INVESTIGACIÓN SOBRE PROCESOS VULNERABLES EN DISPOSITIVOS TECNOLÓGICOS

Carlos Edgar Lozano Cifuentes

Corporación universitaria UNITEC

SEMINARIO DE INVESTIGACIÓN I / 16 SEMANAS - CTP - 121A3

Ingeniero FABIO ANTONIO GONZALEZ MENDIETA

17 de octubre de 2022

INVESTIGACIÓN SOBRE PROCESOS VULNERABLES EN DISPOSITIVOS TECNOLÓGICOS

Autor

Carlos Edgar Lozano Cifuentes

Presentado para obtener el título de: Especialista en Seguridad de la Información

Ingeniero FABIO ANTONIO GONZALEZ MENDIETA

Corporación universitaria UNITEC

ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Bogotá

17 de octubre de 2022

**TABLA DE CONTENIDO**

[**INTRODUCCIÓN** 5](#_Toc116325457)

[**JUSTIFICACION** 7](#_Toc116325458)

[**PLANTEAMIENTO DEL PROBLEMA** 9](#_Toc116325459)

[**PREGUNTA PROBLEMA** 11](#_Toc116325460)

[**OBJETIVOS** 12](#_Toc116325461)

[**GENERAL** 12](#_Toc116325462)

[**ESPECIFICOS** 12](#_Toc116325463)

[**MARCO REFERENCIAL** 13](#_Toc116325464)

[**MARCO TEORICO** 15](#_Toc116325465)

[**INTERNET DE LAS COSAS 16**](#_Toc116325466)

[**ESTRUCTURA 17**](#_Toc116325467)

[**MARCO METODOLOGICO** 18](#_Toc116325468)

[**Aspectos metodológicos de la investigación** 18](#_Toc116325469)

[**Tipo de estudio** 19](#_Toc116325470)

[**Método de investigación** 19](#_Toc116325471)

[**Fuentes y técnicas para la recolección de información** 19](#_Toc116325472)

[**Entrevista al jefe del departamento de TI** 19](#_Toc116325473)

[**Población y muestra** 20](#_Toc116325474)

[**ANÁLISIS, PRESENTACIÓN DE RESULTADOS Y DIAGNÓSTICO** 20](#_Toc116325475)

[**Análisis de la situación actual** 20](#_Toc116325476)

[**Entrevista realizada al responsable del departamento de TI** 21](#_Toc116325477)

[**ALCANCE** 28](#_Toc116325478)

[**Conclusiones** 29](#_Toc116325479)

[**Bibliografía** 30](#_Toc116325480)

**Tabla de ilustraciones**

[Ilustración 1 Proyección dispositivos conectados 17](#_Toc116325402)

[Ilustración 2 Arquitectura 18](#_Toc116325403)

# **Introducción**

La continua evolución de las tecnologías, trae nuevas formas de comunicación, acortando las distancias y teniendo la posibilidad de comunicación en cualquier lugar del mundo, uno de estos avances ha traído consigo la posibilidad de conectar muchos dispositivos a la red de redes, la Internet, transformando la experiencia de vida de los usuarios al conectar desde electrodomésticos de hogar, vehículos, prendas de vestir deportivas, ya que con el uso de sensores estos pueden acoplarse a cualquier elemento y de allí comunicarlos a la red, generando nuevas capacidades en las transferencia de datos, estableciendo una serie de comportamientos que no requieren de la interacción humano-humano, humano-computadora, este avance tecnológico es lo que se conoce como Internet de las cosas.

Por consiguiente el avance tecnológico proporcionado por IoT, puede ser de gran utilidad al momento de controlar una serie de procesos que antes se veían inalcanzables, también la oportunidad de generar una serie de nuevas opciones de negocio basados en la información que cada uno de los dispositivos continuamente está comunicando al conectarse a Internet, ya no es extraño poder contactarnos con dispositivos con los que se interactúa día a día, los cuales hace unos años no se contemplaban que podrían estar conectados a internet y así hacer la vida un poco más cómoda basada en la toma de decisiones inteligentes y autónomas. LoT por tanto ofrece la interconexión de millones de dispositivos utilizando una serie de protocolos que permiten al dispositivo conectarse de manera guiada o no guiada con otros dispositivos y a la red de redes, entre los que destacan conexiones inalámbricas como Wifi que ofrece un rango mayor de alcance con respecto a Zigbee que su cobertura es menor o Bluetooth la cual es más personal, con la comunicación de estos dispositivos inteligentes se generan una serie de soluciones

automatizadas que ayudan en los procesos de las industrias en las que destacan las aseguradoras, agrícolas, transporte, deporte, entretenimiento, manufactura, gobierno, salud, educación, automotriz, pero para generar esas soluciones debe existir un interlocutor entre los dispositivos y el usuario final, quien hace estas funciones son las aplicaciones encargadas de recolectar la información que toma de los dispositivos con el objetivo de hacer un análisis de esa información que en un principio no llega a tener un valor o significado, pero con la ayuda de servicios específicos como el Big data, Machine learning, aprendizaje automático busca estructurar la información para a partir de allí encontrar patrones, conductas, comportamientos y así proveer a los dispositivos inteligencia artificial para la toma de decisiones, de esta manera la información estructurada debe ser enviada al usuario final a través de una interfaz que le permita entender de un manera clara, agradable, interactiva lo que está sucediendo y así mejorar sus procesos y actividades diarias tendiendo una mejor experiencia, entre los beneficios más importantes que aporta IoT son la automatización de procesos, flexibilidad en el trabajo, optimización en el análisis de datos, vigilancia tecnológica, supervisión, datos en tiempo real, conllevando a una nueva concepción de procesos empresariales y nuevas estructuras de trabajo.

# **JUSTIFICACION**

Actualmente con la aparición del IoT internet de las cosas, donde cada dispositivo que pueda imaginarse, tendrá la capacidad de conectarse a internet para cumplir una serie de actividades o procesos, millones de dispositivos generando una serie de información que en un alto porcentaje es considerada como sensible, estará viajando a través de la internet por medio de canales no seguros, de allí la importancia de analizar la seguridad en los dispositivos o cosas, ya que son la primera línea con las que un ciberdelincuentes se va a encontrar y es aquí donde estarán enfocados los diversos ataques que se pueden efectuar, así que si en estos dispositivos no se detectan cuáles son las vulnerabilidades que trae consigo las cuales se presentan en diferentes niveles, los controles que se efectúen no podrán ser efectivos, así que determinar una serie de procesos o guías que permitan al usuario establecer cuáles son las vulnerabilidades concurrentes, adicional identificar cuáles son los ataques a los que se está expuesto, serán de gran utilidad a la hora de minimizar los riesgos asociados que conlleva el uso esta nueva tecnología, a través de la interconexión de miles de dispositivos a Internet.(O. Gasquez, 2015)

Los procesos de comunicación siempre han tenido como fundamento la información, debido a la gran evolución tecnológica que ha sufrido las telecomunicaciones a lo largo de los años, el mundo ha venido cambiado la forma en que se comunica, en un principio tan solo utilizaba unos intérpretes, canales, lenguaje mensajes (información), a medida que estos procesos fueron evolucionando, aparecieron nuevos dispositivos que simplifican la manera de comunicación. Las redes de datos, internet, televisión, radio, satélites, telefonía, cada una de estas tecnologías comunican y gestionan diferentes tipos de información, voz, datos, imágenes, video (J. Moya, 2005).

Así mismo la información que se compartía en un principio, se hacía de manera local este rango se fue ampliando con la aparición de la Internet, creando nuevos modelos de negocio, educación, comercialización, investigación, entretenimiento, permitiendo la globalización de las comunicaciones, pero a su vez a ocasionar una serie de inconvenientes, en la pérdida de control sobre la información, debido a que esta pasaba por diferentes canales y redes que se consideran inseguras (R. Stair, 2000). Es así que empezaron aparecer nuevos desafíos encaminados a establecer estándares y normas que protegieran la información que circula por los diferentes canales comunicativos, conllevando a establecer una serie de buenas prácticas encaminadas a 3 principios básicos, disponibilidad donde la información debe ser aprovechable en cualquier momento, a cualquier hora, en cualquier lugar por quien lo requiera, confidencialidad indica que solo personas autorizadas a través de unos parámetros de seguridad específicos son las únicas que pueden acceder a la información, evitando el acceso a personas no autorizadas, integridad indica que se protege la información de alteraciones o modificaciones en el camino de un origen a un destino (V. Canal, 2004)

Por tal razón es de mucha importancia establecer una adecuada gestión de la información, que involucra una serie de fases entre las que destacan, fortalecimiento de dispositivos, infraestructura, servicios, aplicaciones, sistemas de seguridad donde se establecen vulnerabilidades, amenazas y riesgos a los que se está expuesto, con el fin de establecer una serie de contingencias y planes de seguridad minimizando la pérdida de privacidad de la información (J. Bertolin, 2008)

# **PLANTEAMIENTO DEL PROBLEMA**

Debido al gran número de dispositivos que se conectan día a día a Internet, estos se exponen a una serie de amenazas relacionadas con ciberataques que tienen una complejidad mayor debido a su estructura y alcance, hace unos años las técnicas utilizadas no eran tan estructurados, así que si no se tiene un adecuado nivel de seguridad en los dispositivos, al momento de la puesta en marcha al ser el Internet de las cosas (IoT) una tecnología emergente la cual establece la conexión y comunicación de millones de dispositivos a través de diferentes redes es inherente que surjan una serie de vulnerabilidades tanto a nivel lógico como físico en infraestructuras, protocolos, servicios, dispositivos, aplicaciones, las cuales al no ser atendidas con suficiencia serán punto de partida para los atacantes que aprovecharan esas falencias que puedan hallar, a través del uso de metodologías de ataque, personas no autorizadas puede extraer información o comprometer a un usuario, debido a la forma como se establecen nuevos modelos de trabajo, comunicación, comercialización, vigilancia a través de Internet, permite que información sensible se comparta a través de los canales de Internet, quedando expuestos a terceros, si no se empieza asegurar la pirámide desde su base es decir ,el fortalecimiento de los dispositivos o cosas como se denomina en IoT, muchos serán los sistemas comprometidos, lo que puede conllevar a pérdidas económicas, desastres o algo aún más preocupante la pérdida de la privacidad y confiabilidad de la información. (A. Pinto, 2012).

El avance de la tecnología está permitiendo que muchos dispositivos que en un principio no se pensaba que pudieran conectarse a la internet, hoy en día tengan la posibilidad de hacerlo, televisores, sensores, smartwatch, cámaras, celulares, adicional a los dispositivos que tradicionalmente ya tenían conexión a internet como computadoras, router, puntos de acceso, cambiando la forma de comunicación y transformando el uso de la Internet, esto ha producido un aumento en la asignación de direcciones que ya no puede soportar el protocolo IPV4, el cual agoto la asignación de direcciones a partir de la año 2011, así que desde ese momento los proveedores de servicio empezaron a desplegar direccionamiento basado en un nuevo protocolo ya que la cantidad de dispositivos conectados por usuario estaba en aumento, así que esta situación está ofreciendo la interoperabilidad de dos protocolos ya que muchos dispositivos están conectados bajo el protocolo anterior y nuevos dispositivos se conectan con el nuevo protocolo, esto requiere que las infraestructuras de red cuenten con equipos especializados, protocolos, elementos específicos para cada uno de los protocolos, pero que estos puedan también comunicarse entre sí, así que adoptando esta situación en la coexistencia pueden generar una serie de falencias o debilidades en los sistemas, dispositivos que pueden ser aprovechados por terceros para comprometer la información de los usuarios, debido a que todo estos procesos al ser nuevos presentan una serie de errores, que son base para así mejorar los procesos de aseguramiento (Y. Castillo, 2016)

Por consiguiente IPV6 surge como un nuevo protocolo que soporta esa gigantesca asignación de direcciones para millones de dispositivos que quieren acceder a internet brindando un aumento en la interconexión de dispositivos usados por persona en el mundo, pero que a su vez permite que sean muchos más los objetivos para delincuentes informáticos, estos se puedan aprovechar de las múltiples vulnerabilidades y así basar sus metodologías en ataques informáticos aprovechando la falta de vigilancia, ocasionando perdida de privacidad de la información, debido a que los millones de dispositivos que se van conectando a través de Internet, reunirán una serie de datos basados en comportamientos, actividades, inclinaciones, costumbres, generando una serie de interrogantes acerca de las consideraciones de seguridad a tener en cuenta en los dispositivos en el momento de implementar IoT y este no altere o afecte los 3 principios de la seguridad de la información, disponibilidad, integridad y confidencialidad (D. Evans, 2011).

# **PREGUNTA PROBLEMA**

A través del desarrollo de un estudio de carácter **inductivo - deductivo** ¿Qué tan expuestos están los dispositivos tecnológicos a vulnerabilidades?

# **OBJETIVOS**

# **GENERAL**

Analizar los aspectos de seguridad relacionado con las vulnerabilidades y ataques más frecuentes que se presentan en dispositivos tecnológicos (cámaras de seguridad, smartwatch, router, punto de acceso), estableciendo una ruta de buenas prácticas en el aseguramiento de los dispositivos.

# **ESPECIFICOS**

* Conocer las características de la arquitectura IoT.
* Consultar los fallos de seguridad generales, más frecuentes e importantes que se presentan en los dispositivos.
* Identificar los fallos de seguridad específicos más frecuentes e importantes que se presentan en los dispositivos.
* Establecer a través de una matriz DOFA los diferentes aspectos de IoT, relacionados con seguridad en 4 dispositivos que se tomaran como ejemplo de estudio.
* Elaborar una guía que detalle una ruta de buenas prácticas en el aseguramiento de los dispositivos.

## **MARCO REFERENCIAL**

Las redes de datos nacen con la necesidad de compartir recursos, servicios a través de sistemas informáticos con el fin de procesar la información de un manera más adecuada, de allí se determina que cuando una red de computadoras comparten un espacio local, de no mucha extensión, se conoce como LAN ( Red de área local), cuando comparte un espacio geográfico un poco más amplio pero sin exceder una extensión mayor se conocen como PAN ( Red de área panamericana), cuando su extensión es mayor conectado varias extensiones geográficas, se conoce como WAN( red de área extensa), lo que se conoce como Internet (A. tanenbaum, 2003).

La conexión de varias redes informáticas fue lo que fundamento la creación de la Internet, generando una revolución en la forma de comunicación de los seres humanos, a través de unos protocolos o reglas estandarizadas, su principal función era la de compartir información entre dispositivos, ubicados en extensiones geográficas diferentes, el Internet ha evolucionado constantemente, agregando servicios, aplicaciones, haciendo que millones de personas establezcan comunicación a través de diferentes plataformas, es así como se ha convertido en la conjunción de todas las tecnologías, radio, televisión, telefonía, eso ha conllevado a crear un nuevo lenguaje donde se establecen una serie de términos, ciberespacio, Ciber ciudadano, que han generado un cambio cultural en las sociedades.

Pero todo este cambio cultural ha influenciado la parte negativa de la sociedad, donde personas inescrupulosas ven al internet como una fuente de aprovechamiento de vulnerabilidades, buscando la manera de sacar provecho, a través del robo de información, violentar la privacidad de la información de las organizaciones o personas del común aumentando los delitos informáticos cada día, es importante definir que la Internet es un espacio de mucha importancia en el mundo actual, ya que establece una nueva forma de comunicación sin limitantes, ni barreras, pero en la otra arista encontramos que es un espacio de poca confiabilidad y que se debe tener muchas precauciones de seguridad al momento de colocar un dispositivo, servicio o información, ya que esto va estar expuesto a terceros.

Los dispositivos conectados a internet deben basar su comunicación en el protocolo IPV4, es un protocolo que asigna un identificador numérico, para que pueda interconectarse con otros dispositivos, utiliza direcciones numéricas de 32 bits ( 4 Bytes), teniendo una capacidad limitante de asignación de direcciones de 4.294.967.295, de este total algunas direcciones son de uso privado para conectar equipos a través de redes locales, direcciones de uso público asignadas por los proveedores de servicio y son las direcciones con las cuales podemos navegar por Internet, otras direcciones que tiene usos específicos.

Debido al avance de la tecnología y la conexión de millones de usuarios, el protocolo IPV4 ha agotado la asignación de direcciones públicas, así que aquellos nuevos usuarios que quieran conectarse a Internet no pueden hacerlos, a partir de allí viendo la necesidad de ampliar la asignación de direcciones, aparece un nuevo protocolo conocido como IPV6 el cual establece 128 bits, 8 bloques numéricos de 16 bits, para un total de 340.282.366.920.938.463.463.374.607.431.768.211.456 (340 sextillones), es decir que cada usuario puede conectar muchos dispositivos a Internet (S. Deering, 2017).

Paulatinamente el aumento de dispositivas se ha estado dando, es allí donde el internet de las cosas toma fuerza, generando la primera revolución del Internet logrando esta evolución que el Internet sea más sensorial, este basada en la comunicación de dispositivos con el fin de que sean ellos los que determinen una serie de comportamientos y permitan ejercer un control, sin tener que tener la intervención del usuario, en la búsqueda de llegar a lugares a los que nunca antes se había llegado a través de la comunicación, pero este avance aún necesita de tener un parámetros claros y estandarizados en cuanto a la seguridad, privacidad, arquitectura, la IEEE es una de la organizaciones que trabaja fuertemente para permitir que los paquetes IP puedan ser entendibles en los diferentes tipos de redes que atraviesa y esta comunicación no sea interrumpida (Dave Evans, 2011).

La tendencia indica que su implementación está acelerándose día a día, en el presente ya se cuenta con unos dispositivos controlando una serie de dispositivos de manera inteligente, en varias áreas creando su propio lenguaje y así determinando una serie de comportamientos, se espera que en el futuro esto se expanda y se aplique al término de ciudades inteligentes, industrias inteligentes, comercio inteligente, donde cada uno de los dispositivos cuenten con mucha más inteligencia, versatilidad y toma de decisiones, lo que va a generar la aceleración de las comunicación y forma de vivir de los seres humanos (Telefónica, 2011).

## **MARCO TEORICO**

**Seguridad Informática**. Se refiere a la protección de la información y de sistemas de información de acceso no autorizado, divulgación, alteración, modificación o destrucción para proporcionar confidencialidad integridad y disponibilidad.

En un sentido más amplio, según el libro Seguridad Informática Ethical Hacking de la ACISS (Asociación de Auditores, Consultores en la Instalación y Aseguramiento de Sistemas de Información) ; la seguridad informática representa un conjunto de medios y técnicas implementadas para asegurar la integridad y que no se difundan involuntariamente los datos que recorren un Sistema de Información, entendiendo como tal un conjunto de datos y de recursos (físicos, lógicos y humanos) que permiten almacenar y circular la información que contiene.

**Confidencialidad**. Se refiere a la propiedad de la información que garantiza que está sea accesible únicamente por personal autorizado a acceder a dicha información. Según la Organización Internacional de Estandarización (ISO) en la norma ISO/IEC 13335-1:2004: característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados

**Disponibilidad**. Es la característica, cualidad o condición de la información de estar a disposición de quienes tienen el privilegio de acceder a ella, sean personas, procesos o aplicaciones. En general, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que lo requieran; garantizar dicha disponibilidad implica también la prevención de

ataques de denegación de servicio (DoS). Para poder manejar con mayor facilidad la seguridad de la información, las empresas o negocios se pueden ayudar con un sistema de gestión permita conocer, administrar y minimizar los posibles riesgos que atenten contra la seguridad informativa del negocio.

**Integridad**. Se entiende por integridad el servicio de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado. Suelen integrarse varios conceptos análogos en este segundo aspecto de la seguridad: precisión, integridad y autenticidad. El concepto de integridad significa que el sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga. Esta propiedad permite asegurar que no se ha falseado la información. Por ejemplo, que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados, sin que se haya producido ninguna modificación, adición o borrado.

**Dispositivos móviles**. Se puede definir como un dispositivo de tamaño reducido (portable), con ciertas capacidades de procesamiento y almacenamiento de información, conexión permanente o intermitente a una red, que ha sido diseñado específicamente para una función, pero que adicionalmente puede llevar a cabo otras funciones. De acuerdo con esta definición existen multitud de dispositivos móviles, desde los reproductores de audio portátiles hasta los

navegadores GPS, pasando por los teléfonos móviles, los PDA o los Tablet PC

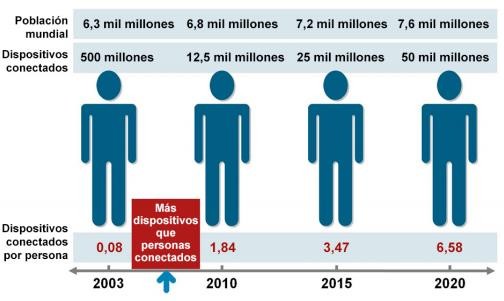
**Criptografía**. La criptografía (del griego κρύπτω krypto, «oculto», y γράφως graphos, «escribir», literalmente «escritura oculta») es la técnica, bien sea aplicada al arte o la ciencia, que altera las representaciones lingüísticas de un mensaje para proteger su contenido; en esencia la criptografía trata de enmascarar las representaciones caligráficas de una lengua, de forma discreta

**Redes 3G**. Se conoce con este nombre a la tercera generación de redes de comunicación móvil (para transmisión de voz, datos y video a través de teléfonos móviles), basada en el estándar UMTS (por sus siglas en ingles Universal Mobile Telecommunications System), su tecnología es una evolución de las redes 2G y representan un aumento en la velocidad de transmisión de información y aumento en la prestación de servicios, algunas de las características de estas redes de datos son:

* Velocidad de bit mayor a 2 Mbps, Velocidad variable de bit
* Múltiples servicios con diferentes requerimientos de calidad en una sola conexión.
* Coexistencia de sistemas de segunda y tercera generación y entre sistemas de
* handovers para aumentar cobertura y balanceo de carga
* Soporte asimétrico de tráfico en el Up link y Down link
* Alta eficiencia espectral
* Coexistencia del modo FDD y TDD

# **INTERNET DE LAS COSAS**

Es un término que cobra fuerza cada día, es un concepto tecnológico que busca conectar una serie de objetos a internet con el fin de automatizar una serie de procedimientos, utilizando un intercambio de información de manera sistematizada e inteligente, una gran parte de los objetos que están presentes en el Internet de las cosas son sensores que se entrelazan y conectan a través de redes inalámbricas, en la ilustración 1 se evidencia el crecimiento de dispositivos conectados para los años 2010, 2015, estimando un aumento muy significativo para el año 2020 de aproximadamente 50 mil millones de dispositivos conectados, de igual manera el crecimiento de dispositivos que se conectan por persona (A. Everlet, J. Pastor, 2013).

Ilustración Proyección dispositivos conectados

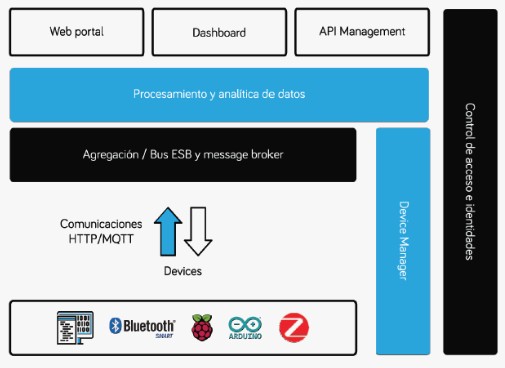
Fuente: Cisco IBSG, abril de 2011

Es así que toda esta conexión de diversos dispositivos, será la nueva generación del internet, ya que tendrá la capacidad de establecer nuevas formas para que los seres humanos establezcan comunicación, logrando impactos sensoriales a través de una serie de variables como temperatura, humedad, luz. Adicional con el Internet de las cosas se pueden llegar a una serie de lugares que en otras épocas se veían inalcanzables, esto permite que se creen sin números de aplicaciones

# **ESTRUCTURA**

El Internet de las cosas es un concepto naciente por tal razón aún no hay una tecnología definida, pero su estructura está basada en varios componentes importantes que definen su implementación, un componente son los sensores, dispositivos, actuadores que son conocidos como cosas que se conectan a internet, otro componente son los buses o canales por donde las cosas conectadas envían y reciben información, el otro componente son las pasarelas que sirven de puente de conexión entre las cosas, los buses o canales, para que estos puedan interactuar en la internet debido a que esta red de redes requiere de un protocolo o lenguaje de vital importancia para que se entiendan las comunicaciones, es así que las pasarelas realizan la comunicación utilizando el protocolo de internet obteniendo conectividad y tasa de cómputo según el requerimiento de la cosa, la ilustración 2 se puede observar una serie de capas de IoT, desde una inferior donde inicia el proceso con los dispositivos generando información, pasando por una capas intermedias que permiten la intercomunicación de dispositivos con protocolos, procesamiento de los datos, hasta una superior donde se brinda información ya estructurada al usuario de lo que genero el dispositivo por medio de aplicaciones (L. Jurado, A. Velásquez, F. Escobar, 2014).

Ilustración Arquitectura



Fuente: Zemsania Tech Services & Solutions Draft Arquitectura referencia

## **MARCO METODOLOGICO**

La metodología de investigación es de carácter **inductivo - deductivo** porque no se plantea una hipótesis, sino que se elabora una serie de conclusiones partiendo de los antecedentes de investigaciones similares dentro del campo de la seguridad informática más exactamente en las vulnerabilidades y amenazas en dispositivos tecnológicos

# **Aspectos metodológicos de la investigación**

# **Tipo de estudio**

El plan de mejoras para planificar, solucionar y controlar la seguridad informática y la seguridad de los dispositivos dentro de una empresa está basado en los siguientes tipos de estudio:

**Investigación exploratoria**: La finalidad de realizar esta investigación será analizar los problemas de seguridad informática , seguridad en dispositivos y de la información dentro de la organización, previo a la investigación los antecedentes o datos similares eran escasos y por ende se tuvo que explorar todos los temas referentes al desarrollo y gestión de la seguridad.

**Investigación no experimental:** Los sujetos de estudio que en este caso son el personal de la organización, fueron observados en su contexto natural y en su realidad cotidiana. No se los sometió a un experimento en particular sobre la falta de procedimientos para resolver casos de seguridad informática y de la información.

**Investigación de campo:** El estudio se realizó en el ambiente natural en el cual se desenvuelven los encargados del SGSI, mediante entrevistas se pudo obtener datos relevantes de la situación actual de la seguridad informática y de la información.

# **Método de investigación**

De acuerdo al análisis de la investigación y acciones correctivas que van a ser presentadas para la evaluación y mejor toma de decisión en el ámbito de la seguridad informática, hemos encontrado que lo realizaremos basándonos en el siguiente método de investigación:

**Método inductivo - deductivo:** De nuestras hipótesis e ideas debemos llegar a una conclusión, para que así tanto nosotros como la empresa podamos tomar las acciones correctivas a seguir para asegurar el cumplimiento de lo propuesto.

# **Fuentes y técnicas para la recolección de información**

## **Entrevista al jefe del departamento de TI**

Se realizó una única entrevista al jefe del departamento de TI, con los demás miembros del departamento se mantuvieron conversaciones durante el desarrollo de la auditoría, todo fue relacionado al desempeño actual del sistema de seguridad informática y de la información. Para efectos de este trabajo el personal que participó fue todo el personal del departamento de TI de la empresa, puesto que conocen con gran detalle el estado actual de la gestión de la seguridad de la información de la organización.

# **Población y muestra**

• Población

Personal del departamento de TI, los cuales conocen al detalle la situación actual del SGSI de la empresa.

• Muestra

La totalidad del personal de TI, el departamento cuenta con 6 personas donde cada uno cumple con funciones específicas en la administración del SGSI.

# **ANÁLISIS, PRESENTACIÓN DE RESULTADOS Y DIAGNÓSTICO**

## **Análisis de la situación actual**

La gran mayoría de las vulnerabilidades que se presentan en la empresa se debe al poco conocimiento e importancia que representa la seguridad de la información para los gerentes, los cuales son los responsables directos del estancamiento tecnológico que puede sufrir una organización, es difícil lograr que entiendan que la prioridad del negocio no es solo el ingreso económico sino también los procesos intermedios.

A este nivel, resulta imprescindible conocer la problemática, lo que determina la necesidad de efectuar un estudio de seguridad o, al menos, una auditoría competente, el resultado de llevar a cabo la ejecución de procesos de auditoría informática, dará como resultado conocer con exactitud los diversos riesgos y las diferentes soluciones posibles ante alguna vulnerabilidad o amenaza, así como del coste de cada una. Sobre la base de estos elementos, la dirección del organismo puede ya plantear los objetivos que resuelvan, en el espacio y en el tiempo, la problemática de seguridad existente, lo que se traducirá en el establecimiento de prioridades y plazos para su remediación.

Las empresas que no cuentan con el conocimiento acerca de sus vulnerabilidades y puntos débiles que pueden presentar pérdida de información, ya sea por un evento natural, por el ataque de hackers, trabajadores que se van de la firma o personas que se lucran con la información, debido a la mala implementación de políticas y normas de seguridad de la información; por lo tanto se le debe dar mucha importancia a la inversión de recursos sistemas informáticos y a su vez contar con el personal certificado en prácticas de seguridad informática y resguardo de información.

## **Entrevista realizada al responsable del departamento de TI**

a) **Sobre políticas de seguridad de la información**

¿Cuentan con políticas de seguridad de la información?

Si, existen políticas de seguridad informática y de la información definidas a manera general en las cuales existen prohibiciones y sanciones si no son acatadas por el personal en general.

¿Existen controles para comprobar el cumplimiento de sus políticas?

Si, existen controles definidos, pero no implementados en su totalidad. Muchas de las políticas expuestas y aprobadas por Gerencia general son cumplidas, pero no comprobadas al no existir un seguimiento de las mimas.

¿Todo el personal tiene conocimiento de las políticas de seguridad de la información?

El personal nuevo que ingresa a recibe charlas de inducción para conocer las políticas de seguridad informática y de la información, pero el personal que ha estado laborando algunos años en la empresa no conoce en su totalidad las políticas de seguridad informática.

b) **Sobre la gestión de activos**

¿Los activos informáticos están debidamente registrados por el departamento de TI en un inventario?

Si, existe un control de ingreso de información de los activos de información por parte del área de administración de activos fijos, pero como departamento de TI llevamos un control eventual, básico y no gestionado ni controlado del registro de activos de computación.

¿Este inventario está automatizado?

El inventario no está automatizado debido a que no contamos con un software que pueda facilitarnos la tarea de administración y control de los activos de computación.

¿El inventario de activos informáticos se actualiza periódicamente?

No necesariamente, la tarea de actualización se realiza cada año o pasando 2 dependiendo de la necesidad de algún requerimiento especifico de dicha información debido a que en varias ocasiones por tema de control de compras se requiere conocer si los activos se encuentran en buen estado, quienes son los custodios de los mismos, cambios de equipos por garantías y equipos que se dan de baja por el tiempo de uso.

c) **Sobre el personal de TI**

¿Los incidentes en los activos informáticos son reportados rápidamente por los usuarios?

Si, los usuarios en general reportan todos los incidentes relacionados con los activos.

¿El departamento de TI cuenta con actas de responsabilidad sobre los activos firmadas por cada usuario?

No, el procedimiento de asignación de activos de computación no se encuentra definido por procesos de entrega con actas de responsabilidad sobre su uso.

**d) Sobre la seguridad física y del entorno**

¿cuenta con mecanismos de respaldo del servicio eléctrico para garantizar la continuidad de las operaciones?

Si, existen mecanismos de respaldo del servicio eléctrico que funciona correctamente cada vez que exista alguna interrupción con la energía eléctrica.

¿Se realiza mantenimiento periódico al hardware y software?

No, el mantenimiento de los equipos se realiza solo si por sus condiciones de mal funcionamiento lo amerita; esto quiere decir que no son periódicas y tampoco hay algún tipo tarea o gestión creada para que este proceso sea preventivo.

¿Existen controles para los activos informáticos al estar fuera de la empresa?

No, no existen controles o normas definidas para equipos o activos de computación de propiedad de la empresa cuando están fuera de las instalaciones de la empresa.

¿Hay procedimientos para la reutilización de activos informáticos y para cuando estos son dados de baja?

Si, la mayoría de los equipos dependiendo de sus características pueden ser reutilizados o dados de baja; tal proceso se realiza en conjunto con el área de activos fijos para los registros de auditoría general.

e) **Sobre la gestión de comunicaciones y operaciones**

¿Tienen manuales de operación para cada uno de los sistemas informáticos?

No, contamos con pocos manuales de operación de los sistemas informáticos.

¿El personal de TI registra los cambios hechos en los sistemas informáticos (aplicaciones, software y sistema operativo)?

No, el departamento no tiene registros de incidentes sobre los sistemas informáticos.

¿Están debidamente segregadas las tareas del personal TI?

Si, cada uno sabe sus funciones y tareas a cumplir como parte de su trabajo.

¿Cuenta con controles contra software malicioso (Firewall, parches del SO, antivirus, antispyware, etc.)?

Si, contamos con herramientas de monitoreo y otras instaladas en las estaciones de trabajo (Antivirus) para la detección de código malicioso y virus.

¿Cuentan con mecanismos de respaldo para los medios de almacenamiento?

Si, existen mecanismos generales definidos para el respaldo de información tanto de estaciones de trabajo como de servidores.

¿Existen controles para la buena administración de los recursos de red (ancho de banda, direccionamiento IP, etc.)?

Si, cuenta con herramientas de control y monitoreo del uso general del ancho de banda; obteniendo con esto índices de consumo de Internet por usuarios, así como también controles de direccionamiento IP asignados a los mismos.

¿El área de TI ha implementado controles de monitoreo de actividades de red?

Si, el departamento cuenta con controles de monitoreo de sucesos en la red.

¿Registran actividades y eventos de seguridad en los sistemas de información?

Si, en la mayoría de los casos las actividades de seguridad informática relacionadas a los sistemas de información son registradas por el personal responsable del área de TI.

¿Se registra la actividad de los usuarios y administradores en los sistemas de información?

Si, se lleva a cabo registros de actividades de los usuarios sobre los recursos informáticos a los que puedan acceder.

f) **Sobre los controles de acceso**

¿Para los sistemas de información existen políticas de control de acceso?

Si, la mayoría de los sistemas de información tienen políticas de control de acceso.

¿Las políticas de control de acceso son aplicadas?

Si, las políticas son aplicadas en su totalidad por todos los miembros de GNN7 TV.

¿Hay un registro de los accesos otorgados a los sistemas informáticos?

Si, aunque este registro de accesos es actualizado esporádicamente.

¿Se aplican controles para el registro de nuevos usuarios?

Si, los controles para el registro de usuarios se aplican cada vez exista algún incidente con los mismos ya sea creación, eliminación o modificación de algún usuario.

¿Cuentan con procedimientos para agregar o quitar accesos a los usuarios a los sistemas de información?

Si, el agregar o quitar accesos a los usuarios a los sistemas de información es gestionado y revisado por el personal del área de TI.

¿Todas las aplicaciones tienen ID y contraseña para dar acceso a los usuarios?

Si, el uso de usuarios y contraseñas es único para todo el personal.

¿Hay políticas para la creación de contraseñas?

Si, existen lineamientos a cumplir para la creación de contraseñas.

¿El departamento de TI restringe y controla las aplicaciones autorizadas?

Si, existen aplicaciones permitidas dependiendo del perfil del usuario, así como también accesos a sistemas de información o utilización de algún recurso.

¿Hay controles para las sesiones inactivas de los usuarios?

Si, existen mecanismos definidos para gestionar sesiones activas por usuarios.

g) **Sobre el reporte de incidentes**

¿cuenta con un procedimiento formal para reportes de incidentes?

Si, contamos con un procedimiento general pero no formal de reportes de incidentes.

¿El departamento de TI tiene una herramienta de gestión de incidentes?

No, no contamos con herramientas de registro de incidentes.

¿Al reporta un incidente de seguridad se cuenta con un plan de respuesta?

Si, existen planes de respuesta de seguridad establecidos para gestionar cualquier incidente ocurrido con los sistemas de información.

h) **Sobre los planes de continuidad**

¿Se realizan pruebas, mantenimiento y evaluación constante de los planes de continuidad de las operaciones?

No, no existen planes de continuidad definidos y por ende no se realizan ni simulacros o pruebas de dichos planes.

## **ALCANCE**

El desarrollo de esta actividad contempla nivel de seguridad para el aseguramiento de la

información como metodología de vulnerabilidades y amenazas en dispositivos tecnológicos

1. Revisión de la documentación existente sobre las vulnerabilidades y amenazas en dispositivos tecnológico

2. Descripción de las vulnerabilidades y riesgos a los que se encuentran expuestos los dispositivos tecnológicos

3. Análisis de las vulnerabilidades y riesgos a los que se encuentran expuestos los dispositivos.

4. Aplicación de técnicas de validación de vulnerabilidades a los dispositivos.

5. Elaboración de un documento que contenga las mejoras prácticas enfocadas a la protección de la información.

## **Conclusiones**

La arquitectura, está basada en una serie de capas que permiten entender el funcionamiento de los dispositivos desde el momento que empiezan a generar información, hasta el momento en que se puede consultar esa información desde un cliente en cualquier lugar solo contando con un acceso a Internet.

Debido al auge, cada vez más dispositivos se conectan a la red, pero muchos de ellos no cuentan con medidas esenciales de seguridad, evidenciando una serie de vulnerabilidades relacionadas con los controles de acceso y el cifrado de la información, lo que conlleva a una serie de ataques relacionados con denegación de servicios, accesos no autorizados, por medio del uso de exploits sofisticados

Las amenazas más frecuentes evidenciadas en los 4 dispositivos utilizados como objeto de estudio, seleccionados están basados en malware, exploits, denegación de servicios, fuerza bruta, aprovechando las vulnerabilidades que trae consigo cada dispositivo

EL uso de la matriz DOFA, estableció una serie de fortalezas y debilidades para los 4 dispositivos que se tomaron como objeto de estudio, aprovechando las oportunidades con que cuenta cada uno para minimizar las debilidades encontradas, usando las fortalezas con que cuenta cada uno para evitar las amenazas concurrentes, y minimizar las debilidades a través de medidas de aseguramiento

## **Bibliografía**

EVERLET, Alvaro; PASTOR, Javier. Introducción al Internet de las cosas. *Construyendo un proyecto de IOT. España: Universidad Rey Juan Carlos*, 2013.

CAMA-PINTO, Alejandro; DE LA HOZ, Emiro; CAMA-PINTO, Dora. Las redes de sensores inalámbricos y el internet de las cosas. 2012.

TANENBAUM, Andrew. *Redes de computadoras*. Pearson educación, 2003.

ACERO, Luis. *Dirección estratégica*. Ecoe Ediciones, 2010.

BANKINTER, Fundación. El Internet de las cosas. *Sl: Fundación de La Innovación Bankinter*, 2011C. Narvaez. (2004).

MIRANDA, David, et al. *Seguridad de la información en la internet de las cosas*. 2016. Tesis de Licenciatura. Universidad Piloto de Colombia.

CHECK POINT. *2018 Security report.* Tel Aviv: Check point research. 2018.

EVANS, Dave. Internet de las cosas. *Cómo la próxima evolución de Internet lo cambia todo. Cisco Internet Bussiness Solutions Group-IBSG*, 2011, vol. 11, no 1, p. 4-11.

GONZÁLEZ, Daniel; TRINH, Anthanh. Análisis, diseño e implementación de un SDK híbrido basado en tecnologías web para la integración de clientes contra una plataforma de servicios RESTFul/JSON. 2015.

SOSA, Eduardo; GODOY, Diego. Internet del futuro. Desafíos y perspectivas. *Revista de Ciencia y Tecnología*, 2014, vol. 16, no 21, p. 40-46.

EVANS, Dave. Internet de las cosas. *Cómo la próxima evolución de Internet lo cambia todo. Cisco Internet Bussiness Solutions Group-IBSG*, 2011, vol. 11, no 1, p. 4-11.

USECHE, David. Cyberintelligence for IoT. 2018.

DI MONTE, Eduardo; SOLÍS, Daniel. Aquae Security: Un paso por delante de los ciberataques dirigidos. *Revista SIC: ciberseguridad, seguridad de la información y privacidad*, 2017, vol. 26, no 126, p. 68-70.

DOMÍNGUEZ, Enrique; MARRERO, Francisco. Diseño y desarrollo de la Interfaz de Comunicación del Sistema Diramic. *Revista CENIC. Ciencias Biológicas*, 2005, vol. 36.

MORENO, Francesc. *Demostrador arquitectura publish/subscribe con MQTT*. 2018. Tesis de Licenciatura. Universitat Politècnica de Catalunya.

MEJIA, Fernando. El internet de las cosas es algo genial, pero sumamente peligroso. *Enter*. 2018.

SUÁREZ, Isabella, et al. Monografía primer módulo maestría en territorio y ciudad. 2018.

GARCÍA, Jonathan. Sistema prototipo Fly-by-Wire. 2005.

BERTOLÍN, Javier, et al. *Seguridad de la información. Redes, informática y sistemas de información*. Editorial Paraninfo, 2008.

DÍAZ, Joaquín. Modelado de comunicaciones entre servicios internos y aplicaciones entre servicios internos y aplicaciones externas mediante APIS en el entorno bancario. 2017.

MOYA, José, TEJEDOR, Ramón; MARTÍNEZ, David. *Tecnologías de telecomunicaciones*. Creaciones Copyright, 2005.

ROMERO, Jose, et al. Prueba de plataformas para el desarrollo de aplicaciones de la Internet de las cosas. 2015.

MO, Jianpeng. *OPSWAT*. {En linea}. {9 de Enero de 2019}*.* disponible en: (https[://www](http://www.opswat.com/blog/why-advanced-persistent-threats-are-targeting-internet-).op[swat.com/blog/why-advanced-persistent-threats-are-targeting-internet-](http://www.opswat.com/blog/why-advanced-persistent-threats-are-targeting-internet-) things)