CENTRO DE CIENCIAS BÁSICAS
DEPARTAMENTO DE SISTEMAS DE INFORMACIÓN
MAESTRÍA EN INFORMÁTICA Y TECNOLOGÍAS COMPUTACIONALES.

TRABAJO PRÁCTICO

PROPUESTA DE IMPLEMENTACIÓN DE BUENAS PRÁCTICAS EN LAS POLÍTICAS DEL SERVICIO DE RED INALÁMBRICA EN CIUDAD UNIVERSITARIA (CAMPUS CENTRAL).

PRESENTA
I.S.C. EDSON TAYDE MACIEL RUMBO.

PARA OBTENER EL GRADO EN MAESTRÍA EN INFORMÁTICA Y TECNOLOGÍAS COMPUTACIONALES.

TUTOR
DRA. LIZETH ITZIGUERY SOLANO ROMO.

COMITÉ TUTORIAL
DR. CARLOS ARGELIO AREVALO MERCADO.
DR. JOSE MANUEL ANDRADE.
M.A. JOSÉ ANTONIO PÉREZ HERNANDEZ.

Aguascalientes, Aguascalientes., A 23 de Enero del 2018.

UNIVERSIDAD AUTONOMA
DE AGUASCALIENTES

FORMATO DE CARTA DE VOTO APROBATORIO

M. EN C. JOSÉ DE JESÚS RUIZ GALEGOS.
DECANO (A) DEL CENTRO DE CIENCIAS BÁSICAS
PRESENTE

Por medio del presente como Tutor designado del estudiante **EDSON TAYDE MACIEL RUMBO** con ID 210153 quien realizó el trabajo práctico titulado: **PROPUESTA DE IMPLEMENTACIÓN DE BUENAS PRÁCTICAS EN LAS POLÍTICAS DEL SERVICIO DE RED INALÁMBRICA EN CIUDAD UNIVERSITARIA (CAMPUS CENTRAL)** y con fundamento en el Artículo 175, Apartado II del Reglamento General de Docencia, me permito emitir el **VOTO APROBATORIO,** para que él pueda imprimirla, y así como continuar con el procedimiento administrativo para la obtención del grado.

Pongo lo anterior a su digna consideración y sin otro particular por el momento, me permito enviarle un cordial saludo.

A T E N T A M E N T E
"Se Lumen Proferre"
Aguascalientes, Ags., a 15 de Enero del 2018.

Dra. Lizeth Itziguery Solano Romo
Tutor de Trabajo Práctico

c.c.p.- Interesado
c.c.p.- Secretario de Investigación y Postgrado
c.c.p.- Jefatura del Depto. De Sistemas de Información
c.c.p.- Consejero Académico
c.c.p.- Minuta Secretario Técnico

UNIVERSIDAD AUTONOMA DE AGUASCALIENTES

FORMATO DE CARTA DE VOTO APROBATORIO

M. EN C. JOSÉ DE JESÚS RUIZ GALEGOS.
DECANO (A) DEL CENTRO DE CIENCIAS BÁSICAS
PRESENTE

Por medio del presente como Integrante del Comité Tutoral designado del estudiante **EDSON TAYDE MACIEL RUMBO** con ID 210153 quien realizó el trabajo práctico titulado: **PROPUESTA DE IMPLEMENTACIÓN DE BUENAS PRÁCTICAS EN LAS POLÍTICAS DEL SERVICIO DE RED INALÁMBRICA EN CIUDAD UNIVERSITARIA (CAMPUS CENTRAL)** y con fundamento en el Artículo 175, Apartado II del Reglamento General de Docencia, me permito emitir el **VOTO APROBATORIO,** para que él pueda imprimirla, y así como continuar con el procedimiento administrativo para la obtención del grado.

Pongo lo anterior a su digna consideración y sin otro particular por el momento, me permito enviarle un cordial saludo.

A T E N T A M E N T E
"Se Lumen Proferre"
Aguascalientes, Ags., a 15 de Enero del 2018.

M.A. José Antonio Pérez Hernández
Integrante del Comité Tutoral

c.c.p.- Interesado
c.c.p.- Secretario de Investigación y Postgrado
c.c.p.- Jefatura del Depto. De Sistemas de Información
c.c.p.- Consejero Académico
c.c.p.- Minuta Secretario Técnico

UNIVERSIDAD AUTONOMA
DE AGUASCALIENTES

FORMATO DE CARTA DE VOTO APROBATORIO

M. EN C. JOSÉ DE JESÚS RUIZ GALEGOS.
DECANO (A) DEL CENTRO DE CIENCIAS BÁSICAS
PRESENTE

Por medio del presente como Integrante del Comité Tutoral designado del estudiante **EDSON TAYDE MACIEL RUMBO** con ID 210153 quien realizó el trabajo práctico titulado: **PROPUESTA DE IMPLEMENTACIÓN DE BUENAS PRÁCTICAS EN LAS POLÍTICAS DEL SERVICIO DE RED INALÁMBRICA EN CIUDAD UNIVERSITARIA (CAMPUS CENTRAL)** y con fundamento en el Artículo 175, Apartado II del Reglamento General de Docencia, me permito emitir el **VOTO APROBATORIO,** para que él pueda imprimirla, y así como continuar con el procedimiento administrativo para la obtención del grado.

Pongo lo anterior a su digna consideración y sin otro particular por el momento, me permito enviarle un cordial saludo.

A T E N T A M E N T E
"Se Lumen Proferre"
Aguascalientes, Ags., a 15 de Enero del 2018.

Dr. Carlos Argelio Arévalo Mercado
Integrante del Comité Tutoral

c.c.p.- Interesado
c.c.p.- Secretario de Investigación y Postgrado
c.c.p.- Jefatura del Depto. De Sistemas de Información
c.c.p.- Consejero Académico
c.c.p.- Minuta Secretario Técnico

UNIVERSIDAD AUTONOMA
DE AGUASCALIENTES

FORMATO DE CARTA DE VOTO APROBATORIO

M. EN C. JOSÉ DE JESÚS RUIZ GALEGOS.
DECANO (A) DEL CENTRO DE CIENCIAS BÁSICAS
PRESENTE

Por medio del presente como Integrante del Comité Tutoral designado del estudiante **EDSON TAYDE MACIEL RUMBO** con ID 210153 quien realizó el trabajo práctico titulado: **PROPUESTA DE IMPLEMENTACIÓN DE BUENAS PRÁCTICAS EN LAS POLÍTICAS DEL SERVICIO DE RED INALÁMBRICA EN CIUDAD UNIVERSITARIA (CAMPUS CENTRAL)** y con fundamento en el Artículo 175, Apartado II del Reglamento General de Docencia, me permito emitir el **VOTO APROBATORIO,** para que él pueda imprimirla, y así como continuar con el procedimiento administrativo para la obtención del grado.

Pongo lo anterior a su digna consideración y sin otro particular por el momento, me permito enviarle un cordial saludo.

A T E N T A M E N T E
"Se Lumen Proferre"
Aguascalientes, Ags., a 15 de Enero del 2018.

Dr. José Manuel Andrade
Integrante del Comité Tutoral

c.c.p.- Interesado
c.c.p.- Secretario de Investigación y Postgrado
c.c.p.- Jefatura del Depto. De Sistemas de Información
c.c.p.- Consejero Académico
c.c.p.- Minuta Secretario Técnico

UNIVERSIDAD AUTONOMA
DE AGUASCALIENTES

EDSON TAYDE MACIEL RUMBO
MAESTRÍA EN INFORMATICA Y TECNOLOGIAS COMPUTACIONALES
P R E S E N T E.

Estimado alumno:

Por medio de este conducto me permito comunicar a Usted que habiendo recibido los votos aprobatorios de los revisores de su trabajo de tesis y/o caso práctico titulado: **"PROPUESTA DE IMPLEMENTACIÓN DE BUENAS PRÁCTICAS EN LAS POLÍTICAS DEL SERVICIO DE RED INALÁMBRICA EN CUIDAD UNIVERSITARIA (CAMPUS CENTRAL)** hago de su conocimiento que puede imprimir dicho documento y continuar con los trámites para la presentación de su examen de grado.

Sin otro particular me permito saludarle muy afectuosamente.

A T E N T A M E N T E
Aguascalientes, Ags., a 17 de enero de 2018
"Se lumen proferre"
EL DECANO

M. en C. JOSÉ DE JESÚS RUÍZ GALLEGOS

c.c.p.- Archivo.

AGRADECIMIENTOS

A la Doctora Lizeth, por su gran apoyo durante este proceso de desarrollo.

A mi Maestro Oswaldo por brindarme su gran sabiduría y apoyo durante todo el desarrollo de este trabajo.

Al ingeniero José Antonio, por darme la oportunidad de conocer la gran persona que es, por apoyarme siempre proporcionándome la información y documentos necesarios para el desarrollo de este trabajo práctico.

DEDICATORIAS

A Mitzi por ser tan importante en mi vida, un gran ejemplo a seguir y por estar conmigo en las buenas y las malas.

A mi papá Tayde, a mi mama Teresa y a mis hermanos, por ser mi mayor tesoro, apoyarme en a salir adelante y por ser la mejor familia del mundo.

A Don Francisco y Doña Mirna por ser unas extraordinarias personas y apoyarnos siempre.

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Actualmente, cualquier empresa u organización tiene la necesidad contar con una interconexión de manera geográfica o global con la finalidad de realizar intercambios de información. De tal manera que, en el ambiente de las Tecnologías de Información, existe una tecnología que se adapta a esa necesidad, la cual tiene por nombre “Redes Inalámbricas”. Algunos se preguntarán ¿Qué es una red inalámbrica?, una red inalámbrica es una serie de interconexiones entre dispositivos, que permiten realizar un enlace entre ellos sin el uso de cables, tanto de manera local como de manera remota, teniendo como ventajas: la movilidad, flexibilidad, el bajo costo y una fácil instalación para lograr una transferencia de información con el uso de esa tecnología.

Existen empresas internacionalmente reconocidas, que implementaron esta tecnología, pero desafortunadamente, tuvieron algunas eventualidades orientadas a seguridad que ocasionaron algunos problemas dentro de ellas.

Durante el paso de los años, la tecnología de redes inalámbricas, han venido presentados problemas significativos en sus protocolos. A esos problemas también se les conoce o son llamados vectores de ataque y estos pueden afectar seriamente la integridad de esta tecnología. Tomando en cuenta que esta tecnología de redes inalámbricas es mayormente utilizada en la actualidad, los vectores de ataque han ido creciendo significativamente, clara razón está que el año 2017 es uno en los que mayores vulnerabilidades relacionadas a las redes inalámbricas, se han presentado.

La Universidad Autónoma de Aguascalientes se ofrece un servicio de red inalámbrica a aproximadamente más de 13,000 usuarios, y para conseguir brindar el servicio es necesario contar con la tecnología e infraestructura necesaria para lograrlo. Durante el proceso de investigación, se realizaron diversas entrevistas con el personal encargado de la gestión de todos los accesos inalámbricos de la universidad y posteriormente se observó e identificó que existe una problemática la cual es: la falta de gobernanza en los niveles de servicio, una estrategia de

seguridad y de implementación de normatividades para el servicio, todo esto basado en seguridad.

Por lo cual en base a lo identificado el objetivo general de este trabajo practico es: generar una propuesta de implementación de buenas prácticas en las políticas del servicio de red inalámbrica basadas en seguridad, en ciudad universitaria que aporten valor a la institución, permitiendo así, el seguro y correcto funcionamiento de la misma, basándose en los siguientes puntos:

- Analizar el estado actual del objeto de estudio
- Identificar las vulnerabilidades del servicio de red inalámbrica
- Identificar las amenazas a las que se encuentran expuestos los usuarios que se conectan al servicio de red inalámbrica.
- Generar un decálogo de buenas prácticas que apoye al seguro y correcto funcionamiento de la red inalámbrica en ciudad universitaria.

ABSTRACT

Currently, any company or organization has the need to have a geographical or global interconnection to be able to exchange information. In such a way that, in the environment of Information Technology, there is a technology that adapts to this need, which is called "Wireless Networks". Some may ask: What is a wireless network? A wireless network is a series of interconnections between devices that allow a link between them without the use of cables, both locally and remotely, with the following advantages: mobility, flexibility, low cost and easy installation to achieve a transfer of information with the use of that technology.

There are companies internationally recognized that implemented this technology, but unfortunately, they had some security-oriented eventualities that caused some problems within them.

Over the years, wireless network technology has presented major problems in its protocols. These problems are also known or called attack vectors and can seriously affect the integrity of this technology. Considering that this wireless network technology is mainly used today, attack vectors have been growing significantly, it is clear that 2017 is one in which there have been major vulnerabilities related to wireless networks.

The Autonomous University of Aguascalientes offers a wireless network service to approximately more than 13,000 users, and to obtain the service it is necessary to have the technology and infrastructure necessary to achieve it. During the research process, several interviews were conducted with the personnel in charge of the management of all the wireless accesses of the university and then it was observed and identified that there is a problem that is: the lack of governance in the service levels, a security strategy and implementation of regulations for the service, all this based on security.

Therefore, based on what has been identified, the general objective of this practical work is: to generate a proposal for the implementation of good practices in the

policies of wireless network services based on security, in a university city that adds value to the institution, which allows insurance and the proper functioning of them, depending on the following points:

- Analyze the current state of the object of study
- Identify the vulnerabilities of the wireless network service
- Identify the threats to which users who connect to the wireless network service are exposed.
- Generate a decalogue of good practices that support the safe and correct operation of the wireless network in the university city.

CAPÍTULO I

INTRODUCCIÓN: FUNDAMENTOS GENERALES DE LA INVESTIGACIÓN.

1.1 INTRODUCCIÓN.

La Universidad Autónoma de Aguascalientes (UAA) fundada en el año de 1973 por el gobernador de ese entonces J. Jesús Gómez Portugal; es una de las universidades de más alto prestigio a nivel nacional, la cual cuenta con extensas instalaciones completamente equipadas para ofrecer la mejor formación de profesionales e investigadores en distintas ramas que están relacionadas con el desarrollo socioeconómico de la región y a nivel nacional. La UAA cuenta con aproximadamente 19,463 alumnos activos actualmente y 1871 docentes activos (estadística institucional, diciembre 2016) que se dividen entre los 65 programas académicos de pregrado que oferta como lo son las 14 ingenierías y 51 licenciaturas; también ofrecen 14 especialidades médicas, una especialidad a distancia, 16 maestrías y 10 doctorados.

La Universidad Autónoma de Aguascalientes también se destaca por su amplio equipamiento tecnológico en su infraestructura; donde sale a relucir, el gran trabajo que se realiza dentro del departamento de Redes ***y Telecomunicaciones***, brindando a sus usuarios un muy buen servicio de ***red inalámbrica en ciudad universitaria***. Las redes inalámbricas en entornos educativos brindan una gran comodidad al utilizarlas, ya que les da a los usuarios el acceso a servicios locales ofrecidos por la organización (comunicaciones unificadas, plataformas educativas, plataformas administrativas, fuentes digitales) o el acceso a servicios externos mediante un enlace a internet (redes sociales, fuentes de investigación académica, compras, noticias, streaming, entre otros). El uso de tecnología de redes inalámbricas ha ido creciendo a pasos agigantados en los últimos años, como lo ha ido haciendo también los altos volúmenes de información que se mueve dentro de la red, las

vulnerabilidades, amenazas que están evolucionando. La falta de medidas de seguridad de la información, aplicada en las redes inalámbricas, puede tornar a ser un problema que tiene un impacto significativo en las organizaciones, esto debido a las amenazas existentes y los vectores de ataque que han sido desarrollados para aprovechar cada vulnerabilidad que se identifique en la red inalámbrica.

Para poder establecer una propuesta de implementación de buenas prácticas que permita mantener un servicio de red inalámbrica seguro y funcionalmente estable es necesario investigar los diferentes tipos de ataque de hoy en día, identificar las vulnerabilidades a las que está expuesta el objeto que se está estudiando. Al utilizar herramientas para realizar pruebas de penetración, ayudara a analizar y evaluar los diferentes escenarios a los que se expone la red inalámbrica y en base a ello, presentar las propuestas de buenas prácticas que apoyen a mejorarlos.

1.2 PROBLEMA DE INVESTIGACIÓN.

1.2.1 DESCRIPCIÓN DEL PROBLEMA DE INVESTIGACIÓN.

En el área involucrada en la administración del servicio de red inalámbrica de ciudad universitaria (Campus Central), se identificaron áreas de oportunidades que se basan en buenas prácticas, las cuales son descritas a continuación:

- Falta de gobernanza basada en los niveles de servicios (SLA).
- Falta de estrategias para el apoyo al cumplimiento de normas informáticas basadas en seguridad.
- Falta de estrategias para la implementación de normas informáticas basadas en seguridad para el servicio de red inalámbrica en ciudad universitaria.

1.2.2 PREGUNTAS DE INVESTIGACIÓN.

- ¿Se puede crear una gobernanza de TI basada en los niveles de servicio (SLA)?
- ¿Se puede crear una estrategia que apoye al cumplimiento de normas informáticas basadas en seguridad?
- ¿Se puede crear una estrategia de implementación de normas informáticas que estén basadas en seguridad para el servicio de red inalámbrica en ciudad universitaria?

1.3 OBJETIVOS DE LA INVESTIGACIÓN.

1.3.1 OBJETIVO GENERAL.

Generar una propuesta de implementación de buenas prácticas en las políticas del servicio de red inalámbrica basadas en seguridad, en ciudad universitaria que aporten valor a la institución, permitiendo así el seguro y correcto funcionamiento de la misma.

1.3.2 OBJETIVOS ESPECÍFICOS.

- Analizar el estado actual del objeto de estudio.
- Identificar las vulnerabilidades del servicio de red inalámbrica.
- Identificar las amenazas a las que se encuentran expuestos los usuarios que se conectan al servicio de red inalámbrica.
- Generar un decálogo de buenas prácticas que apoye al seguro y correcto funcionamiento de la red inalámbrica en ciudad universitaria.

1.4 JUSTIFICACIÓN.

La finalidad de este Trabajo Practico es investigar y analizar a fondo el estado actual de la Red Inalámbrica de Ciudad Universitaria (Campus Central), identificar a detalle cada una de las vulnerabilidades con las que cuenta en su momento el servicio tomando en cuenta el análisis realizado sobre el objeto de estudio (personas, tecnología, procesos) y base a esto lograr

identificar las amenazas a las que se encuentran expuestos los usuarios que utilizan día con día este servicio en el cual se conectan para realizar actividades académicas o personales.

Así mismo y tomando en cuenta cada uno de los puntos críticos mencionados, se realiza una investigación centrada en la información obtenida en el análisis del objeto de estudio y se genera un decálogo de buenas prácticas que apoye al equipo de personal del departamento que se encarga de gestionar el servicio de red inalámbrica a tomar la mejor decisión para mantener una red segura y funcionalmente estable.

1.5 ALCANCE.

El alcance del desarrollo de esta investigación de trabajo practico, es aportar un decálogo con medidas que apoyen a mantener redes de comunicación inalámbrica seguras, lo suficientemente sólidas que soporten la mayor parte de los vectores de ataque que están dispuestos a atacar y generar intrusiones y violaciones a la información que fluye dentro de la red inalámbrica. Prevenir problemas que pueden ser muy delicados y llegar a ser irreversibles en algunos casos, de igual forma el dar a conocer importantes recomendaciones para la mejora de la tecnología ya utilizada.

Este trabajo practico de investigación solo abarca fines informativos y manifiestos, proveer la información necesaria para que la organización obtenga los conocimientos de nuevas y buenas prácticas que garanticen una amplia protección en la transmisión de la información y seguridad de datos dentro de una red inalámbrica, también es necesario crear conciencia a los usuarios y administradores sobre la seguridad de la información, ante ataques y frecuentes vulnerabilidades a las que podrían estar expuestos.

CAPITULO II.

2 MARCO CONCEPTUAL.

2.1 ANTECEDENTES.

CASO 1.- SISTEMAS EMPRESARIALES PARA LOS DISTRIBUIDORES DE HARLEY-DAVIDSON.

Harley Davison Motocycles es una compañía estadounidense que cuenta con casi 800 distribuidores en su país, las cuales son controlados por el sistema de distribuidores de la compañía HDDS (Harley-Davison Dealer Systems, por sus siglas en ingles). HDDS en conjunto con sus colaboradores, brindan un amplio conjunto de soluciones y servicios personalizados para cada uno de los distribuidores de la compañía. La compañía maneja sistemas sumamente importantes, como el portal de compras, ventas, sistemas de procesamiento de pagos, manejo de inventarios, etc.

Impulsado por el panorama de amenazas constantes, los distribuidores de Harley-Davison recurren a HDSS para recibir de manera correcta retroalimentación sobre las mejores maneras de proteger la gran cantidad de datos que se manejan. Uno de los principales motivos que los ha llevado a realizar esto es debido a la existencia de software malicioso como el Ransomware, que encripta intencionalmente los datos críticos de la compañía a cambio de pagar un valioso rescate para poder recuperarlo.

Todo esto los llevo a estandarizar soluciones de seguridad con un único proveedor, ofreciendo la seguridad como un servicio a los distribuidores de Harley-Davison de una manera sencilla y fácil de reproducir en cada una de las sucursales que existen. Brindando herramientas que les facilitan la manera de visualizar y controlar los dispositivos, y además de esto, pudiendo así abordar

eficientemente los problemas sin ningún inconveniente (GLOBAL HEADQUARTERS & Fortinet Inc., s/f-a).

CASO 2.- PARQUE TEMÁTICO POPULAR, POTENCIÓ SUS VENTAS Y RENTABILIDAD CON EL USO DE ANÁLISIS DE DATOS.

Bobbejaanland fundada en 1960, es uno de los parques de diversiones más populares de Bélgica. Este parque cuenta con más de 40 atracciones y tienen entre 750,000 a 800,000 visitantes por año. Ante estos datos y con la finalidad de mejorar la rentabilidad y de aumentar la asistencia de personas al parque; decidieron innovar usando la tecnología WIFI para captar la inteligencia de cada uno de los visitantes y así lograr impulsar las ventas en general.

La compañía, al identificar la importante tendencia social y el impacto generado por el uso de la telefonía móvil, se creyó que al desplegar una infraestructura WIFI en todo el parque para los visitantes y el personal mismo, utilizarían este medio para aumentar las ventas per cápita y mejorar la eficiencia operativa e impulsar la lealtad de los visitantes del parque.

Así que en abril del 2014 se instaló y habilito WIFI utilizando proveedores externos para administrar los dispositivos instalados en todo el parque. Con esto se lograron utilizar herramientas para medir en tiempo real el tiempo promedio de permanencia, flujos de tráfico de cada uno de los visitantes que estuvieran conectados a la red del parque.

Los resultados fueron impresionantes, ya que del 30% esperados a medir, se logró identificar más del 60 al 80% de estos visitantes mediante el uso estas herramientas. Gracias al éxito del uso de esta tecnología, después se comenzaron a implementar nuevas herramientas para el análisis de datos que ayudaron a potenciar las ventas de comida y bebidas dentro del parque. También implementaron la distribución de anuncios publicitarios a través de los dispositivos móviles de los visitantes que se mantenían conectados a la red

WIFI, utilizando aplicaciones de autentificación dentro de los dispositivos (gestionadas por los sistemas administrativos de la red), solicitando el correo electrónico del visitante o su Facebook ID (GLOBAL HEADQUARTERS & Fortinet Inc., s/f-b).

CASO 3.- UNA DE LAS MAYORES ORGANIZACIONES DENTALES DE ESTADOS UNIDOS, DISFRUTA DE UNA PROTECCIÓN MEJORADA DE SUS SISTEMAS CON UN COSTO DE PROPIEDAD INFERIOR.

Heartland Dental es la organización de soporte dental más grande en Estados Unidos, esta se encarga de brindar servicios administrativos, contables y de marketing digital, a las oficinas dentales del país y ofrece a sus miembros, colaboración y entrenamiento profesional, incluyente también el intercambio profesional entre ellos. Esta compañía brinda soporte a más de mil dentistas en más de 750 oficinas a nivel nacional.

Heartland Dental siempre ha realizado énfasis en garantizar la infraestructura general de seguridad de TI. Anteriormente esta compañía implemento firewalls de un fabricante de alto prestigio, pero las capacidades administrativas de estos dispositivos y el conjunto de características con las que contaban no cumplían con los requerimientos en el rápido crecimiento de la compañía, por lo que se vieron obligados a realizar una reestructuración de la infraestructura y de buscar a un nuevo proveedor que se adaptara a los requerimientos de la empresa.

Tomando en cuenta lo anterior, el departamento de TI de la compañía, lanzo un proyecto para mejorar el monitoreo, la administración y elevar la postura general de seguridad. Después de una rigurosa búsqueda identificaron a un proveedor que apoyaría a proteger la diversa superficie de ataque con la que contaba la empresa, mediante una arquitectura de seguridad que se basa en la prueba del rendimiento.

Después de ser aprobada la propuesta en todas las dependencias de la compañía se implementó esta arquitectura basada en seguridad, junto con avanzados sistemas de detección de amenazas que evalúan código sospechoso y URLs de manera separada, autónoma y en un ambiente seguro.

Todo esto aseguro que cualquier solución implementada pudiera ser escalable con el propósito de simplificar y facilitar la gestión, elevando una protección elevada, gobernanza y visibilidad en toda la infraestructura (GLOBAL HEADQUARTERS & Fortinet Inc, s/f).

2.2 TRABAJOS SIMILARES.

- Diseño y Evaluación de un proceso Integrado de Gestión de Asistencia-Incidentes de Servicios de TI: Caso LabDC UAA(Jesus Carlos Bautista Ramos, s/f).
- Metodología para la evaluación del desempeño de controles en sistemas de gestión de Seguridad de la información (Juan Pablo Berrio López, Universidad Nacional de Colombia).
- Diseño y evaluación de un proceso de gestión de Seguridad de servicios de TI: caso LABDC-UAA (Ing. David Alejandro Montoya Murillo, s/f)
- Diseño y evaluación de un proceso de gestión de configuraciones de servicios de TI: caso LABDC-UAA (Alma Karina Jimenez Estrada, s/f).

2.3 MARCO TEÓRICO.

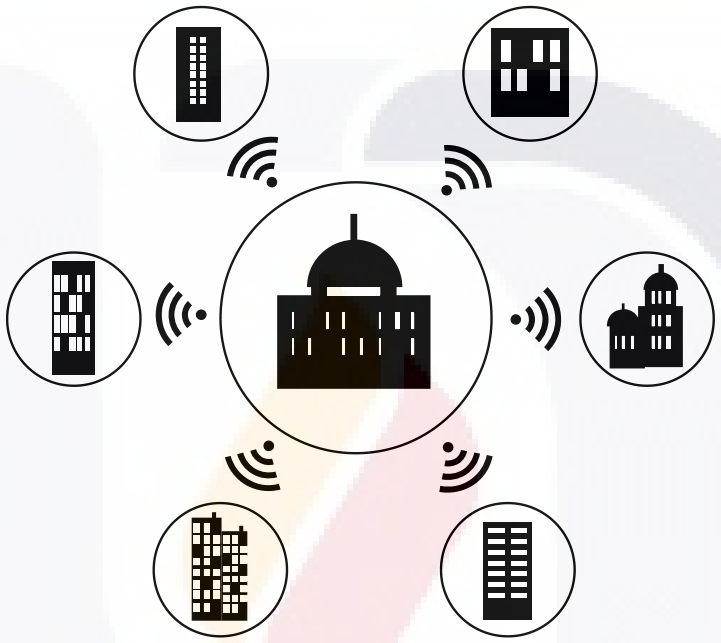
2.3.1 REDES INALÁMBRICAS.

DEFINICIÓN.

Una red inalámbrica permite la interconexión entre dispositivos electrónicos sin cables. Estas Redes inalámbricas nos permiten obtener un documento del servidor cuando está en la sala de conferencias, acceder al sistema de inventario desde el

almacén, todo esto lo facilita mediante ondas de radio que permiten que los dispositivos móviles de un área determinada se conecten y comuniquen entre sí.
Las redes inalámbricas están compuestas por nodos conectados entre sí por medio de ondas de radio frecuencia que son transportadas por a través del aire como se puede observar en la Figura 1 (Edge, Barker, Hunter, & Sullivan, 2010).

Figura 1. Conexiones inalámbricas entre edificios (Adaptada de: Barry Lewis & Peter T. Davis).



Cada uno de esos nodos se constituyen por una variedad de elementos como:

- **Antenas** (para enviar y recibir la señal).
- **Puntos de acceso** (su tarea principal es la de codificar y decodificar la información o los datos que son transmitidos por medio de la red a la que pertenecen).
- **Clientes inalámbricos** (los equipos de cómputo o dispositivos móviles que utilizan las personas para acceder a la red inalámbrica).
- **Componentes electrónicos** (para proporcionar energía a todos los elementos que se encuentran enlazando la red), torres (elemento

físico donde se colocan las antenas para enviar y captar señal en una posición privilegiada),

- **Conectores y adaptadores** (para realizar la conexión correspondiente de todos los dispositivos que intervienen en el funcionamiento de la red).

La mayoría de estos elementos se pueden encontrar el mercado a precios accesibles en el mejor de los casos (Battiti, Cigno, Sabel, Orava, & Pehrson, s/f). La implementación y el uso de estándares abiertos, generaron la posibilidad de que exista una amplia variedad de marcas de componentes o dispositivos de red que son compatibles entre sí y pueden interconectarse sin problema de depender de un solo proveedor de estos mismos.

En la actualidad la mayoría de las empresas que están encargadas de producir tecnología de redes, nos brindan equipos sofisticados y novedosos, los cuales permiten modificar su firmware o su software cargado con la finalidad de optimizar su funcionalidad (rendimiento, potencia, alcance, etc.) (“Types of Wireless Network Security Technology”, 2006) lo mejor posible para generar beneficios a la organización que los adquiere y utiliza.

CARACTERÍSTICAS.

- Facilidad de movilidad del usuario.
- Los dispositivos inalámbricos usan tecnología de radiofrecuencia (RF) y facilitar la comunicación.
- Ofrecen varios tipos de soluciones de visión, a menudo variables en el mayor de casos.
- Transmisión omnidireccional
- Transmisión dirigida.
- Uso al aire libre.
- No tienen ancho de banda limitado.

- Señales transmitidas en todas las direcciones (Sheetal Joseph, 2008, p. 8,9).

VENTAJAS.

La tecnología de LAN inalámbrica (WLAN) ofrece muchas ventajas para organizaciones de pequeña y gran escala, en términos de costos y productividad y sus principales beneficios son:

- **Movilidad:** los usuarios móviles equipados con computadoras portátiles y PDA pueden acceder a recursos de red e información digital desde cualquier lugar dentro o fuera de su organización.
- **Flexibilidad: las** organizaciones no están restringidas a la red cableada tradicional existente y pueden ampliar fácilmente el tamaño de su red. Además, se pueden usar equipos inalámbricos donde los cables no se pueden instalar.
- **Bajo costo:** no es necesario invertir en equipos de infraestructura con cable, como concentradores, conmutadores, paneles de conexión y cables.
- **Instalación fácil:** la instalación inalámbrica se completa en cuestión de horas, mientras que la instalación de la red por cable puede tardar días (Sheetal Joseph, 2008, p. 3).

DESVENTAJAS.

Las redes inalámbricas ofrecen muchos beneficios, pero también es importante comentar que también presentan problemas e inconvenientes en particular como:

- **Seguridad:** Esta es la mayor desventaja con la que nos encontramos al utilizar una red inalámbrica. Por ello es necesario diseñar y desarrollar las redes inalámbricas con un nivel de seguridad alto con la finalidad de evitar accesos no autorizados. Cuando se originaron los estándares de las redes inalámbricas no

se prestó la atención suficiente al tema de seguridad, por ende, quedando poco definido. En la actualidad la seguridad ha tornado a ser de los temas más fundamentales e importantes a tomar en cuenta, por eso es que hablaremos de ello más adelante(“Introducción a las redes inalámbricas.pdf”, s/f, p. 17) .

- **Interferencias:** Entre esta tecnología y las WLAN existen serios problemas de interferencias, algunos dispositivos que se encuentren en las cercanías afectarán produciendo algún tipo de interferencia en nuestra red. Este tipo de interferencias pueden provenir de otras redes inalámbricas próximas y algunos puntos que pueden provocar este tipo de problemas puede ser la tecnología Bluetooth, que es utilizada para equipos a corta distancia y baja capacidad.

- **Limitación en frecuencias:** El ancho de banda a una frecuencia de 2.4 GHz, está restringido a unos 100 MHz, que equivale a 3 canales. En la banda de 5 GHz, se tienen un total de 8 canales no dedicados para Wi-Fi.

- **Limitación en distancia:** El radio de trabajo de una red inalámbrica está condicionado mediante una potencia máxima que se puede emitir según la legislación de telecomunicaciones vigente. Para extender la zona de operación de la red sólo se puede aumentar nuevos puntos de acceso o instalar una mayor cantidad de repetidores (“Introducción a las redes inalámbricas.pdf”, s/f, p. 20).

2.3.2 SEGURIDAD DE LAS REDES INALÁMBRICAS.

ESTANDARES DE SEGURIDAD DE LAS REDES INALÁMBRICAS.

Los estándares de redes son normas definidas que facilitan la interoperabilidad de componentes con características similares o diferentes. Estos estándares realizan algunas operaciones que ofrecen como garantía la calidad y seguridad de la funcionalidad, sin importar el dispositivo que la implementa ni la manera de cómo está construido. Estos estándares ya se encuentran originados por algunos organismos internacionales involucrados en el área de Telecomunicaciones, algunos de ellos son: Unión Internacional de Telecomunicaciones (UIT), Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) (Chen, Nixon, & Mok, 2010,p.12).

LISTA DE ESTANDARES DE REDES INALÁMBRICOS:

- 802.11b.- Transmite a 2.4 GHz, envía datos de hasta 11 Mbps utilizando la modulación de espectro ensanchado de secuencia directa. Cuenta con un rango de 100 -150 pies
- 802.11a.- Transmite a 5 GHz y envía datos de hasta 54 Mbps usando la multiplexación de división de frecuencia ortogonal (OFDM). Rango de 50-75 pies. No interoperable es 802.11b.
- 802.11g.- combina característica de ambos estándares (a, b), 2.4 GHz frecuencia, 54 Mbps de velocidad, rango de 100-150 pies y es interoperable con 802.11b.
- 802.11i.- mejora el cifrado WEP al implementar Wi-Fi Protected Access (WPA2). Este utiliza un cifrado de datos utilizando una encriptación llamada Advanced Encryption Standard (AES).
- 802.11n.- 600 Mbps al agregar la entrada múltiple de entrada múltiple (MIMO) y la vinculación de canal / operación de 40 MHz a la capa física (PHY), y la agregación de cuadros a la capa MAC. 802.11n usa WPA y WPA2 para proteger la red (Sheetal Joseph, 2008, p. 4).

IEEE 802.11.

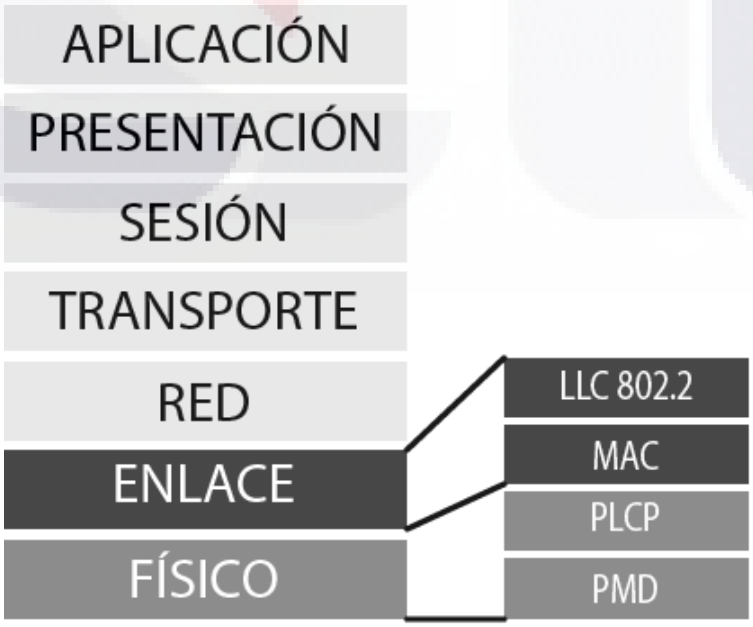
El estándar IEE802.11fue creado en 1997 con la finalidad de proporcionar acceso inalámbrico a las redes de área local (LAN). Este estándar se enfoca en los 2 niveles inferiores del modelo llamado “OSI”, los cuales son: la capa de enlace de datos y la capa física, *mostrados en la Figura 2.*

OSI (Modelo de Interconexión de Sistemas Abiertos).

El modelo OSI es un marco utilizado para comprender la manera en la que transita la información a través de una red informática. De igual manera, el modelo OSI es utilizado para para representar información viajando a través un medio de transporte entre distintos dispositivos(Las siete capas del modelo OSI “Definición de las siete capas del modelo OSI y explicación de las funciones”, s/f, p. 1).

El modelo OSI se encuentra constituido por siete capas. A continuación de describe de manera gráfica cada una de ellas, empezando por la más baja en la jerarquía (la física) y siguiendo hacia la más alta (la aplicación). Las capas se apilan de esta forma:

Figura 2. Capas de modelo OSI (Fuente: Chen, Nixon & Mok, 2010).



Dentro del estándar 802.11, la capa física está dividida en 2 subcapas, las cuales son PMD y PLCP. PMD *(Physical Medium Dependant)* está encargada ed modular y aplicar técnicas de espectro ensanchado de la señal. De las técnicas de espectro ensanchado disponibles es utilizada la de secuencia directa *(DSSS, Direct Sequence Spread Spectrum)* y en vez de *(FHSS, Frecuency Hopping Spread Spectum)* debido a falta de cumplimiento en las regulaciones establecidas por la comisión federal de comunicaciones FCC *(Federal Communications Comision).* PLCP *(Physical Layer Convergent Procedure)* se encarga de acondicionar las tramas que provienen de la capa MAC para su envío a través del medio radio, añadiéndoles un preámbulo y una cabecera. En la Tabla 1 se muestra detalladamente cada una de las características descritas de los estándares:

Tabla 1. Características técnicas de la familia de estándares IEEE 802.11

	802.11b	802.11g	802.11a	802.11n
Estándar Aprobado	Si	Si	Si	Si
Canales sin Solapamiento.	3	3	23	23
Banda de Frecuencia de Operación	2.4 Ghz	2.4 Ghz	5 Ghz	2.4 Ghz , 5 Ghz
Máxima Taza de transferencia.	11Mbps	54Mbps	54Mbps	600Mbps
Fuentes de Interferencia.	Bluetooth, monitores de bebé, hornos microondas, transmisores de video.	Bluetooth, monitores de bebé, hornos microondas, transmisores de video.	Teléfonos inalámbricos, transmisores de video.	Los mismos que 802,11b/g a 2.4GHz. Los mismos que 802.11a a 5GHz.

VECTORES DE ATAQUE Y VULNERABILIDADES EN LAS REDES INALÁMBRICAS.

Si bien la tecnología WLAN ofrece muchos beneficios, el hecho de que utilice el aire como medio para la transmisión de datos representa en realidad un riesgo de seguridad importante, ya que este medio hace que la red sea vulnerable a una variedad de ataques.

- **War Driving.** Es una forma de obtener acceso no autorizado a una red inalámbrica, sin utilizar ningún software o conocimiento sofisticado. El atacante maneja con una computadora portátil, o incluso una PDA, y busca un punto de acceso inalámbrico sin protección(Lopez, Roman, & Alcaraz, 2009, p. 292).

- **Eavesdropping.** Por naturaleza, el equipo WLAN usa el aire como medio para transferir tráfico de red. Lamentablemente, los terceros pueden interceptar los datos generados en el aire. Usando herramientas simples de monitoreo disponibles para descargar desde Internet, un atacante puede fácilmente "olfatear" el tráfico de la red y obtener acceso no autorizado a su red y a una compañía importante.

- **Man in the middle.** En un ataque de hombre en el medio, el atacante se ubica entre una estación inalámbrica y un punto de acceso inalámbrico, y utiliza una aplicación inteligente para presentarse como un punto de acceso autorizado a la estación inalámbrica, y como una estación inalámbrica autorizada para el punto de acceso inalámbrico. El atacante puede capturar paquetes transmitidos y reúna información valiosa sobre sus recursos de red (Lopez et al., 2009, p. 293).

- **Spoofing.** es un tipo común de vulnerabilidad sobre una red inalámbrica, y requiere muy poco esfuerzo o conocimiento del atacante. Un atacante puede suplantar un punto de acceso inalámbrico de las siguientes maneras:

- El atacante configura su punto de acceso para enmascararse como un punto de acceso autorizado. Para determinar el SSID del proveedor predeterminado, el atacante puede simplemente buscar puntos de acceso cuyos SSID contengan frases como "Predeterminado".
- Una vez que el atacante ha falsificado el punto de acceso autorizado, las estaciones inalámbricas se conectan al punto de acceso del atacante, lo que permite al atacante acceder a la información que contienen.
- El atacante transmite paquetes falsos, usando la dirección IP y / o la dirección MAC de una estación inalámbrica legítima.

- **Denial of service and RF signal jamming (DoS Attack).** El objetivo de un ataque de denegación de servicio (DoS) es hacer que el punto de acceso seleccionado sea inaccesible o inutilizable para las estaciones inalámbricas. Un atacante puede lanzar un ataque DoS de las siguientes maneras:

  - El atacante puede inundar el punto de acceso inalámbrico con flujos de datos sin sentido de información, o con un número extremadamente grande de solicitudes, haciendo que el punto de acceso inalámbrico deje de responder.
  - El atacante puede bloquear la señal de RF (Radio Frecuencia) del punto de acceso inalámbrico, mediante el uso de transmisores potentes en el área del equipo inalámbrico para transmitir en la misma frecuencia que el punto de acceso inalámbrico (generalmente 2.4 GHz).
  - La interferencia de señales de RF también puede ser causada por factores ambientales, como dispositivos eléctricos (por ejemplo, teléfonos inalámbricos y microondas), dispositivos que

usan espectro de ancho de banda ilegal en el área o incluso otros puntos de acceso inalámbrico transmitiendo en la misma frecuencia(Lopez et al., 2009, p. 294).

2.3.3 TENDENCIAS DE VULNERABILIDADES EN LOS ULTIMOS 3 AÑOS.

DESCRIPCIÓN.

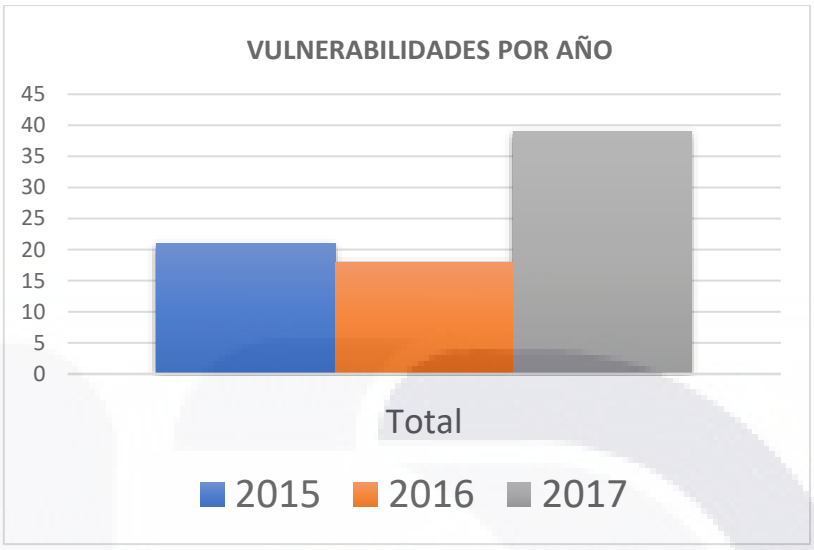
Aunado a todo mostrado en el punto 3.5, desafortunadamente todos estos usuarios que tienen acceso al servicio, pueden sufrir de distintas eventualidades dentro de la red, que se basan en las distintas vulnerabilidades que pueden generar esas eventualidades, como se muestra en la Tabla 2.

Tabla 2. Vulnerabilidades de Seguridad de los últimos 3 años (Fuente: Clay Keller & Serkan Özkan, s/f).

Year	DoS	Code Execution	Overflow	Sql Injection	XSS (Scripting)	Directory Traversal	Bypass something	Gain Information	Gain Privileges	CSRF	Total
2015	1	2	1		11		1	4	1		21
2016		2	1		8	1	1	4	1	1	18
2017	1	15		1	12			7	2	1	39

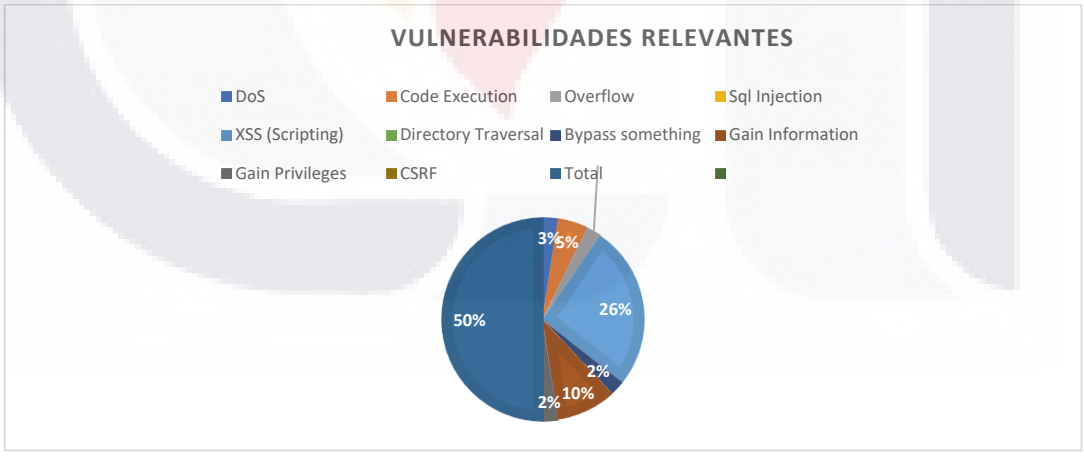
Si nos preguntamos cuales son las tendencias de las vulnerabilidades mostradas en la Tabla 2 de los 3 últimos años, lo mostramos en la Figura 3. Si observamos el crecimiento que se muestra en la gráfica, el año 2017 ha sido el más alto, tomando en cuenta que la tecnología es más utilizada hoy en día, pero también los vectores de ataque son más recurrentes a aprovechar cada una de las vulnerabilidades que van surgiendo.

Figura 3. Vulnerabilidades por año (Fuente: Clay Keller & Serkan Özkan, s/f).



En la gráfica mostrada a continuación en la Figura 4 se ilustran las vulnerabilidades más relevantes y el porcentaje de penetración real, para el robo de la información.

Figura 4. Vulnerabilidades más relevantes (Fuente: Clay Keller & Serkan Özkan, s/f).

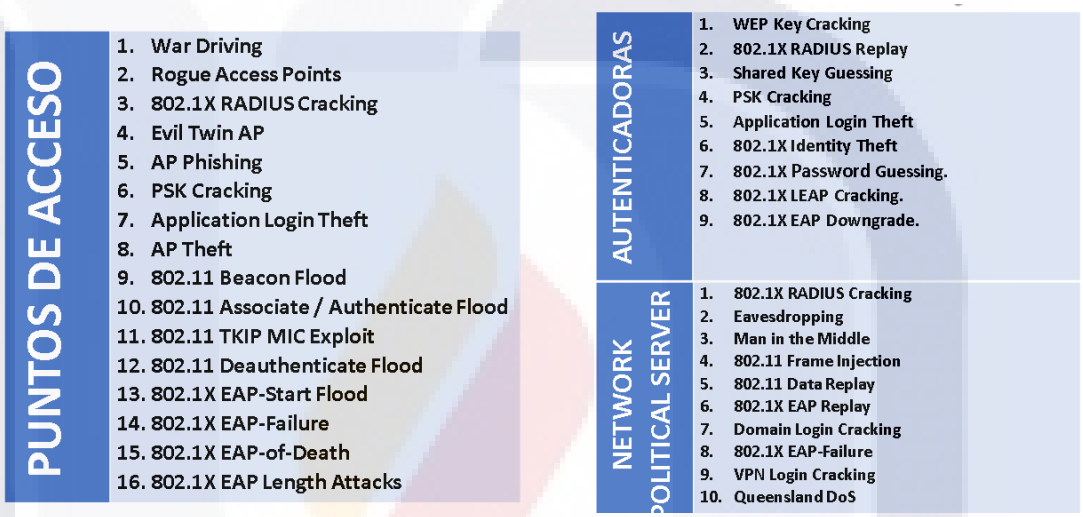


2.3.4 TECNOLOGÍA DE LA RED INALÁMBRICA VS VECTORES DE ATAQUE.

DESCRIPCIÓN.

En la Figura 5 se muestran los vectores de ataque, específicamente los que generan eventualidades en la tecnología de red inalámbrica de Ciudad universitaria.

Figura 5. Tecnología vs Vectores de Ataque (Fuente: Clay Keller & Serkan Özkan, s/f).



2.3.5 TENDENCIA DE VECTORES DE ATAQUE EN LOS ULTIMOS 3 AÑOS.

DESCRIPCIÓN.

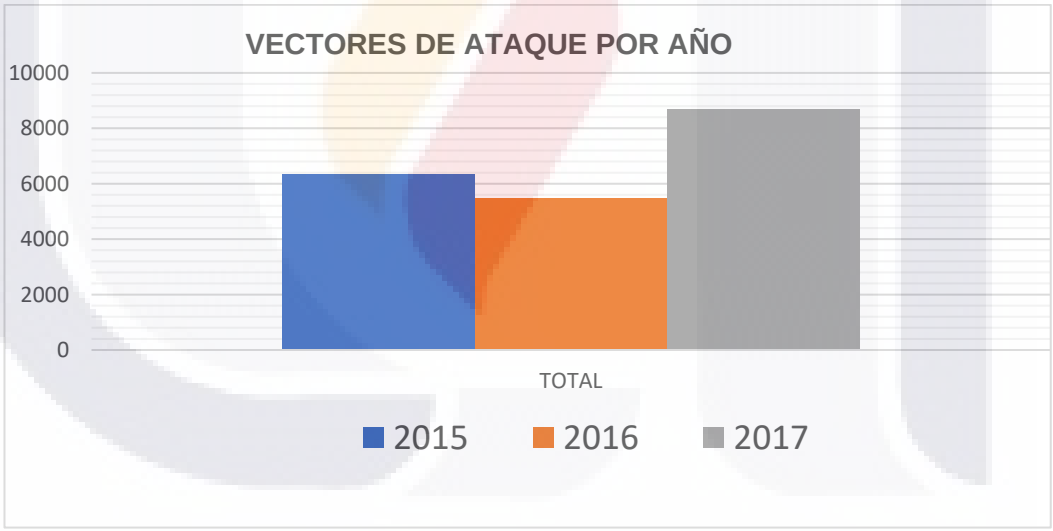
En la Tabla 3 mostrada a continuación y la gráfica de la Figura 6 se describen detalladamente las tendencias de cada uno de los vectores de ataque de los últimos 3 años, por ello se creó la tabla mostrada a continuación.

Tabla 3.Tendencia Vectores de ataque de los últimos 3 años. (Fuente: Clay Keller & Serkan Özkan, s/f).

YEAR	DOS	CODE EXECUTION	MEMORY CORRUPTION	SQL INJECTION	XSS	DIRECTORY TRAVERSAL	HTTP RESPONSE SPLITTING	BYPASS SOMETHING	CSRF	TOTAL
2015	**1792**	**1825**	**749**	**217**	**776**	**149**	**12**	**577**	**248**	6345
2016	**2029**	**1494**	**717**	**94**	**497**	**99**	**15**	**446**	**87**	5478
2017	**2827**	**2575**	**611**	**356**	**1274**	**238**	**9**	**513**	**294**	8697

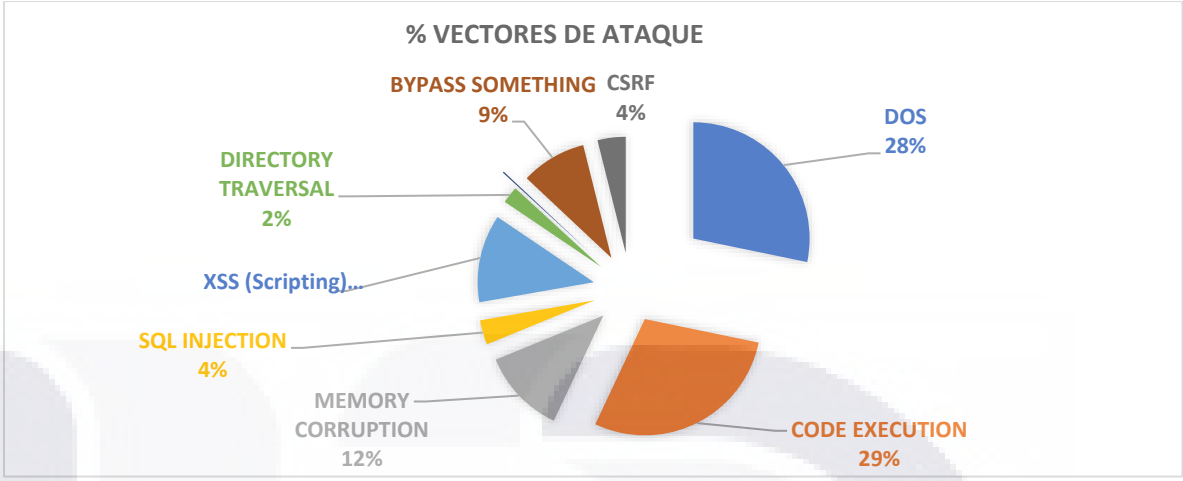
Se logra notar que, en el año 2017 nuevamente es un dato muy alto por encima de los años anteriores.

Figura 6. Vectores de ataque por año (Fuente: Clay Keller & Serkan Özkan, s/f)



En la gráfica mostrada a continuación en la Figura 7, se ilustran los vectores de ataque más representativos y que han generado más problemas en los últimos 3 años.

Figura 7. Porcentaje de los vectores de ataque por año (Fuente: Clay Keller & Serkan Özkan, s/f)



2.3.6 APLICACIONES PARA PRUEBAS EN LAS REDES INALÁMBRICAS.

AIROLIB-NG (DESIGNED TO STORE AND MANAGE ESSID AND PASSWORD LISTS).

DESCRIPCIÓN.

Airolib-ng es una herramienta de suite aircrack-ng de Kali Linux diseñada para almacenar y gestionar listas de essid y contraseñas, calcular sus llaves maestras pairwise (PMK) y usarlas en agrietamiento WPA / WPA2. El programa usa la base de datos liviana SQLite3 como el mecanismo de almacenamiento que está disponible en la mayoría de las plataformas (Airolib-ng Creative Commons, s/f).

El craqueo WPA / WPA2 implica el cálculo de la clave maestra por pares, de la cual se deriva la clave transitoria privada (PTK). Usando el PTK, podemos calcular el código de identidad del mensaje de marco (MIC) para un paquete dado y potencialmente encontrará que el MIC es idéntico al del paquete, por lo que el PTK era correcto, por lo tanto, el PMK también era correcto.

AIRDECAP-NG (DECRYPT WEP/WPA/WPA2 CAPTURE FILES).

DESCRIPCIÓN.

Con el uso de airdecap-ng consigues desencriptar archivos capturados que tengan encriptación WEP/WPA/WPA2. También puede utilizarse para distinguir la cabecera de una captura Wireless sin encriptación(Airdecap-ng Creative Commons, s/f).

PROBLEMAS IDENTIFICADOS.

- Ninguno identificado a la fecha (Airdecap-ng Creative Commons, s/f).

PACKETFORGE-NG (CREATE ENCRYPTED PACKETS THAT CAN SUBSEQUENTLY BE USED FOR INJECTION).

DESCRIPCIÓN.

El propósito principal de packetforge-ng es crear paquetes encriptados que posteriormente puedan usarse para inyección. Puede crear varios tipos de paquetes, como solicitudes de arp, UDP, ICMP y paquetes personalizados. El uso más común es crear solicitudes ARP para inyección posterior.

Para crear un paquete cifrado, debe tener un archivo PRGA (algoritmo de genre pseudoaleatorio). Esto se usa para encriptar el paquete que creas. Esto se obtiene típicamente de aireplay-ng chopchop o ataques de fragmentación (Packetforge-ng Creative Commons, s/f).

2.3.7 METODOLOGÍAS / MARCOS DE TRABAJO.

OWISAM (OPEN WIRELESS SECURITY ASSESSMENT METHODOLOGY).

DEFINICIÓN.

OWISAM es una metodología abierta para el análisis de seguridad Wireless fundada por los hermanos Tarascó presentada en la pasada RootedCon (*conferencia que reúne a todo tipo de gente del sector de la Seguridad Informática),* para que todo aquel que estuviera interesado colaborase editando sus páginas y contribuyendo con ideas. Es un concepto similar a OWASP (*proyecto abierto de seguridad en aplicaciones web*), donde se describen controles técnicos a bajo nivel, herramientas y procedimientos para el análisis informático. Entre los apartados que contienen algunos muy interesantes, ejemplo el top 10 de riesgos descritos en la Tabla 4 mostrada a continuación:

Tabla 4. Top 10 Riesgos OWISAM.

#	Código	Tipo de control	Descripción de los controles
1	OWISAM-DI	Descubrimiento de dispositivos	Recopilación de información sobre las redes inalámbricas
2	OWISAM-FP	Fingerprinting	Análisis de las funcionalidades de los dispositivos de comunicaciones.
3	OWISAM-AU	Pruebas sobre la autenticación	Análisis de los mecanismos de autenticación
4	OWISAM-CP	Cifrado de las comunicaciones	Análisis de los mecanismos de cifrado de información
5	OWISAM-CF	Configuración de la plataforma	Verificación de la configuración de las redes
6	OWISAM-IF	Pruebas de infraestructura	Controles de seguridad sobre la infraestructura Wireless
7	OWISAM-DS	Pruebas de denegación de servicio	Controles orientados a verificar la disponibilidad del entorno
8	OWISAM-GD	Pruebas sobre directivas y normativa	Análisis de aspectos normativos que aplican al uso de las redes de Wi-Fi
9	OWISAM-CT	Pruebas sobre los clientes inalámbricos	Ataques contra clientes inalámbricos
10	OWISAM-HS	Pruebas sobre hostspots y portales cautivos	Debilidades que afectan al uso de portales cautivos.

En Latinoamérica existen gran variedad de personas que han desarrollado herramientas para el apoyo a la mejora de la seguridad como: wireless y su wifislax, donde salen a relucir temas relacionados con OWISAM. Todo el mundo se beneficia en estos casos, los auditores podrán saber qué y cómo identificar puntos rojos de seguridad en una auditoría, tomando como referencia estas tecnologías que se han mencionado (Andres Tarasco & Miguel Tarasco, s/f).

OWASP (PROYECTO ABIERTO DE SEGURIDAD EN APLICACIONES WEB).

DEFINICIÓN

OWASP es una comunidad abierta dedicada a habilitar a las organizaciones para desarrollar, comprar y mantener aplicaciones confiables. Todas las herramientas, documentos, foros y capítulos de OWASP son gratuitos y abierto a cualquiera interesado en mejorar la seguridad de aplicaciones. Abogamos por resolver la seguridad de aplicaciones como un problema de gente, procesos y tecnología porque las soluciones más efectivas incluyen mejoras en todas estas áreas (Andrew van der Stock, Brian Glas, Neil Smithline, & Tosten Gigler, s/f, p. 4).

OWASP es un nuevo tipo de organización. Nuestra libertad de presiones comerciales nos permite proveer información sobre seguridad en aplicaciones sin sesgos, práctica y efectiva. OWASP no está afiliada a ninguna compañía de tecnología, aunque soportamos el uso informado de tecnologías de seguridad comerciales. Parecido a muchos proyectos de software de código abierto, OWASP produce muchos materiales en una manera abierta y colaborativa. La Fundación OWASP es una entidad sin ánimo de lucro para asegurar el éxito a largo plazo del proyecto.

ESTRUCTURA

La fundación OWASP es una entidad sin ánimo de lucro 501(c)(3) que provee la infraestructura para la Comunidad OWASP. La fundación provee nuestros servidores y ancho de banda, instalaciones del proyecto y los capítulos, y administra las Conferencias OWASP AppSec mundiales (Andrew van der Stock et al., s/f, p. 4)..

ITIL (BIBLIOTECA DE INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN).

DEFINICIÓN.

ITIL, es un marco de trabajo de las mejores prácticas desarrollado con el propósito de facilitar la entrega de servicios de tecnologías de la información (TI) de alta calidad. El marco de trabajo ITIL abrevia un extenso conjunto de procedimientos de gestión pensados para ayudar a las organizaciones a alcanzar eficacia y validez en las operaciones de TI (Tecnologías de Información). Estos procedimientos son independientes del proveedor y han sido desarrollados para servir de guía para que tome en cuenta toda infraestructura, personal y operaciones de TI (*ITIL Service Design*, s/f, p. 15).

Aunque fue desarrollado entre los años 1980, ITIL no fue ampliamente adoptada hasta mediados de los años 1990. ITIL se considera a menudo junto con otros marcos de trabajo de mejores prácticas como:

- ISPL (Information Services Procurement Library).
- ASL (Application Services Library).
- DSDM (Dynamic Systems Development Method).
- CMM/CMMI (Modelo de Capacidad y Madurez).

Todo esto a menudo se relaciona con la gobernanza de tecnologías de la información utilizada en COBIT (Control Objectives for Information and related Technology).

ITIL contiene una sección titulada “Gestión de Servicios de TI” (la combinación de los apartados de Servicio de Soporte y Prestación de Servicios, que son un ejemplo específico de un marco ITSM), pero sin embargo es importante señalar que existen otros marcos parecidos. La Gestión de Servicio ITIL está actualmente integrado en el estándar ISO 20000.

ITIL se construye en torno a una vista basada en proceso-modelo del control y gestión de las operaciones que es atribuida a W. Edwards Deming. Las recomendaciones de ITIL fueron desarrolladas en los años 1980 por la CCTA (Central Computer and Telecommunications Agency) del gobierno británico como respuesta a la creciente dependencia de las tecnologías de la información y al reconocimiento de que sin prácticas estándar, los contratos de las agencias estatales y del sector privado creaban independientemente sus propias prácticas de gestión de TI y duplicaban esfuerzos dentro de sus proyectos TIC, lo que resultaba en errores comunes y mayores costes (*ITIL Service Design*, s/f, p. 23).

ITIL fue desarrollada observar que las organizaciones dependen cada vez más de las TI para alcanzar sus objetivos corporativos. Esta dependencia en aumento ha dado como resultado una necesidad creciente de servicios TI de calidad que se correspondan con los objetivos del negocio, y que satisfaga los requisitos y las expectativas del cliente. A través de los años, el énfasis pasó de estar sobre el desarrollo de las aplicaciones TI a la gestión de servicios TI (*ITIL Service Design*, s/f, p. 24).

3 MARCO METODOLÓGICO.

3.1 METODOLOGÍA DE INVESTIGACIÓN.

El objetivo principal del desarrollo y uso de esta metodología es identificar y analizar el significado de los datos recaudados del objeto de estudio, todo esto con el propósito de guiar a una investigación de trabajo practico que a partir de eso localizar, exponer, impugnar y aportar un conocimiento. La principal

cualidad que la distingue es a partir de lo recaudado, seleccionar diferentes datos, agruparlos de una manera adecuada y conseguir información que apoye a la adquisición de conocimiento.

Los métodos que fueron utilizados en este trabajo practico de investigación fueron: la realización de análisis del estado actual del objeto de estudio, elaboración y aplicación de cuestionarios a una muestra de 211 usuarios en ciudad universitaria (campus central) de manera aleatoria y elaboración de entrevistas con personal encargado de gestionar el servicio de red inalámbrica de ciudad universitaria, todo esto con la finalidad de obtener información tangible y de valor para el desarrollo de este trabajo práctico.

TÉCNICAS UTILIZADAS.

En el desarrollo del trabajo practico de investigación se implementaron técnicas tales como entrevistas de manera personal dirigidas a los encargados de cada proceso del departamento de Redes y Telecomunicaciones de la Universidad Autónoma de Aguascalientes.

INSTRUMENTOS UTILIZADOS.

Después de seleccionar las metodologías que se utilizaron para el desarrollo de la propuesta de buenas prácticas en el servicio de red inalámbrica en ciudad universitaria (campus central). Se elaboraron instrumentos como: cuestionarios para la correcta aplicación e implementación del trabajo, así como también la ejecución de entrevistas que permitieron la recolección de información adicional del área de Redes y Telecomunicaciones.

3.2 TIPO DE INVESTIGACIÓN.

DESCRIPCIÓN.

Se requiere conocer que conforma el problema, como limitarlo, en qué dirección va, que incidencia tiene entre sus elementos y hasta dónde puede llegar y terminar. Se establece que el tipo de metodología que se maneja en este proyecto es investigativo con enfoque cuantitativo, ya que se expone la manera

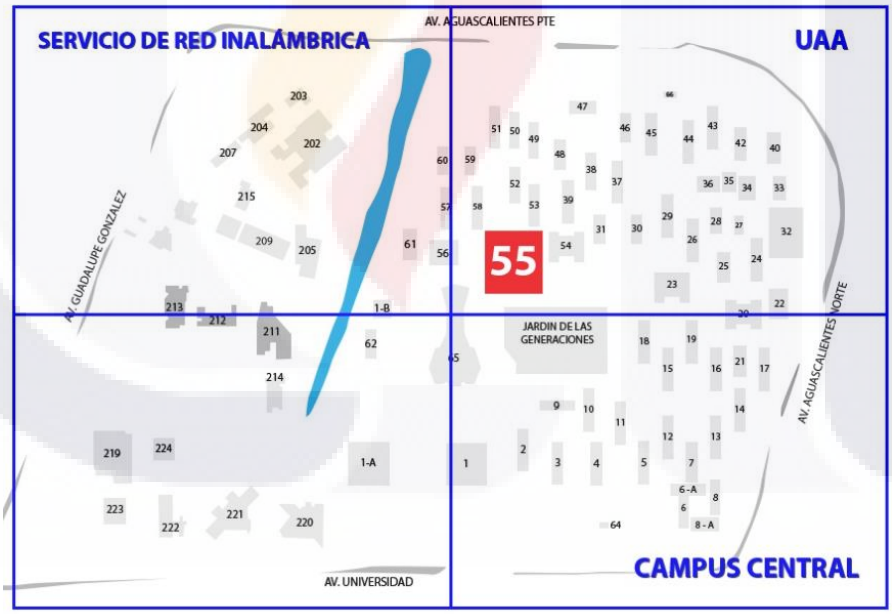
como se va a realizar el estudio, los pasos para realizarlo y su método. Donde es posible hablar de una metodología aplicada a todos los campos, que recoge las pautas presentes en cualquier proceder con el aumento del conocimiento y solución de problemas.

3.3 OBJETO DE ESTUDIO.

DESCRIPCIÓN.

La Universidad Autónoma de Aguascalientes, cuenta con un servicio de Red Inalámbrica, por el cual se logró diseñar un mapa que ilustra la manera en la que se encuentra consolidada la infraestructura que se encarga de brindar el servicio de red inalámbrica, se presenta el siguiente cuadrante. Si se observa la Figura 8, existe un punto de partida que es donde se gestiona todos los accesos a internet y a intranet que son utilizados por los usuarios de campus central.

Figura 8. Servicio General de Red Inalámbrica en Campus Central (Fuente: Propia).



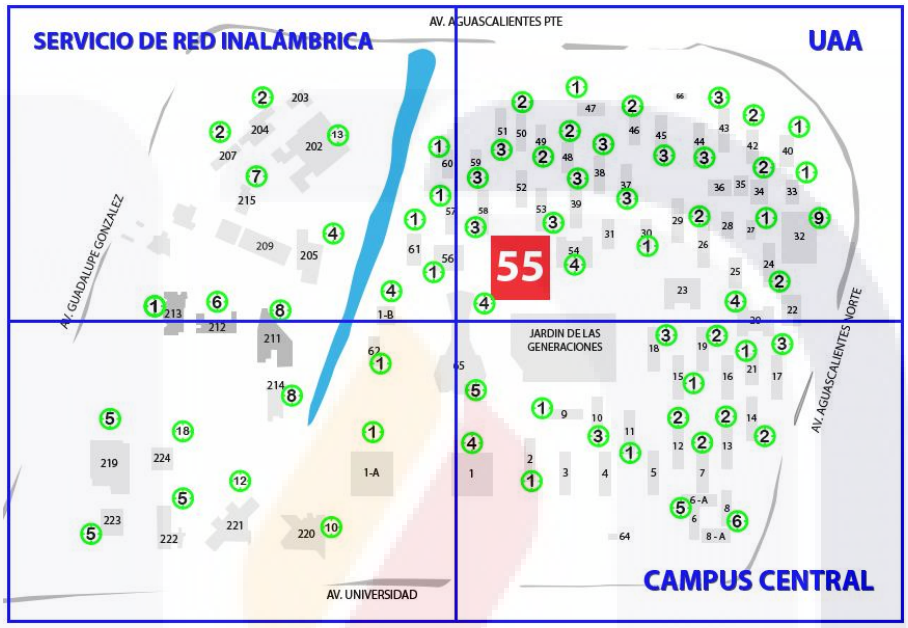
3.4 DISTRIBUCIÓN DEL OBJETO DE ESTUDIO.

DESCRIPCIÓN.

La grafica mostrada a continuación en la Figura 9 describe la distribución general del servicio del objeto de estudio. En este caso cada uno de los puntos

marcados, representa a los dispositivos requeridos para que los usuarios tengan acceso a ese servicio. Donde como ya fue mencionado anteriormente, todo es controlado y gestionado por el EDIFICIO 55, que se muestra en el pequeño cuadrante rojo dentro de la ilustración.

Figura 9. Servicio General de Red Inalámbrica en Campus Central (Fuente Propia).



3.5 TECNOLOGÍA DEL OBJETO DE ESTUDIO.

DESCRIPCIÓN.

Para lograr ofrecer un servicio de red inalámbrica dentro de Ciudad Universitaria (Campus Central), es necesario el uso de tecnología como:

- Autenticadoras.
- Controladoras.
- Switches.
- Puntos de Acceso (Ap's).
- Network Political Server(NPS).
- Protocolos de Seguridad.
- Firewall.
- Enlace a Internet.

3.6 SERVICIOS OFRECIDOS POR EL OBJETO DE ESTUDIO.

La red inalámbrica de ciudad universitaria (campus central), a través La tecnología mostrada y descrita anteriormente se encarga de brindar a los usuarios (alumnos, docentes, administrativos) el acceso a diferentes plataformas o servicios internos (intranet) como lo son:

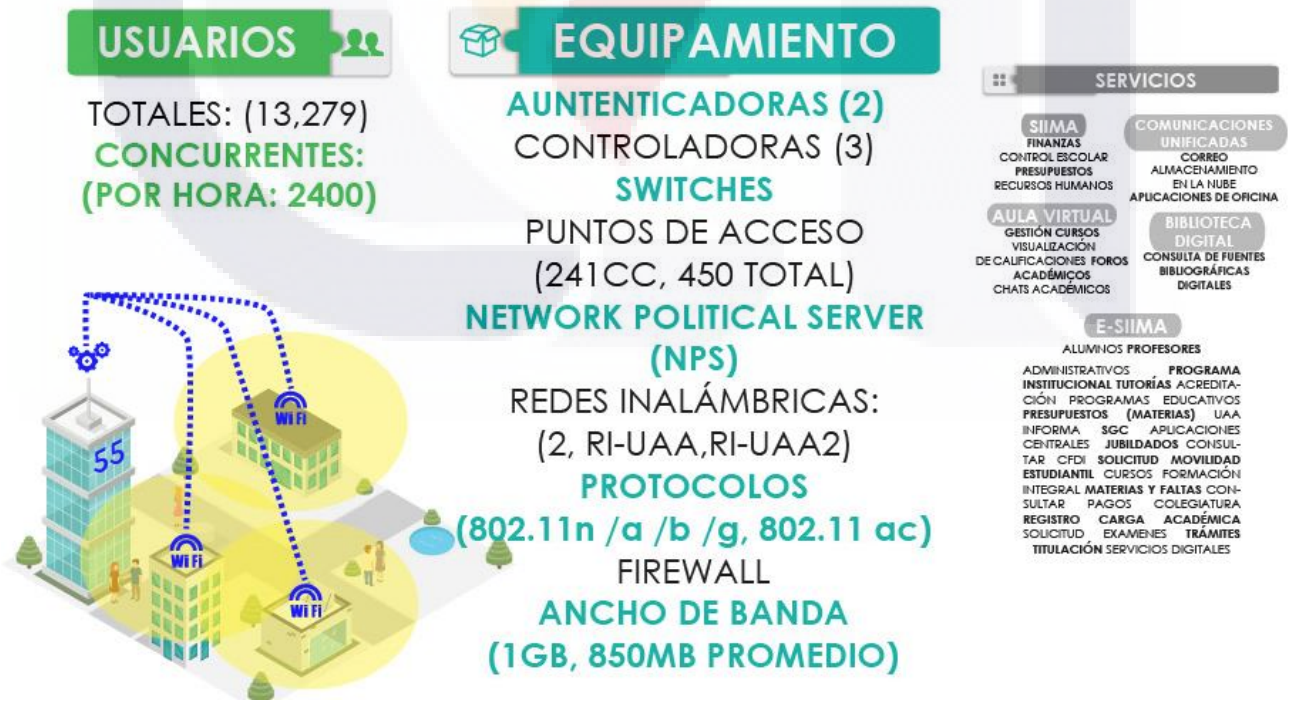
- **SIIMA.**
  - Finanzas.
  - Control Escolar.
  - Presupuestos.
  - Recursos Humanos.
- **AULA VIRTUAL.**
  - Gestión de Cursos.
  - Visualización de calificaciones.
  - Foros Académicos.
  - Chats Académicos.
- **E-SIIMA.**
  - Alumnos.
  - Profesores.
  - Administrativos.
  - Programas institucionales de Tutorías.
  - Acreditación de Programas Educativos.
  - Presupuestos (Materias).
  - UAA Informa.
  - SGC.
  - Aplicaciones Centrales.
  - Jubilados.
  - Consultar CFDI.
  - Solicitud de Movilidad Estudiantil.
  - Cursos de Formación Integral.
  - Materias y Faltas.

- Consultar Pagos de Colegiaturas.
- Registro de Carga Académica.
- Solicitud de Exámenes.
- Tramites de Titulación.
- Servicios Digitales.

- **COMUNICACIONES UNIFICADAS.**
  - Correo.
  - Almacenamiento en la Nube.
  - Aplicaciones de Oficina.
- **BIBLIOTECA DIGITAL.**
  - Consulta de Fuentes Bibliográficas Digitales.

Gracias a estos **servicios** ofrecidos por la Red Inalámbrica más de 13,000 usuarios (tomando en cuenta alumnos, docentes, personal administrativo) pueden tener acceso a ellos, como se muestra en la Figura 10.

Figura 10. Tecnología de la Red Inalámbrica en Campus Central (Fuente: Propia).

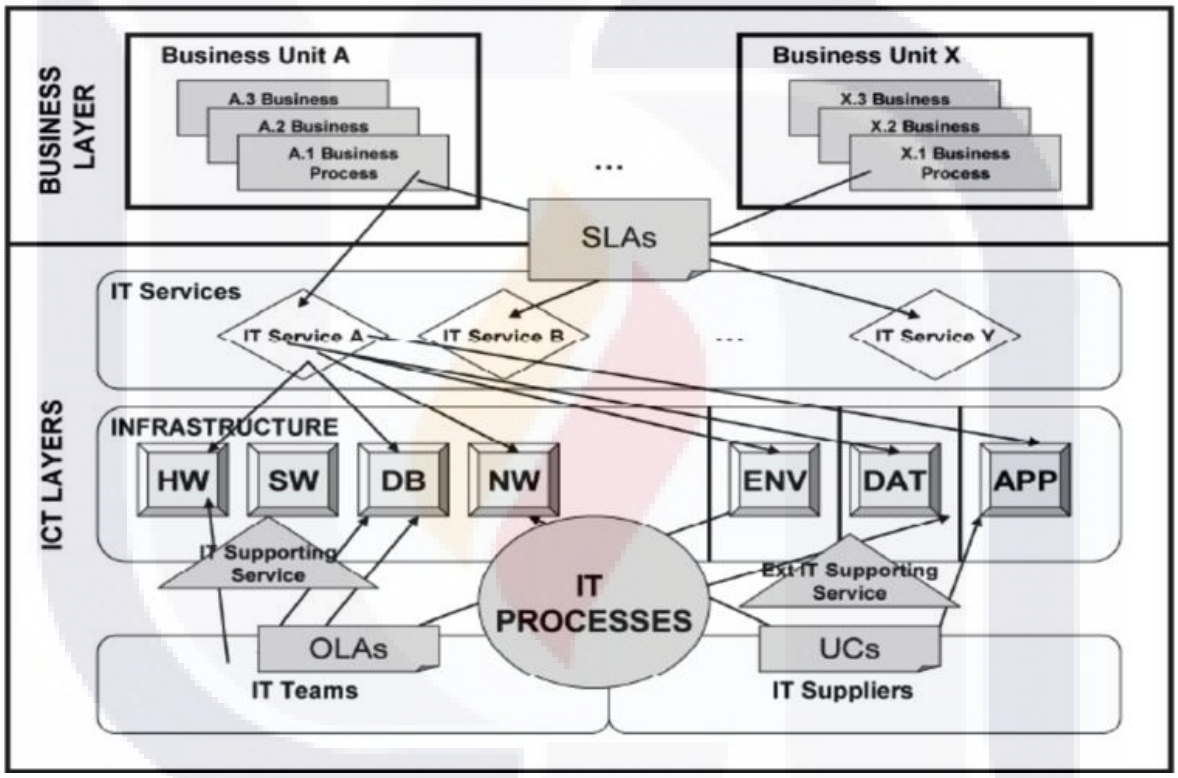


3.7 CAPAS DEL NEGOCIO ITIL.

DESCRIPCIÓN.

Como parte de la investigación realizada, fue necesario identificar y entender la manera en cómo ITIL ve el servicio, ya que es una de las mejores prácticas que existen en la actualizad, mostrado en la Figura 11.

Figura 11. Framework ITIL. (Fuente: Dr. Manuel Mora T).



Para el desarrollo de este trabajo practico, el servicio se encuentra dividido de la siguiente manera:

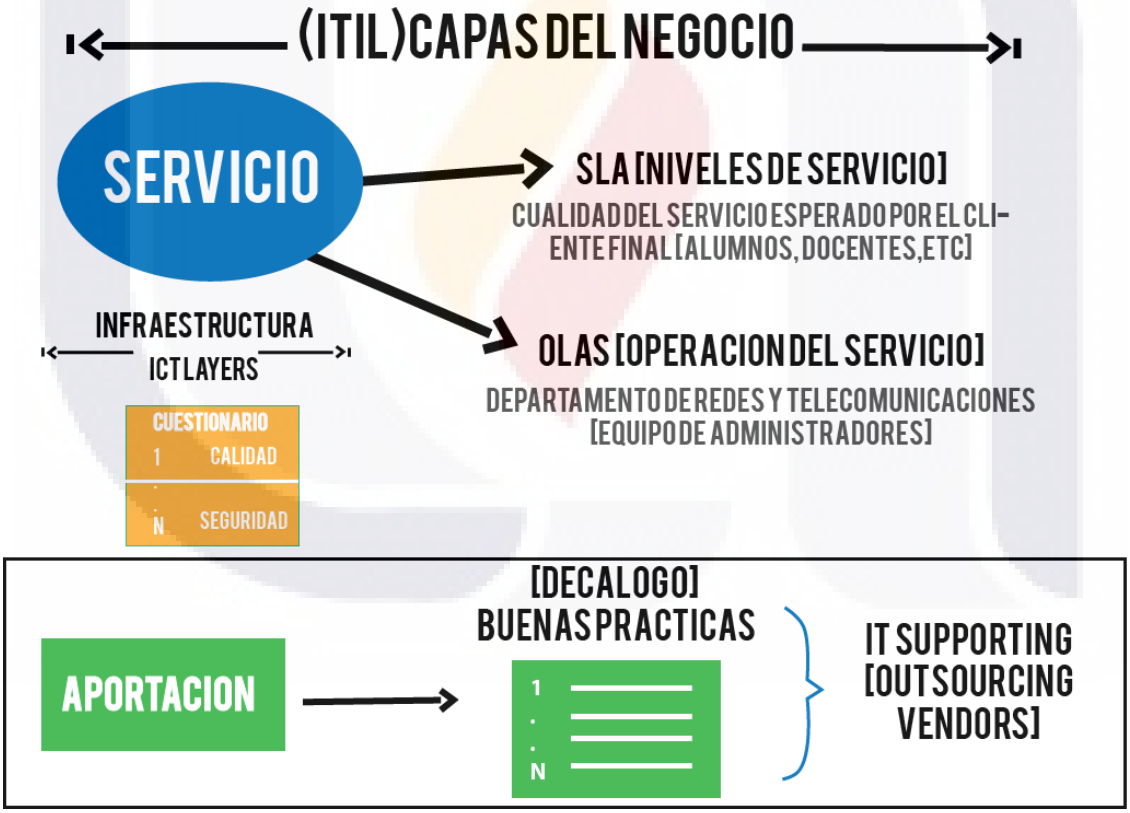
- **SLA** define los Niveles del Servicio basados en la cualidad esperada por el cliente final.

- **OLAS,** hace referencia a toda la operación del servicio, se define observa la forma como se encuentran estructurados los procesos del departamento para orientar y operar el servicio.

De igual manera fue necesaria la aplicación de un cuestionario tomando una muestra de 211 usuarios al azar, donde se realizaron preguntas orientadas al servicio y seguridad tomando en cuenta la satisfacción del cliente.

De lo anterior, la aportación es el desarrollo de un Decálogo de buenas prácticas basadas en seguridad orientadas al servicio, todo esto como se muestra en la Figura 12 de a continuación.

Figura 12. Capas del Negocio (Fuente: Propia).

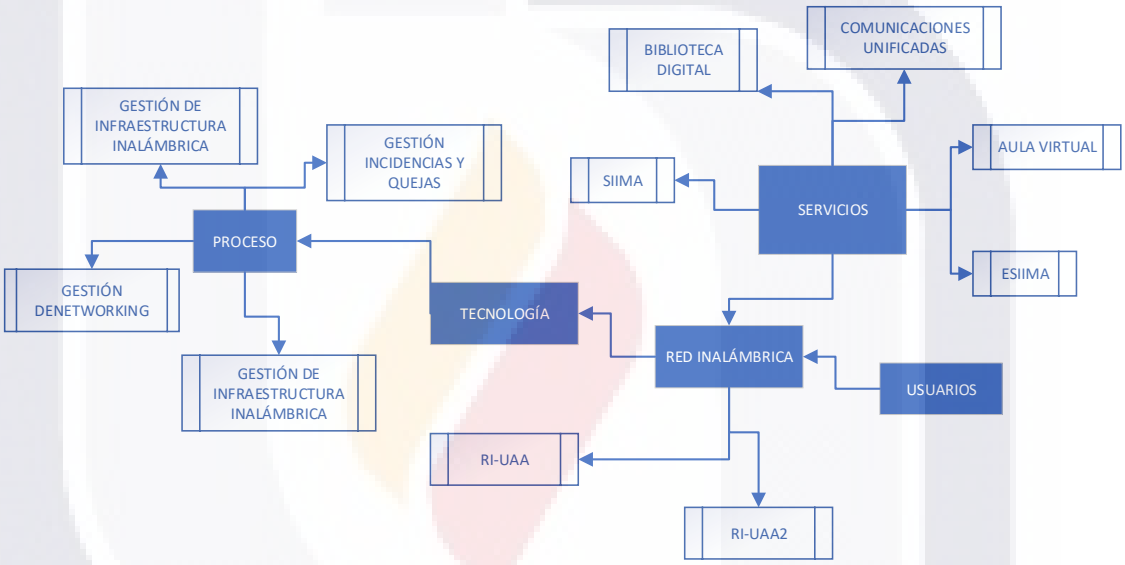


3.8 MODELADO DE PROCESOS.

DESCRIPCIÓN.

Como parte de la documentación realizada, se desarrolló un diagrama utilizando la tecnología UML con el propósito de describir los procesos en un contexto general, mostrado en la Figura 13.

Figura 13. Modelo de Procesos en UML (Fuente: Propia).



Así como también se utilizó un modelo de referencia llamado IDEF, con el propósito de modelar detalladamente cada uno de los procesos importantes del objeto de estudio, mostrados en las figuras: 14, 15, 16 y 17.

Figura 14. Proceso de Gestión de Infraestructura Inalámbrica. (Fuente: Propia).

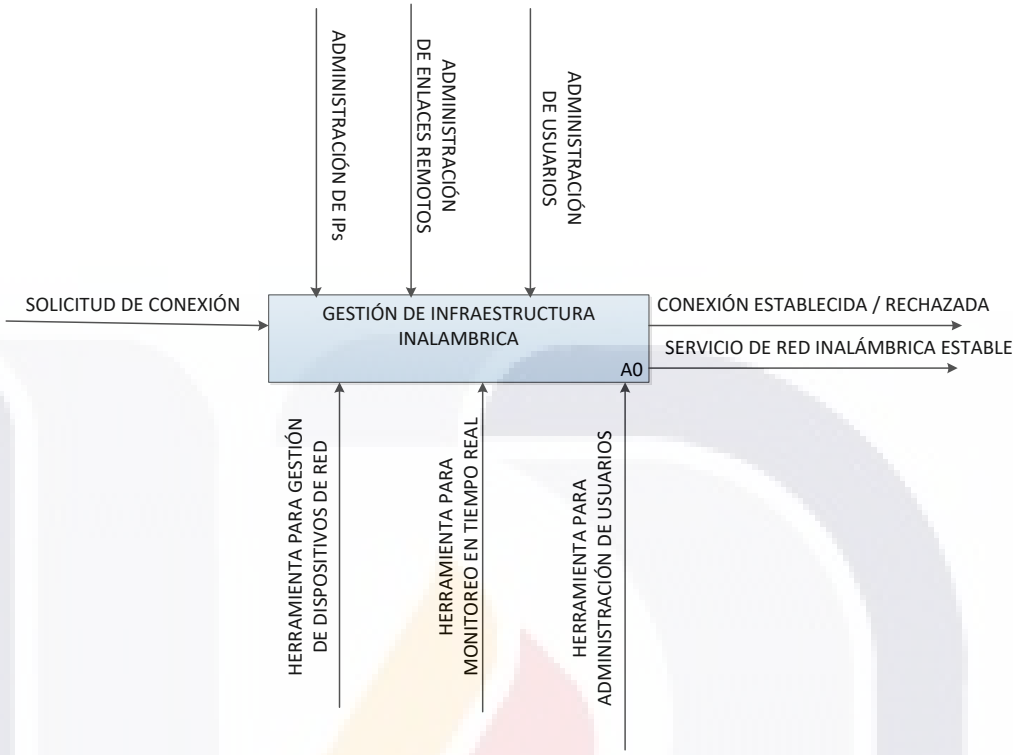


Figura 15. Proceso de Gestión de Networking (Fuente: Propia).

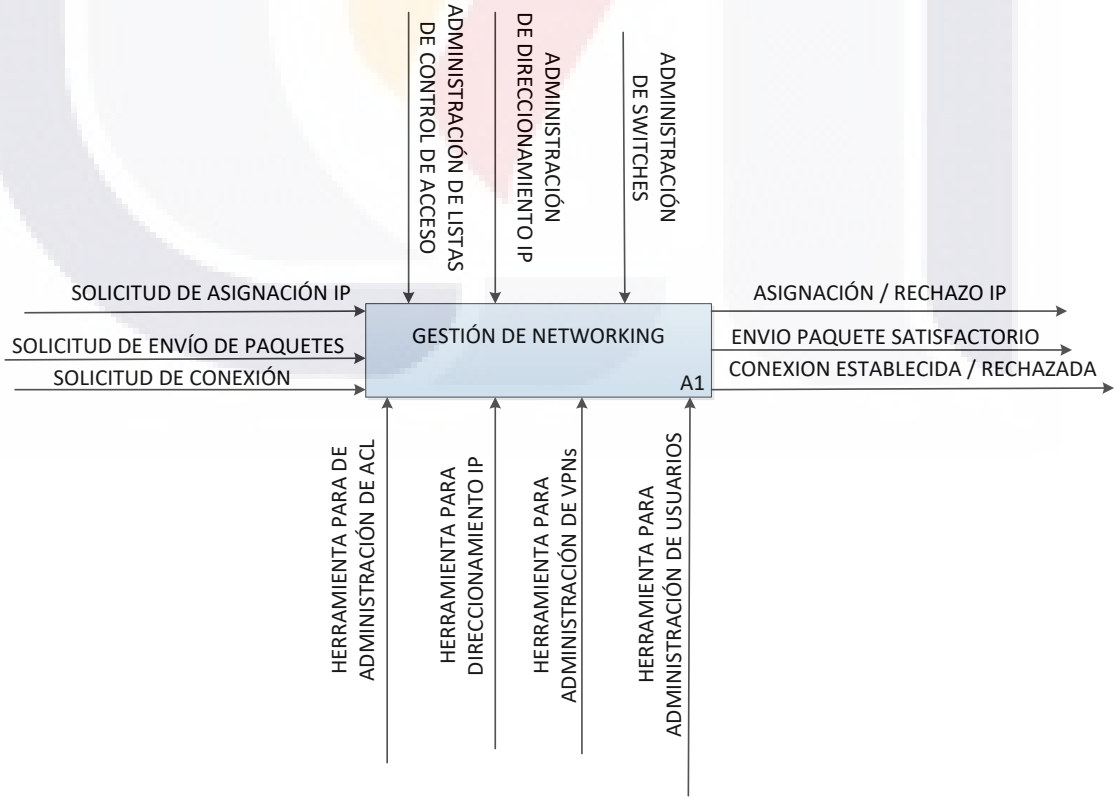


Figura 16. Proceso de Gestión de Firewall (Fuente: Propia).

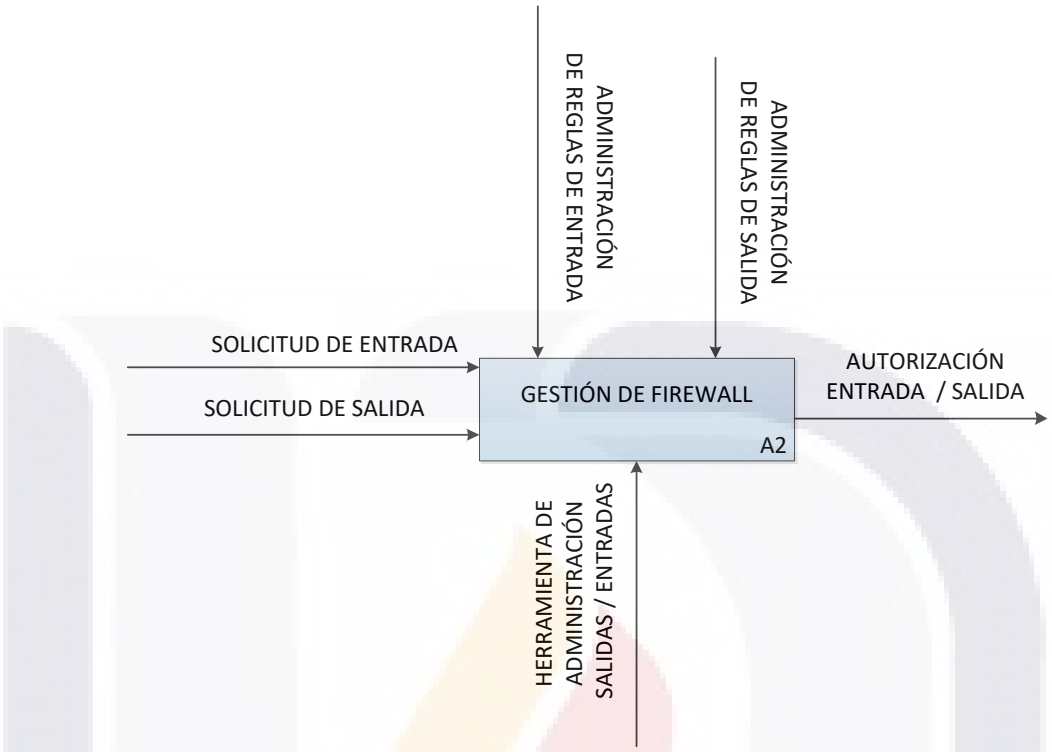
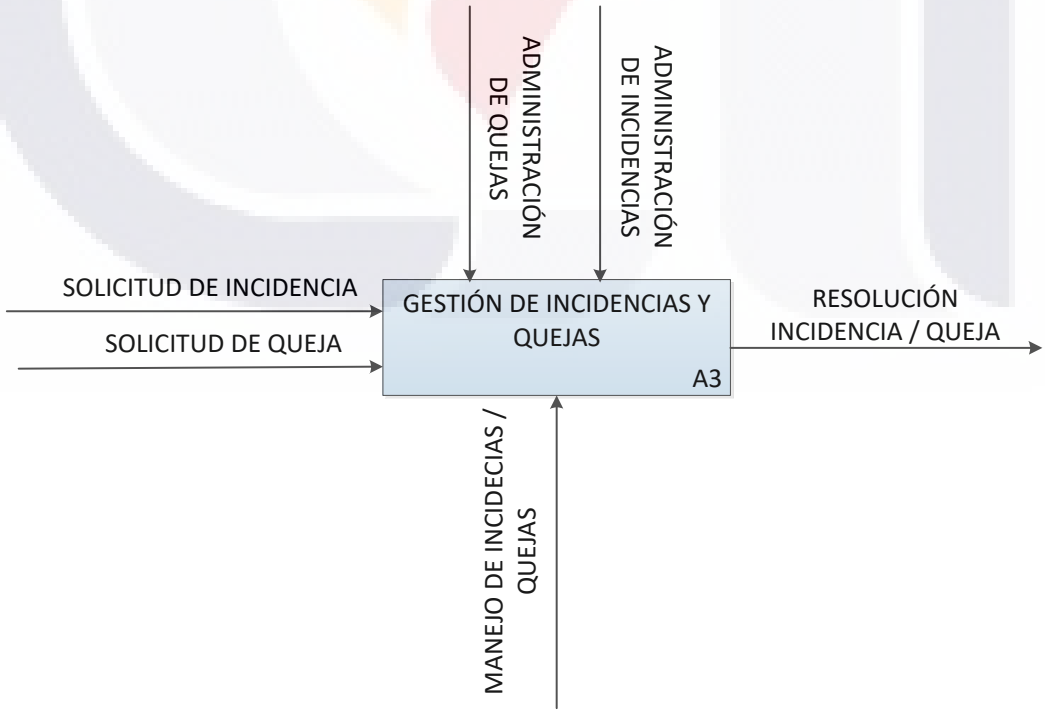


Figura 17. Proceso de Gestión de Incidencias y Quejas (Fuente: Propia).



4 ANALISIS DE DATOS.

DESCRIPCIÓN.

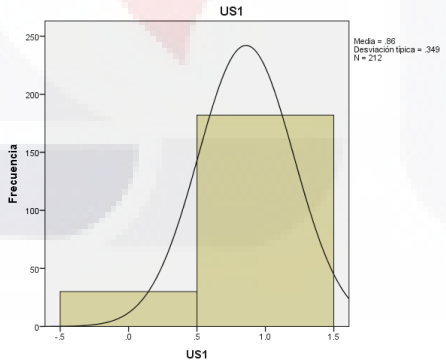
Con la finalidad de recaudar la información requerida para el desarrollo del trabajo practico que lleva por nombre “Propuesta de Implementación de Buenas Prácticas en las Políticas del Servicio de Red inalámbrica en Ciudad universitaria (Campus Central)”, se desarrolló y aplico un cuestionario relacionado al uso y seguridad del servicio de red inalámbrica, a una población de 211 usuarios en campus central, a continuación se muestra de manera gráfica y detallada los resultados de cada pregunta de los cuestionarios aplicados a los usuarios.

US 1. Usted hace uso del servicio de red inalámbrica **durante todos los días de la semana.**

Figura 18. Gráficos US1.

US1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	30	14.2	14.2	14.2
	si	182	85.8	85.8	100.0
	Total	212	100.0	100.0	

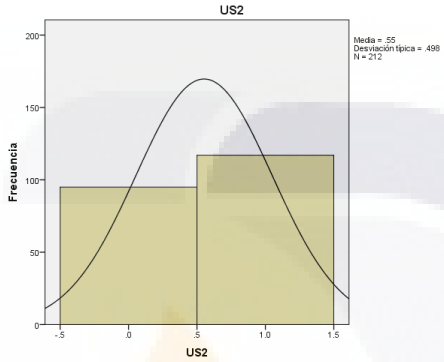


US 2. Usted hace uso del servicio de red inalámbrica **varias veces durante la semana.**

Figura 19. Gráficos US2.

US2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	95	44.8	44.8	44.8
	si	117	55.2	55.2	100.0
	Total	212	100.0	100.0	

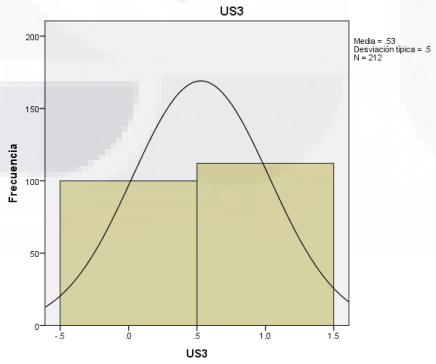


US 3. Usted hace uso del servicio de red inalámbrica **varias veces al mes.**

Figura 20. Gráficos US3.

US3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	100	47.2	47.2	47.2
	si	112	52.8	52.8	100.0
	Total	212	100.0	100.0	

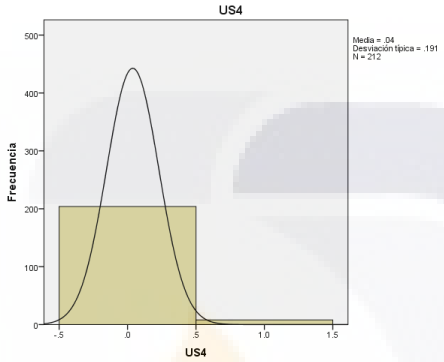


US 4. Usted hace uso del servicio de red inalámbrica **casi nunca.**

Figura 21. Gráficos US4.

US4

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	204	96.2	96.2	96.2
	si	8	3.8	3.8	100.0
	Total	212	100.0	100.0	

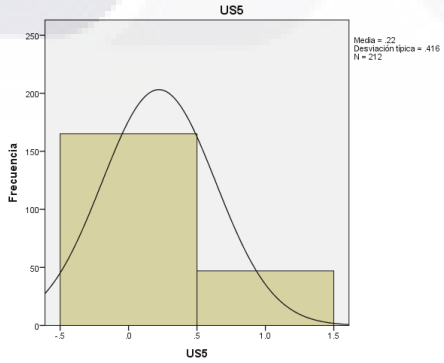


US 5. Usted tiene conocimiento sobre la **información técnica y normativa oficial sobre el uso de la red** inalámbrica de la UAA

Figura 22. Gráficos US5.

US5

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	165	77.8	77.8	77.8
	si	47	22.2	22.2	100.0
	Total	212	100.0	100.0	

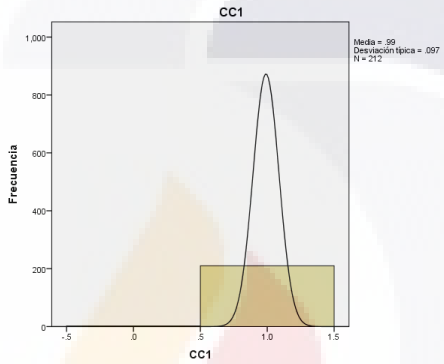


CC 1. Usted utiliza el servicio de red inalámbrica para consultar contenido relacionado con asuntos **académicos.**

Figura 23. Gráficos CC1.

CC1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	2	.9	.9	.9
	si	210	99.1	99.1	100.0
	Total	212	100.0	100.0	

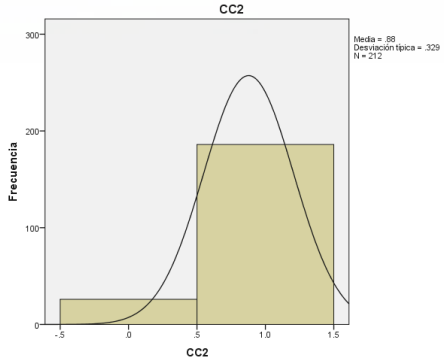


CC 2. Usted utiliza el servicio de red inalámbrica para consultar contenido relacionado con asuntos **informativos, noticias, etc**.

Figura 24. Gráficos CC2.

CC2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	26	12.3	12.3	12.3
	si	186	87.7	87.7	100.0
	Total	212	100.0	100.0	

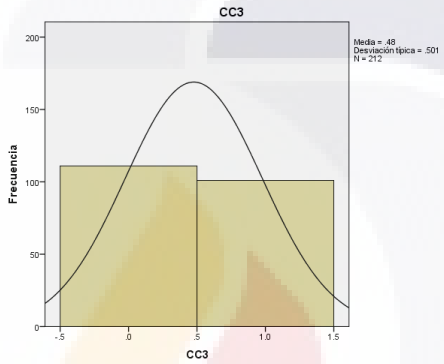


CC 3. Usted utiliza el servicio de red inalámbrica para consultar contenido relacionado con asuntos de **gestión administrativa**

Figura 25. Gráficos CC3.

CC3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	111	52.4	52.4	52.4
	si	101	47.6	47.6	100.0
	Total	212	100.0	100.0	

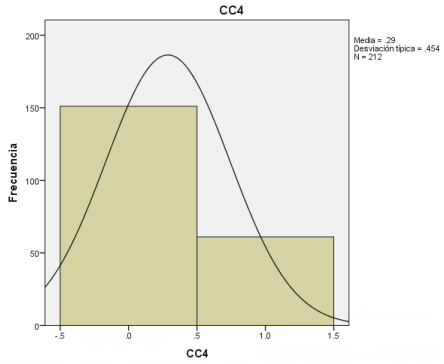


CC 4. Usted utiliza el servicio de red inalámbrica para consultar contenido relacionado **al manejo de información personal (tarjetas bancarias, nombres direcciones, datos sensibles).**

Figura 26. Gráficos CC4.

CC4

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	151	71.2	71.2	71.2
	si	61	28.8	28.8	100.0
	Total	212	100.0	100.0	

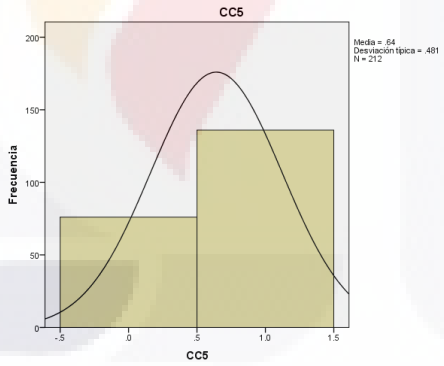


CC 5. Usted utiliza el servicio de red inalámbrica para consultar contenido relacionado **a la visualización de contenido a través de streaming (Spotify, Apple Music, Google Music, Netflix, Twitch, etc).**

Figura 27. Gráficos CC5.

CC5

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	76	35.8	35.8	35.8
	si	136	64.2	64.2	100.0
	Total	212	100.0	100.0	

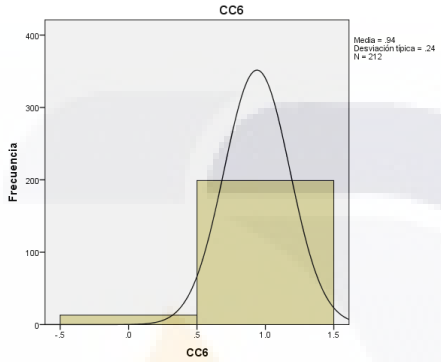


CC 6. Usted utiliza el servicio de red inalámbrica para consultar contenido relacionado **al uso de redes sociales (Facebook, Twitter, Snapchat, Instagram, Tumblr).**

Figura 28. Gráficos CC6.

CC6

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	13	6.1	6.1	6.1
	si	199	93.9	93.9	100.0
	Total	212	100.0	100.0	

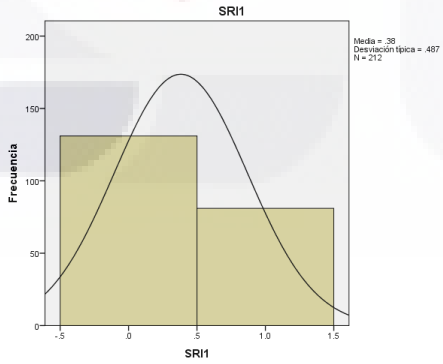


SRI 1. Considera que el tiempo de espera de conexión a internet es el adecuado

Figura 29. Gráficos SRI1.

SRI1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	131	61.8	61.8	61.8
	si	81	38.2	38.2	100.0
	Total	212	100.0	100.0	

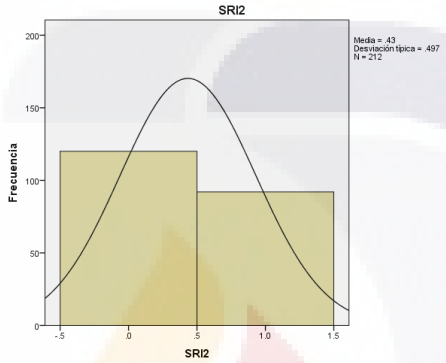


SRI 2. Es fácil conectarse al servicio de red inalámbrica de la UAA.

Figura 30. Gráficos SRI2.

SRI2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	120	56.6	56.6	56.6
	si	92	43.4	43.4	100.0
	Total	212	100.0	100.0	

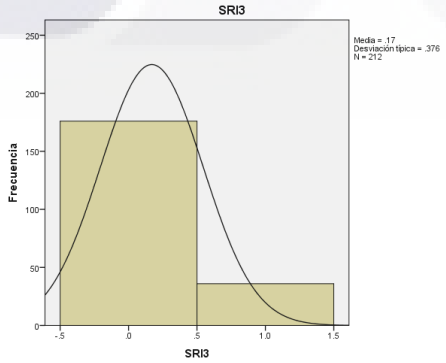


SRI 3. Es posible acceder a cualquier contenido desde la red inalámbrica de la UAA.

Figura 31. Gráficos SRI3.

SRI3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	176	83.0	83.0	83.0
	si	36	17.0	17.0	100.0
	Total	212	100.0	100.0	

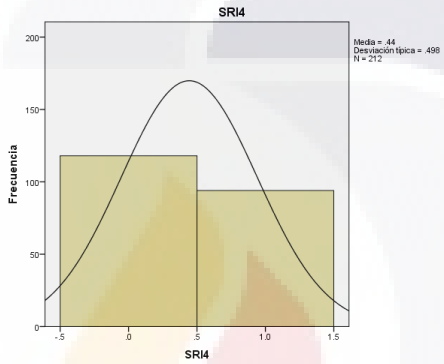


SRI 4. La facilidad de acceder a la red inalámbrica de la UAA hace que usted quiera utilizarla.

Figura 32. Gráficos SRI4.

SRI4

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	118	55.7	55.7	55.7
	si	94	44.3	44.3	100.0
	Total	212	100.0	100.0	

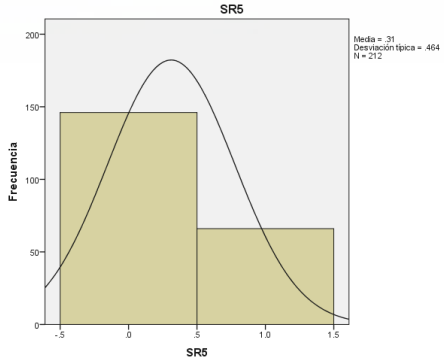


SRI 5. Usted se encuentra satisfecho con el servicio de red inalámbrica de la UAA

Figura 33. Gráficos SRI5.

SR5

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	146	68.9	68.9	68.9
	si	66	31.1	31.1	100.0
	Total	212	100.0	100.0	

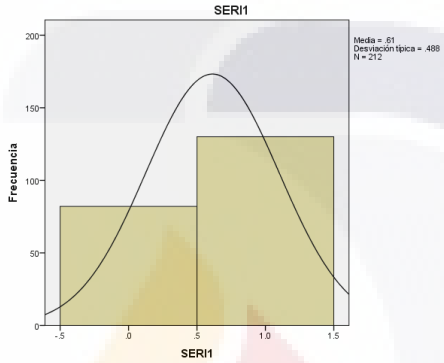


SERI 1. ¿Usted considera que la red inalámbrica de la UAA es segura?

Figura 34. Gráficos SERI1.

SERI1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	82	38.7	38.7	38.7
	si	130	61.3	61.3	100.0
	Total	212	100.0	100.0	

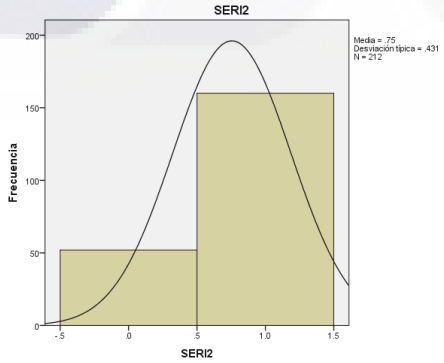


SERI 2. ¿Usted está consciente de los riesgos a los que se expone mientras está conectado en una red inalámbrica publica?

Figura 35. Gráficos SERI2.

SERI2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	52	24.5	24.5	24.5
	si	160	75.5	75.5	100.0
	Total	212	100.0	100.0	

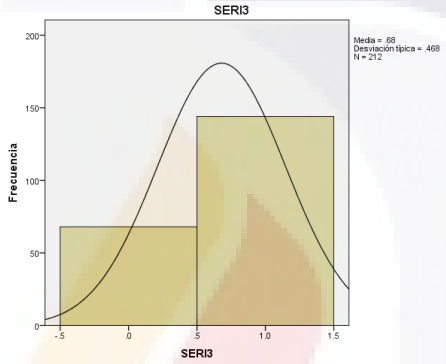


SERI 3. ¿Usted hace uso de contraseñas seguras para el uso de aplicaciones de manejo de información delicada (Banca Móvil, Tarjetas de Crédito, Compras Online, Sistemas Administrativos, Redes Sociales, Cloud personal, etc)?

Figura 36. Gráficos SERI3.

SERI3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	68	32.1	32.1	32.1
	si	144	67.9	67.9	100.0
	Total	212	100.0	100.0	

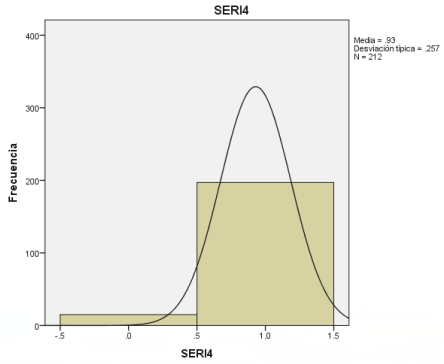


SERI 4. Dentro de sus contraseñas que utiliza en sus aplicaciones mientras está conectado a la red inalámbrica, ¿usted combina entre caracteres especiales, números, mayúsculas y minúsculas?

Figura 37. Gráficos SERI$.

SERI4

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	15	7.1	7.1	7.1
	si	197	92.9	92.9	100.0
	Total	212	100.0	100.0	

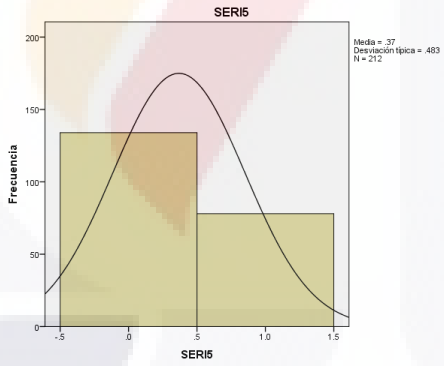


SERI 5. ¿Usted almacena todas las contraseñas en su computadora personal o dispositivo móvil?

Figura 38. Gráficos SERI5.

SERI5

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	134	63.2	63.2	63.2
	si	78	36.8	36.8	100.0
	Total	212	100.0	100.0	

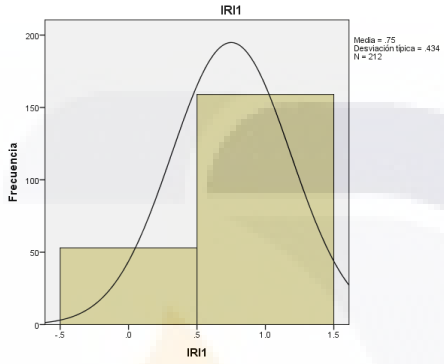


IRI 1. ¿Usted ha tenido alguna incidencia, inconveniente o problema mientras se ha intentado conectar o cuando ya está conectado a la red inalámbrica de la UAA?

Figura 39. Gráficos IRI1.

IRI1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	53	25.0	25.0	25.0
	si	159	75.0	75.0	100.0
	Total	212	100.0	100.0	

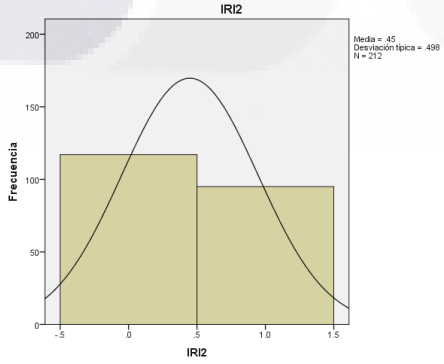


IRI 2. Mientras ha estado conectado a la red inalámbrica de la UAA ¿usted accede de manera regular a sitios (http://www.) que no cuentan con los certificados de seguridad (https://www.)?

Figura 40. Gráficos IRI2.

IRI2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	117	55.2	55.2	55.2
	si	95	44.8	44.8	100.0
	Total	212	100.0	100.0	

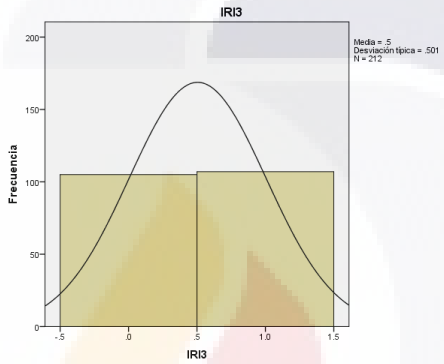


IRI 3. Mientras ha estado conectado a la red inalámbrica de la UAA ¿usted realiza descargas (de software, archivos, música, etc) de sitios no oficiales?

Figura 41. Gráficos IRI3.

IRI3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	105	49.5	49.5	49.5
	si	107	50.5	50.5	100.0
	Total	212	100.0	100.0	

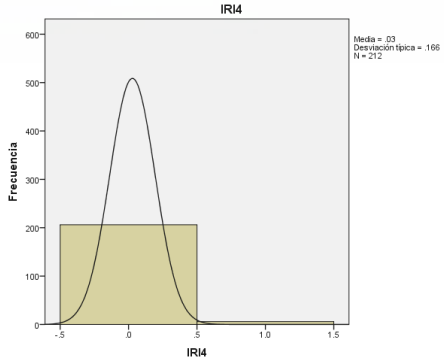


IRI 4. Mientras ha estado conectado a la red inalámbrica de la UAA ¿usted ha sufrido algún robo de información?

Figura 42. Gráficos IRI4.

IRI4

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	no	206	97.2	97.2	97.2
	si	6	2.8	2.8	100.0
	Total	212	100.0	100.0	



5 RESULTADOS.

DEFINICIÓN.

Durante el desarrollo y documentación del trabajo practico, fue necesario seguir un cronograma de actividades a realizar como las siguientes:

- Análisis del contexto actual del objeto de estudio (descrito gráficamente en las Figura 8 y 9). Fue necesario desarrollar un mapa donde se ilustra la manera en la que se encuentra considerada la infraestructura que se encarga de proporcionar el servicio a los usuarios (alumnos, profesores, administrativos). Dentro de este objeto de estudio de describe, la distribución general del servicio y el punto inicial que se encarga de brindarlo a los usuarios.
- Identificación de la problemática inicial realizando diversas entrevistas con el personal encargado de realizar la gestión de todos los procesos inalámbricos de la universidad.
- Descripción detallada de la tecnología utilizada para ofrecer el servicio.
- La definición del objetivo general del desarrollo del desarrollo de la solución.
- Análisis, identificación y uso de herramientas para realización pruebas de penetración a las redes inalámbricas de la universidad.
- Diseño y desarrollo de las capas del negocio basadas en la forma de que la mejor practica (ITIL) ve e interpreta el servicio.
- Diseño y modelado especifico de los procesos actuales del objeto de estudio.
- Aplicación de entrevistas y cuestionarios a los involucrados en los procesos mencionados en el documento.
- Investigación y relación entre la tecnología identificada en el objeto de estudio contra los vectores de ataque que existen actualmente y que podrían afectar en algún momento.

Después de una exhaustiva investigación y todo lo mencionado anteriormente que desarrollado en este trabajo practico, fue definido el siguiente decálogo de buenas prácticas para el objeto de estudio.

DECÁLOGO DE BUENAS PRÁCTICAS.

1. Actualizar el sistema operativo multiusuario para el NPS (Network Political Server).
2. Si actualmente se utiliza un servicio de firewall de un proveedor tercero, es importante tener en cuenta el servicio de asistencia remota que ellos brindan. Todo esto con el propósito de solucionar las dudas o solicitar las actualizaciones pertinentes para cada uno de los dispositivos con los que se cuenta actualmente.
3. Implementar una estrategia que con las herramientas de pentesting que existen actualmente, generen un valor agregado a los mecanismos de detección de vulnerabilidades.
4. Verificar que los usuarios del servicio están entrenados y conocen los riesgos asociados con su utilización.
5. Crear una estrategia para la difusión general de la información técnica y normatividad oficial sobre el uso de la red inalámbrica de la UAA.
6. Realizar las actualizaciones necesarias de todos los parches en S.O., Access Points, Suplicantes, RADIUS, VPN, Firewalls, etc.
7. Evaluación de la red inalámbrica mediante la aplicación de pruebas de penetración (externas e internas) sobre las redes inalámbricas utilizando distintas herramientas que existen en la actualidad como: AirCrack, Metasploit, NMAP, Wiresshark, Netcat, entre otros.

8. Desarrollo de una guía que describa la implementación de de métricas de seguridad en las redes inalámbricas institucionales.

9. Desarrollo de una aplicación de gestión de incidencias específicamente para el servicio de redes inalámbricas.

10. Desarrollar e implementar un plan de capacitación en las nuevas tecnologías utilizadas actualmente que este orientado a la seguridad informática.

6 CONCLUSIONES.

El desarrollo del trabajo practico “Propuesta de Implementación de Buenas Prácticas en las Políticas del Servicio de Red Inalámbrica en Ciudad Universitaria (Campus Central) ha sido muy importante, ya que que para poder llegar a una conclusión concreta fue necesario pasar por diversas etapas de investigación y desarrollo, las cuales apoyaron significativamente a desarrollar y reforzar el contenido de este documento partiendo desde la identificación de un objeto y terminando con la aportación que le da valor al trabajo práctico.

Toda la información que fue recolectada y documentada en base a la metodología seguida durante el proceso de desarrollo, finalización del trabajo practico, nos ayudó a demostrar que existen diferentes tipos de vulnerabilidades y vectores de ataque a los que se encuentran expuestas las redes inalámbricas. El propósito de identificar los vectores de ataque y las tendencias de vulnerabilidades relacionadas a las redes inalámbricas es utilizar buenas y las mejores prácticas para atacar y prevenir esos vectores de ataque.

Este documento es de gran importancia estratégica y operativamente hablando, ya que, gracias a la aportación definida como decálogo final, se aumenta a percepción de seguridad, se reduce el riesgo de ataque y vulnerabilidad para los atacantes.

Tomando en cuenta a todo lo descrito anteriormente, el equipo que se encargó de desarrollar este trabajo, se encuentra a la mejor disposición de seguir

trabajando en conjunto al área involucrada en el trabajo practico, para implementar y mejorar procesos que agreguen mayor valor al área y mejore significativamente su funcionamiento.

LINEAS FUTURAS DE INVESTIGACION.

Tomando en cuenta la aportación mostrada en este documento y partiendo de ahí, existe un parteaguas al desarrollo de trabajos futuros, ya que, gracias al establecimiento de este decálogo de 10 mejores prácticas para el servicio de red inalámbrica, personas interesadas en este tema, podrán hacer una investigación adentrada, partiendo de cualquiera de estos 10 puntos señalados anteriormente.

7 BIBLIOGRAFÍA.

Alma Karina Jimenez Estrada. (s/f). Diseno y Evaluacion de un proceso de gestion de configuraciones de servicios de TI: Caso LABDC-UAA.

Andres Tarasco, & Miguel Tarasco. (s/f). OPEN WIRELES SECURITY ASSESSMENT METHODOLOGY. Recuperado a partir de https://www.owisam.org/es/

Andrew van der Stock, Brian Glas, Neil Smithline, & Tosten Gigler. (s/f). OWASP Top 2017 The Ten Most Critical Web Application Security Risks.

Battiti, R., Cigno, R. L., Sabel, M., Orava, F., & Pehrson, B. (s/f). Wireless LANs: From WarChalking to Open Access Networks. Mobile Networks and Applications, 10(3), 275–287. https://doi.org/10.1007/s11036-005-6422-4

Chen, D., Nixon, M., & Mok, A. (2010). Future of Wireless and the WirelessHART Standard. En WirelessHART™ (pp. 227–243). Springer US. Recuperado a partir de http://link.springer.com.dibpxy.uaa.mx/chapter/10.1007/978-1-4419-6047-4_18

Creative Commons. (s/f). Aircrack-ng. Creative Commons. Recuperado a partir de www.aircrack-ng.org

Definición de las siete capas del modelo OSI y explicación de las funciones. (s/f). Recuperado el 23 de enero de 2018, a partir de https://support.microsoft.com/es-mx/help/103884.

Edge, C., Barker, W., Hunter, B., & Sullivan, G. (2010). Securing a Wireless Network. En Enterprise Mac Security (pp. 325–350). Apress. Recuperado a partir de http://link.springer.com.dibpxy.uaa.mx/chapter/10.1007/978-1-4302-2731-1_12

GLOBAL HEADQUARTERS, & Fortinet Inc. (s/f-a). HARLEY-DAVIDSON DEALER SYSTEMS Delivering the Promise – Safely and Securely. www.fortinet.com.

GLOBAL HEADQUARTERS, & Fortinet Inc. (s/f). MAJOR DENTAL SUPPORT ORGANIZATION ENJOYS ENHANCED PROTECTION WITH A LOWERED TOTAL COST OF OWNERSHIP. GLOBAL HEADQUARTERS Fortinet Inc.

GLOBAL HEADQUARTERS, & Fortinet Inc. (s/f-b). Popular theme park boosts sales and profi tability with Presence Analytics. Fortinet, Inc. Recuperado a partir de www.fortinet.com

Ing. David Alejandro Montoya Murillo. (s/f). Diseno y evaluacion de un proceso de gestion de seguridad de servicios de TI: Caso LABDC-UAA.

Introducción a lasredes inalámbricas.pdf. (s/f). Recuperado a partir de http://bibing.us.es/proyectos/abreproy/11761/fichero/Volumen1%252F5-Cap%C3%ADtulo1+-+Introducci%C3%B3n+a+las+redes+inal%C3%A1mbricas.pdf+

ITIL Service Design. (s/f). Crown Copyright 2007. Recuperado a partir de www.tsoshop.co.uk

Jesus Carlos Bautista Ramos. (s/f). Diseño y Evaluacion de un Proceso Integrado de Gestion de asistencia-Incidentes de SErvicios de TI: Caso LAbDC UAA.

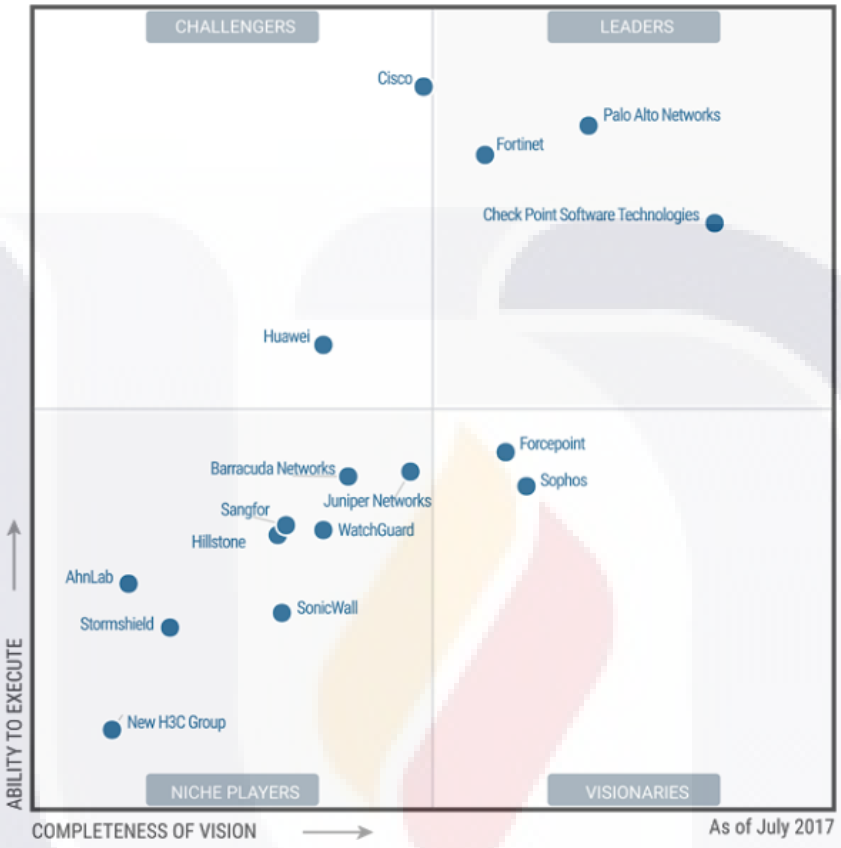
Lopez, J., Roman, R., & Alcaraz, C. (2009). Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Networks. En A. Aldini, G. Barthe, & R. Gorrieri (Eds.), Foundations of Security Analysis and Design V (pp. 289–338). Springer Berlin Heidelberg. Recuperado a partir de http://link.springer.com.dibpxy.uaa.mx/chapter/10.1007/978-3-642-03829-7_10

Sheetal Joseph. (2008, septiembre 22). Wireless Security. Copyright © The OWASP Foundation.

Types of Wireless Network Security Technology. (2006). En Guide to Wireless Network Security (pp. 57–83). Springer US. Recuperado a partir de http://link.springer.com.dibpxy.uaa.mx/chapter/10.1007/978-0-387-29845-0_2

8 ANEXOS.

Anexo A.- Cuadrante Mágico Gartner, tendencias tecnológicas.



Anexo B.- Línea del tiempo sobre las tendencias de las redes inalámbricas desde sus inicios al año 2017.