desvanecimiento por multitrayectoria y multipropagación disminuye en el campo traviesa por la no presencia de obstáculos; no obstante, «Sigfox» emplea el ancho de banda de manera eficiente y experimenta niveles de ruido muy bajos, lo que resulta en una alta sensibilidad del receptor y un consumo de energía ultra bajo. (Pérez, 2018)

Esta tecnología utiliza las frecuencias de las denominadas bandas libres del espectro electromagnético o también conocidas como las bandas (ISM) de sus siglas en inglés de industrial, científico y médico, en el Ecuador la Agencia de Regulación y Control de las telecomunicaciones permite su uso y despliegue en las bandas de 900 MHz. (https://www.arcotel.gob.ec)

Figura 7.
Arquitectura de una red «Sigfox»



Fuente: Elaboración propia (2023)

En la tabla siguiente se muestra algunas características de la tecnología «Sigfox»

Tabla 5.

Características Técnicas de «Sigfox»

CARACTERÍSTICAS	VALORES
Modulación	BPSK
Frecuencia	915 MHz
Ancho de banda	100 Hz
Velocidad de datos Downlink	100 – 600 bps
Velocidad de datos (Uplink	100
Máximos mensajes al día	140 msg/día UL 4msg/día DL /
Distancia	40 km (rural) / 10 km (urbano)
Carga útil	12 bytes UL/ 8 bytes DL
Rango de latencia	< 20 segundos

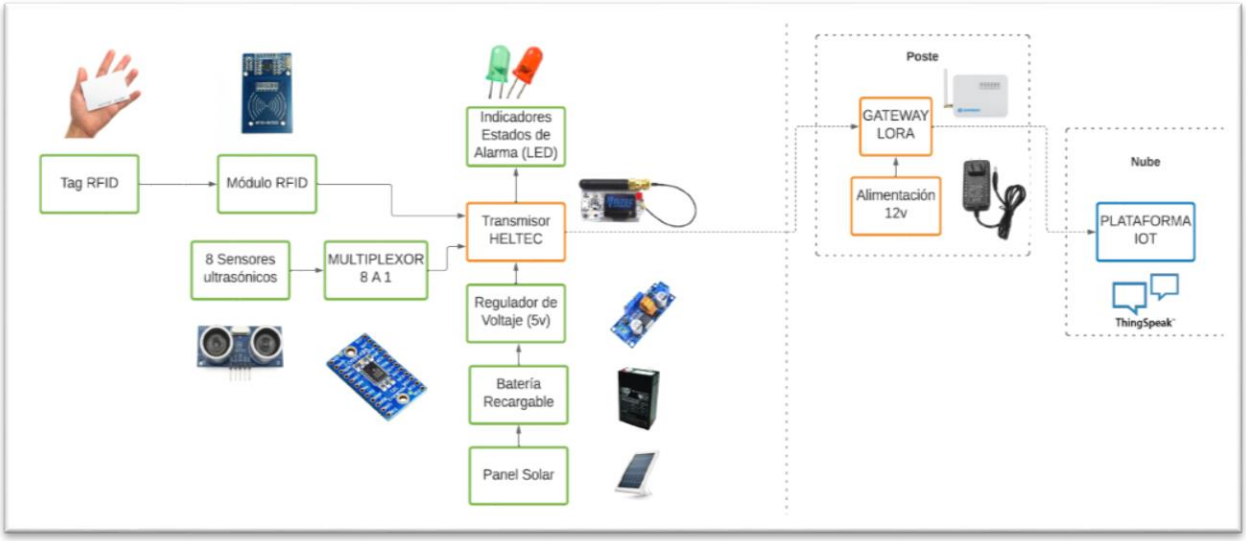
Fuente. Cueva R, (2021), se respeta derechos del autor

2.5.2.2 Redes Lorawan

Esta tecnología ha sido ya previamente definida a lo largo de este documento, como se lo ha mencionado es una tecnología que aún se encuentra en desarrollo, lo que la conlleva a no tener una gran cantidad de bibliografía certificada; sin embargo, en el estricto análisis de una red inalámbrica esta tiene varias certezas que, si son comprobables y que la definen como tal, entre ellas tenemos su modulación, sus frecuencias de uso, su alcance entre otras.

En la figura siguiente se muestra una topología de red Lorawan para la aplicación de la medición de un sensor de presión, este diseño fue parte de un proyecto de ciudades inteligentes presentado por el DMDQ en el año 2021, es importante indicar que se puede hacer un símil a lo que sucede con otros tipos de tecnologías por ejemplo se puede realizar la analogía que «Sigfox» es el producto licenciado como Windows; mientras que Lorawan es el producto de desarrollo libre como Linux.

Figura 8.
Arquitectura de una Red Lorawan



Fuente: Elaboración propia (2023).

2.6 Análisis de Vulnerabilidades de seguridad entre las dos tecnologías

Para el desarrollo de este numeral se ha realizado una investigación bibliográfica en varios documentos, de donde se ha procurado extraer las posibles vulnerabilidades y amenazas que este tipo de tecnologías y comunicaciones sufren por su diseño y poca robustez en ciertos parámetros de configuración.

En la tabla 6., se enlista cada uno de ellos, entendiéndose que, de ninguna manera serán todos, más, lo que se busca es definirlos; evaluarlos como riesgo y mitigarlos por medio de los Técnicas de Control y Controles de la Norma ISO 27001.

Tabla 6.
Vulnerabilidades y Amenazas

Vulnerabilidad o Amenaza	Descripción
Seguridad en capa de percepción	Esta capa realiza la recopilación de los objetos por medio de sensores como RFID, emitiendo o identificándolos con etiquetas, por lo que son susceptibles a ser clonadas o a realizar spoofing emitiendo información falsa o haciéndose pasar por otra fuente diferente a la original.
Seguridad en la Comunicación	Transmisión y Recepción de datos inseguros, no son codificados o encriptados por el poco ancho de banda que presentan estas tecnologías, lo que hace que los bits se transmitan en forma serial sin ninguna seguridad, al usar bandas libres son muy susceptibles a ser inhibidos por equipos inhibidores de señal lo que puede degradar o terminar por completo con la comunicación.
Seguridad en la Gestión de Datos / Transferencia y almacenamiento de datos inseguros	Estos dispositivos pueden tener una configuración predeterminada insegura, lo que los hace de fácil acceso a ellos y por consiguiente se puede tener acceso a los datos que manejan, de igual manera al pensar que no existe una data muy grande y vulnerable las contraseñas de acceso son débiles y ni que pensar de un factor de doble autenticación.
Seguridad en Capa de Red	Autenticación y Autorización Mutua que por lo general no existe, Interfaces inseguras ya que al ser dispositivos electrónicos que de un cierto modo no se los ve como un componente importante de una red sus interfaces son de libre acceso y por lo general no tienen ningún equipo

Vulnerabilidad o Amenaza	Descripción
	de seguridad perimetral y por lo general son puertas generalmente abiertas. De igual manera existen componentes obsoletos que también puede ser susceptibles a variaciones de voltaje o corriente haciendo que el dispositivo funcione de mala manera. Dentro de los ataques que pueden tener estos dispositivos con el ataque Sybil asignando diferentes identidades a un mismo nodo ocasionando información incorrecta. Ataque de privacidad de sueño es cuando mantiene encendidos los nodos agotando su batería y apagándolos. Inyección de código malicioso afectando el comportamiento de la red.
Seguridad en Capa de Nivel Medio	Integración de la Seguridad en todas sus capas los ataques que se pueden dar en esta capa son el de acceso no autorizado y la denegación de Servicios.
Seguridad en Capa de Aplicación	Falta de Actualización, por lo general estos dispositivos no actualizan su firmware por lo que no son actualizados casi nunca, de igual manera en esta capa es prudente realizar una Auditoria de la Seguridad al ser la capa más alta se lo puede hacer con aplicaciones externas.
Endurecimiento de Software y Hardware	Todo dispositivo que contenga software aunque sea del tipo embebido y hardware debe tener un plan de endurecimiento básico que por lo menos comprenda solventar todos los posibles problemas definidos en los campos de la tabla anteriormente citados.

Fuente: Elaboración propia (2023) se respeta los derechos de autor:

(Modelo de seguridad «IOT» Monzon, Todt, Bollatti, 2020)

(Gestión de Riesgos en el Internet de las Cosas, Gantiva, 2020)

(Análisis del Nivel de Seguridad presente en los dispositivos que componen el «IoT», Uribe, 2019)

2.6.1 Valoración de Riesgos

Una vez que se ha levantado algunos de los problemas de seguridad que las redes «LPWAN» pueden sufrir en su funcionamiento y configuración, se ha definido en el procedimiento establecido que cada uno sea caracterizado como un riesgo y valorado bajo la premisa previamente establecida de que el Riesgo es el producto de la Probabilidad de ocurrencia por el impacto que esta pueda dejar u ocasionar.

En tal sentido en la tabla siguiente se muestra esta valoración tomando en cuenta los rangos de 1 a 5 entre la probabilidad por el impacto; esto dará un valor máximo de 25 lo que se conoce como el Nivel de Riesgo; si se multiplica el Nivel de Riesgo por el costo que también puede ser definido en un rango de 1 a 5 tendremos el Riesgo como tal con valores entre 1 y 100 dándose a criterio del autor los rangos de bajo, medio, medio alto y alto cada 25 unidades.

Con estos valores se trata el riesgo definiendo que todo valor menor a 25 unidades en el riesgo este podrá ser asumido, mientras que para todo valor mayor a 25 unidades en el riesgo se deberán aplicar controles, es decir se lo debe transferir, mitigar o evitar mas no aceptar.

Tabla 7.

Valoración del Riesgo y Acciones a tomar

IDENTIFICACIÓN		VALORACIÓN DEL RIESGO						
Vulnerabilidad o Amenaza	**Descripción / Afectación**	**Impacto**	**PBBD**	**IMPAC**	**NR**	**COS**	**RIESGO**	**ACCION A TOMAR**
Seguridad en capa de percepción	Esta capa realiza la recopilación de los objetos por medio de sensores como RFID, emitiendo o identificándolos con etiquetas, por lo que son susceptibles a ser clonadas o a realizar spoofing emitiendo información falsa o haciéndose pasar por otra fuente diferente a la original.	Medio Alto	3	4	12	3	36	Aplicar Controles
Seguridad en la Comunicación	Transmisión y Recepción de datos inseguros, no son codificados o encriptados por el poco ancho de banda que presentan estas tecnologías, lo que hace que los bits se transmitan en forma serial sin ninguna seguridad, al usar bandas libres son muy susceptibles a ser inhibidos por equipos inhibidores de señal lo que puede degradar o terminar por completo con la comunicación.	Alto	4	5	20	4	80	Aplicar Controles
Seguridad en la Gestión de Datos / Transferencia y almacenamiento de datos inseguros	Estos dispositivos pueden tener una configuración predeterminada insegura, lo que los hace de fácil acceso a ellos y por consiguiente se puede tener acceso a los datos que manejan, de igual manera al pensar que no existe una data muy grande y vulnerable las contraseñas de acceso son débiles y ni que pensar de un factor de doble autenticación.	Alto	4	5	20	4	80	Aplicar Controles

IDENTIFICACIÓN		VALORACIÓN DEL RIESGO						
Vulnerabilidad o Amenaza	**Descripción / Afectación**	**Impacto**	**PBBD**	**IMPAC**	**NR**	**COS**	**RIESGO**	**ACCION A TOMAR**
Seguridad en Capa de Red	Autenticación y Autorización Mutua que por lo general no existe, Interfaces inseguras ya que al ser dispositivos electrónicos que de un cierto modo no se los ve como un componente importante de una red sus interfaces son de libre acceso y por lo general no tienen ningún equipo de seguridad perimetral y por lo general son puertas generalmente abiertas. De igual manera existen componentes obsoletos que también puede ser susceptibles a variaciones de voltaje o corriente haciendo que el dispositivo funcione de mala manera. Dentro de los ataques que pueden tener estos dispositivos con el ataque Sybil asignando diferentes identidades a un mismo nodo ocasionando información incorrecta. Ataque de privacidad de sueño es cuando mantiene encendidos los nodos agotando su batería y apagándolos. Inyección de código malicioso afectando el comportamiento de la red.	Alto	5	5	25	4	100	Aplicar Controles
Seguridad en Capa de Nivel Medio	Integración de la Seguridad en todas sus capas los ataques que se pueden dar en esta capa son el de acceso no autorizado y la denegación de Servicios.	Medio Alto	3	4	12	4	48	Aplicar Controles

IDENTIFICACIÓN		VALORACIÓN DEL RIESGO						
Vulnerabilidad o Amenaza	**Descripción / Afectación**	**Impacto**	**PBBD**	**IMPAC**	**NR**	**COS**	**RIESGO**	**ACCION A TOMAR**
Seguridad en Capa de Aplicación	Falta de Actualización, por lo general estos dispositivos no actualizan su firmware por lo que no son actualizados casi nunca, de igual manera en esta capa es prudente realizar una Auditoria de la Seguridad al ser la capa más alta se lo puede hacer con aplicaciones externas.	Medio Alto	4	4	16	4	64	Aplicar Controles
Endurecimiento de Software y Hardware	Todo dispositivo que contenga software aunque sea del tipo embebido y hardware debe tener un plan de endurecimiento básico que por lo menos comprenda solventar todos los posibles problemas definidos en los campos de la tabla anteriormente citados.	Medio Alto	3	4	12	3	36	Aplicar Controles

Fuente: Elaboración propia (2023)

2.7 La Norma ISO 27001 y la aplicación de controles.

Para el desarrollo de este numeral de acuerdo con el procedimiento establecido nos enfocaremos en el Anexo A de la Norma ISO / IEC27002:2013 la misma que nos presenta un conjunto de 14 dominios, 35 técnicas de control, y 114 controles, los cuales serán asignados y escogidos para mitigar las vulnerabilidades y amenazas encontradas para las tecnologías de «IoT» en estudio.

En la tabla 8. Se verificará esta acción siendo la propuesta como tal de este trabajo propuesto.

Tabla 8.

Aplicación de Técnicas de Control y Controles de la Norma ISO 27001:2013

SELECCIÓN DE TÉCNICAS DE CONTROL Y CONTROLES							
AMENAZAS HUMANAS	**AFECTACIÓN**	**ACCIÓN A TOMAR**	**DOMINIOS**	**TÉCNICAS DE CONTROL**		**CONTROL**	
Seguridad en capa de percepción	Clonación Spoofing	Aplicar Controles	9. Control de Accesos	9.4	Control de acceso a sistemas y aplicaciones	9.4.1	Restricción de acceso a la información
						9.4.3	Gestión de Contraseñas de Usuario
			10. cifrado	10.1	Controles Criptográficos	10.1.1	Política de uso de los controles criptográficos
						10.1.2	Gestión de Claves
			11. Seguridad Física y Ambiental	11.1	Áreas Seguras	11.1.2	Controles físicos de entrada
				11.2	Seguridad de los Equipos	11.2.4	Mantenimiento de los Equipos
Seguridad en la Comunicación	No Codificación No Encriptación Interferencia Atenuación		9. Control de Accesos	9.2	Gestión de Acceso a Usuario	9.2.2	Gestión de los derechos de acceso
				9.4	Control de acceso a sistemas y aplicaciones	9.4.1	Restricción de acceso a la información
						9.4.3	Gestión de Contraseñas de Usuario
			10 Cifrado	10.1	Controles Criptográficos	10.1.1	Política de uso de los controles criptográficos

SELECCIÓN DE TÉCNICAS DE CONTROL Y CONTROLES							
AMENAZAS HUMANAS	**AFECTACIÓN**	**ACCIÓN A TOMAR**	**DOMINIOS**	**TÉCNICAS DE CONTROL**		**CONTROL**	
Seguridad en la Gestión de Datos / Transferencia y almacenamiento de datos inseguros	Acceso a datos Configuración Inicial Contraseñas poco seguras		13. Seguridad en la Telecomunicaciones	13.1	Gestión de la seguridad en las redes	10.1.2	Gestión de Claves
						13.1.1	Controles de red
				13.2	Intercambio de Información con partes externas	13.2.4	Acuerdos de confidencialidad y secreto
						13.2.1	Política y procedimientos de intercambio de información
			9. Control de Accesos	9.2	Gestión de Acceso a Usuario	9.2.2	Gestión de los derechos de acceso
				9.4	Control de acceso a sistemas y aplicaciones	9.4.1	Restricción de acceso a la información
						9.4.3	Gestión de Contraseñas de Usuario
			10 Cifrado	10.1	Controles Criptográficos	10.1.1	Política de uso de los controles criptográficos
						10.1.2	Gestión de Claves
Seguridad en Capa de Red	No Autenticación Interfaces		12. Seguridad en la Operativa	12.1	Responsabilidades y procedimientos de operación	12.1.3	Gestión de capacidades

SELECCIÓN DE TÉCNICAS DE CONTROL Y CONTROLES							
AMENAZAS HUMANAS	**AFECTACIÓN**	**ACCIÓN A TOMAR**	**DOMINIOS**	**TÉCNICAS DE CONTROL**		**CONTROL**	
Seguridad en Capa de Nivel Medio	Inseguras Spoofing Man in the Middle Dont Sleep inyección de Código No Autenticación Denegación de Servicios		13. Seguridad en la Telecomunicaciones	12.2	Protección contra código malicioso	12.2.1	Controles contra código malicioso
				13.1	Gestión de la seguridad en las redes	13.1.1	Controles de Red
						13.1.2	Mecanismos de seguridad asociados a servicios en red
						13.1.3	Segregación de redes
			9. Control de Accesos	9.2	Gestión de Acceso a Usuario	9.2.2	Gestión de los derechos de acceso
				9.4	Control de acceso a sistemas y aplicaciones	9.4.1	Restricción de acceso a la información
						9.4.3	Gestión de Contraseñas de Usuario
			10 Cifrado	10.1	Controles Criptográficos	10.1.1	Política de uso de los controles criptográficos
						10.1.2	Gestión de Claves
			11. Seguridad Física y Ambiental	11.2	Seguridad de los equipos	11.2.4	Mantenimiento de los equipos

SELECCIÓN DE TÉCNICAS DE CONTROL Y CONTROLES							
AMENAZAS HUMANAS	**AFECTACIÓN**	**ACCIÓN A TOMAR**	**DOMINIOS**	**TÉCNICAS DE CONTROL**		**CONTROL**	
			12. Seguridad en la Operativa	12.1	Responsabilidades y procedimientos de operación	12.1.2	Gestión de Cambios
						12.1.3	Gestión de capacidades
Seguridad en Capa de Aplicación	Falta de Upgrades Falta de Auditoría		12. Seguridad en la Operativa	12.1	Responsabilidades y procedimientos de operación	12.1.1	Documentación de procedimientos de operación
						12.1.2	Gestión de Cambios
						12.1.3	Gestión de capacidades
				12.2	Protección contra código malicioso	12.2.1	Controles contra el código malicioso
				12.3	Copias de Seguridad	12.3.1	Copias de Seguridad
				12.6	Gestión de la Vulnerabilidad Técnica	12.6.1	Gestión de la vulnerabilidades técnicas
						12.6.2	Restricciones en la instalación de software
Endurecimiento de Software y Hardware	solventar Bugs Controlar Accesos Controlar hardware		9. Control de Accesos	9.2	Gestión de Acceso a Usuario	9.2.2	Gestión de los derechos de acceso
				9.4	Control de acceso a sistemas y aplicaciones	9.4.1	Restricción de acceso a la información

SELECCIÓN DE TÉCNICAS DE CONTROL Y CONTROLES							
AMENAZAS HUMANAS	**AFECTACIÓN**	**ACCIÓN A TOMAR**	**DOMINIOS**		**TÉCNICAS DE CONTROL**		**CONTROL**
						9.4.3	Gestión de Contraseñas de Usuario
			11. Seguridad Física y Ambiental	11.2	Seguridad de los equipos	11.2.4	Mantenimiento de los equipos
			12. Seguridad en la Operativa	12.6	Gestión de la Vulnerabilidad Técnica	12.6.1	Gestión de la vulnerabilidades técnicas
						12.6.2	Restricciones en la instalación de software

Fuente: Elaboración propia

2.8 Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 9.

Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Seguridad de la Información	Definición de Seguridad de la Información.	La metodología de investigación fue bibliográfica que permitió tener los conceptos detallados	Fuente bibliográfica	Sustenta conocimiento previos y necesarios para entender la propuesta	Texto, Figuras e Imágenes
Internet de las cosas	Definición de «IOT» Definición de redes Lorawan	La metodología de investigación fue bibliográfica que permitió tener los conceptos detallados	Fuente bibliográfica	Sustenta conocimiento previos y necesarios para entender la propuesta	Texto, Figuras e Imágenes

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Análisis de Riesgos con el levantamiento de Vulnerabilidades y Amenazas	Teoría sobre el análisis de riesgos cuando se lo evalúa como la probabilidad por el impacto	Aplicación del método de análisis y valoración del Riesgo	Fuente bibliográfica	Se genera Matriz y diagrama de calor con los valores del Riesgo	Matrices, asignación de reglas en Excel
Aplicación de la ISO 27001:2013	Teoría sobre el ciclo de Deming	Análisis del Apéndice A de la Norma ISO 27002 y selección de Técnicas de Control y controles	Fuente bibliográfica	Se genera matriz con los Técnicas de Control y Controles escogidos para mitigar las vulnerabilidades y amenazas levantadas	Matrices, asignación de reglas en Excel

Fuente: Elaboración propia (2023)

CONCLUSIONES

Se ha contextualizado los fundamentos teóricos sobre la Seguridad de la Información, Norma ISO 27001:2013, Internet de las cosas, Redes «LPWAN», análisis de riesgos y tratamiento a los mismos, integrando diferentes mundos en esta propuesta.

Se ha realizado la investigación de qué tipo de vulnerabilidades y amenazas pueden tener los dispositivos de «IoT» y las redes de comunicaciones «LPWAN», definiendo unas cuantas para que puedan ser analizadas y tratadas por medio de una valoración en su riesgo y aplicando los Técnicas de Control y Controlesde la Norma ISO 27001.

Se ha determinado las posibles vulnerabilidades y amenazas de las redes «LPWAN» en específico para las tecnologías de «Sigfox» y de Lorawan, evidenciándose que por su similitud en su arquitectura de red y de transmisión poseen las mismas capas y por lo tanto son susceptibles a las mismas amenazas y vulnerabilidades.

No se puede concluir que haya diferencia o una amenaza y vulnerabilidad única para cada una de las tecnologías en análisis ya que poseen la misma arquitectura, en tal virtud se las ha tratado como una sola y considerado que son afectadas por las mismas vulnerabilidades y amenazas.

La Norma ISO 27001 es una norma enfocada más a la creación de un Sistema de Gestión de Seguridad de la Información SGSI, por lo que no es de gran ayuda plantear sus Técnicas de Control y Controlescomo los mejores pasos a seguir para mitigar las vulnerabilidades y amenazas encontradas en las tecnologías analizadas.

Se puede dar por conclusión que la tendencia a la universalidad de las cosas y la transformación digital traerán consigo muchas nuevas formas de ataques y vulnerabilidades; sin embargo, se considera que de igual manera se procederá a desarrollar técnicas de mitigación para ellos.

Se concluye que se puede integrar a la Norma ISO 27001 cualquier tecnología que deba ser analizada para ser tratada de tener vulnerabilidades por medio de sus técnicas de control y controles.

RECOMENDACIONES

Se recomienda tener un conocimiento previo sobre seguridad informática, Internet de las cosas, telecomunicaciones y la norma ISO para poder obtener un claro entendimiento del trabajo propuesto.

Se recomienda enfatizar en los programas de pregrado y postgrado sobre el desarrollo de aplicaciones para «IoT», conocimientos de seguridad informática y de las formas de transmisión de los datos

Se recomienda utilizar métodos investigativos para el desarrollo de cualquier trabajo de titulación debido a que sus herramientas brindarán la facilidad en la obtención de resultados favorables para la investigación.

Se recomienda que este trabajo propuesto sea desarrollado para más vulnerabilidades y amenazas que puedan afectar a los dispositivos de «IoT».

Es recomendable establecer una norma similar a OWASP o ISO para estrictamente el tema de los componentes de «IoT».

Si bien es cierto para el análisis del riesgo existen varios métodos, es recomendable se identifique y domine al menos el utilizado en la propuesta, toda vez que de su valoración se puede también obtener su posible tratamiento.

Se recomienda integrar diversas tecnologías o ramas de la seguridad informática a una manera de prueba y ensayo para verificar si los controles diseñados para cierta tecnología se pueden acoplar a otras.

BIBLIOGRAFÍA

Everett, C. (2011). *Is ISO 27001 worth it?* Computer Fraud & Security, 2011(1), pp: 5–7. https://doi.org/10.1016/S1361-3723(11)70005-7

ISO27001. (septiembre 2020). Norma ISO 27001. https://normaiso27001.es/

Panel, (10 de enero 2021). *Software QA- ¿Cuáles son los tipos de pruebas software?* https://www.panel.es/software-qa-cuales-son-los-tipos-de-pruebas-software/

Redes Zone. (noviembre 2021). *LoRaWAN, la última amenaza para los dispositivos «IoT»* https://www.redeszone.net/noticias/seguridad/lorawan-amenaza-dispositivos-«IoT»/

Calva, et al. (2021). *Seguridad «IoT»: Principales amenazas en una taxonomía de activos*. HAMUT'AY, 7(3), pp. 51-59.

Computerworld. *(*30 de abril 2019*). Estas son las principales vulnerabilidades del «IoT», según el INCIBE* https://www.computerworld.es/seguridad/estas-son-las-principales-vulnerabilidades-del-«IoT»-segun-el-incibe

Díaz-Piraquive, F. N. (2020). Análisis a la utilización de protocolos de interconexión para internet de las cosas: Una revisión sistemática Manuel Andrés Ramírez Delgado. INVESTIGACIÓN FORMATIVA EN INGENIERÍA, 248.

Eterovic, J., Cipriano, M., & Nicolet, S. (2018). Análisis de Protocolos de Comunicaciones para Internet de las Cosas. XX Workshop de Investigadores en Ciencias de la Computación (WICC 2018, Universidad Nacional del Nordeste).

Hernández, B. A., & Ortiz Galeano, D. P. (2019). Análisis general del enfoque «IOT» en redes. Editorial Universitaria San Mateo.

Martínez Pérez, E. M., & López de Jiménez, R. E. (2021). Sistema telemático para el monitoreo y control de variables microambientales utilizando LoRaWAN en el marco de la e-agricultura: Propuesta para la Escuela Nacional de Agricultura, ENA. Revista Tecnológica; no. 14.

Martínez-Santander, C. J., & Cruz-Gavilánez, Y. de la N. (2018). Tendencias tecnológicas y desafíos de la seguridad informática. Polo del Conocimiento, 3(5), 260-279. https://doi.org/10.23857/pc.v3i5.640

Pérez, N. B., Bustos, M. A., Berón, M., & Rangel Henriques, P. (2018). Análisis sistemático de la seguridad en internet of things. XX Workshop de Investigadores en Ciencias de la Computación (WICC 2018, Universidad Nacional del Nordeste).

Rivera Vera, K. M., & Rocafuerte Mindiolaza, W. J. (2021). Análisis y diseño de una red lorawan para el monitoreo y preservación de obras de artes Patrimoniales en el Complejo Arquitectónico de las Conceptas de la Ciudad de Cuenca. Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas ….

Rondon Sanabria, J. S., & Bravo Montoya, A. F. (s. f.). Esquema de Seguridad de Datos Entre los Nodos y el Gateway en una Red LoRaWan.

Uribe Castro, A. (s. f.). Análisis del nivel de seguridad presente en los dispositivos que componen el internet de las cosas.

ANEXOS

ANEXO 1

FORMATO DE VALIDACIÓN

	**UNIVERSIDAD TECNOLÓGICA ISRAEL** Maestría en Seguridad Informática

El objetivo del presente instrumento es realizar una lectura del documento y realizar comentarios sobre el mismo dando de alguna manera una validación del mismo como un aporte al desarrollo de la seguridad informática en los sistemas de «IoT» y las redes de baja potencia de área extendida

Fecha: _____

1.- Datos Personales

Nombre:	
Título:	
Entidad en la que labora	
Cargo:	

2.- Comentarios

GRACIAS POR SU COLABORACIÓN

Firma

_____
Ci: _____

FORMATO DE VALIDACIÓN

Universidad Israel	**UNIVERSIDAD TECNOLÓGICA ISRAEL** Maestría en Seguridad Informática

El objetivo del presente instrumento es realizar una lectura del documento y realizar comentarios sobre el mismo dando de alguna manera una validación del mismo como un aporte al desarrollo de la seguridad informática en los sistemas de IoT y las redes de baja potencia de área extendida

Fecha: 11 de marzo del 2023

1.- Datos Personales

Nombre:	Ricardo Javier Cuichan Cueva
Título:	MAGISTER EN TECNOLOGIAS DE LA INFORMACION MENCIÓN EN REDES DE COMUNICACIONES
Entidad en la que labora	EPMMOP
Cargo:	Supervisor ejecutor de procesos 2

2.- Comentarios

En el documento se visualiza que se cumplieron los objetivos planteados, existiendo una relación clara con la metodología de desarrollo planteada, los resultados obtenidos y las conclusiones, evidenciando un trabajo investigativo exhaustivo; siendo estos resultados muy importantes en el ámbito de la seguridad de la Información por medio de la Norma Internacional ISO 27001:2013 aplicado en IoT. Este estudio podría servir como base para futuras investigaciones en donde se implemente en laboratorio con dispositivos IoT y se levante información y estadísticas reales.

La redacción del documento es clara, y el contenido incluye todo lo necesario para entender el tema, indicando el aporte de la seguridad informática en IoT y se entiende la importancia de estudiar las redes de baja frecuencia de área extendida.

GRACIAS POR SU COLABORACIÓN

Firma

Ci: 1716048655

ANEXO 1

FORMATO DE VALIDACIÓN

Universidad Israel	**UNIVERSIDAD TECNOLÓGICA ISRAEL** Maestría en Seguridad Informática

El objetivo del presente instrumento es realizar una lectura del documento y realizar comentarios sobre el mismo dando de alguna manera una validación del mismo como un aporte al desarrollo de la seguridad informática en los sistemas de IoT y las redes de baja potencia de área extendida

Fecha: 12/03/2023

1.- Datos Personales

Nombre:	**Ing. Andrés Carrillo L.**
Título:	**Ingeniero en Electrónica y Telecomunicaciones**
Entidad en la que labora	**EPMMOP**
Cargo:	**Supervisor Ejecutor de Procesos 2**

2.- Comentarios

Acorde al desarrollo del PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER con estudio en el ANÁLISIS DE BRECHAS DE SEGURIDAD EN REDES LPWAN - SIGFOX Y LORAWAN EN BASE A LA NORMA ISO 27001:2013 se puede reafirmar que todo sistema dispositivo o tecnología se encuentra expuesta a diversos métodos y procesos de vulnerabilidad tecnológica, los cuales tienen como objetivo la alteración, sustracción o manipulación de la información la cual es indispensable para el desarrollo y giro del negocio. La norma ISO 27001 especifica un sistema de gestión de seguridad de la información por lo cual es imprescindible desarrollar o implementar políticas que especifiquen el control y despliegue hacia las plataformas y modelos que implementen IoT. Pues bien, las seguridades en las plataformas analizadas no se encuentran en su mayor despliegue, se recomienda un análisis exhaustivo que mitigue las posibles vulnerabilidades y riesgos existentes para su posible control y protección.

GRACIAS POR SU COLABORACIÓN

CI: 1804000618

ANEXO 1

FORMATO DE VALIDACIÓN

	UNIVERSIDAD TECNOLÓGICA ISRAEL Maestría en Seguridad Informática

El objetivo del presente instrumento es realizar una lectura del documento y realizar comentarios sobre el mismo dando de alguna manera una validación del mismo como un aporte al desarrollo de la seguridad informática en los sistemas de IoT y las redes de baja potencia de área extendida

Fecha: 14-03-2023

1.- Datos Personales

Nombre:	**Diego Javier Pérez Sandoval**
Título:	**Magister en Ciberseguridad**
Entidad en la que labora	**Municipio de Quito**
Cargo:	**Ejecutor de Procesos 2**

2.- Comentarios

El documento de investigación realiza un análisis profundo sobre la aplicabilidad de la ISO 27001, contenido práctico, de fácil comprensión.

GRACIAS POR SU COLABORACIÓN

Firma

DIEGO JAVIER PEREZ SANDOVAL

CI: 1714416169

ANEXO 2

DOMINIOS, TÉCNICAS DE CONTROL Y CONTROLESDE LA NORMA ISO 27001:2013

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATRONICADO POR:

GES CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

Octubre-2013