REPÚBLICA DEL ECUADOR

UNIVERSIDAD TECNOLÓGICA EMPRESARIAL DE GUAYAQUIL

TRABAJO DE TITULACIÓN
PARA LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN GESTIÓN DE TELECOMUNICACIONES MENCIÓN REDES DE ACCESO Y TELEFONIA

TEMA:

IMPLEMENTACIÓN DE SERVIDORES RADIUS PARA CONTROLAR LOS ACCESOS NO AUTORIZADOS A REDES INALÁMBRICAS, CASO OSFL.

AUTOR:

JUAN CARLOS MENA MOLINA

2019

GUAYAQUIL – ECUADOR

AGRADECIMIENTO

En estas líneas deseo expresar mi más profundo y sincero agradecimiento a cada una de las personas que han hecho posible la realización de este trabajo, no sin antes agradecer a Dios, ya que gracias a Él y sus bendiciones pude culminar una de las metas propuestas como la obtención de mi título; por supuesto agradezco a mi familia, mama, papa y hermanas; a mis amigos, quienes se hicieron presente dándome ánimos; a cada uno de ellos les quedo totalmente agradecido por la comprensión, la paciencia y el ánimo recibidos. Gracias por estar siempre a mi lado y entender que el tiempo sacrificado ha sido en búsqueda del éxito y para disfrutar un mejor futuro.

DEDICATORIA

A mi madre Gloria por ser el respaldo incondicional durante todos estos años y por todo su esfuerzo y su sacrificio empleado para mi beneficio: a mi familia que estuvieron cerca siempre para apoyarme y por estar siempre pendientes de mí todos estos años de estudio y esfuerzo.

A ustedes, mi familia, les dedico este logro, nuestro logro, porque nada de esto hubiera sido posible sin su apoyo.

La responsabilidad de este trabajo de investigación, con sus resultados y conclusiones, pertenece exclusivamente al autor.

……..

Juan Carlos Mena Molina

IMPLEMENTACIÓN DE SERVIDORES RADIUS PARA CONTROLAR LOS ACCESOS NO AUTORIZADOS A REDES INALÁMBRICAS, CASO OSFL.

Juan Carlos Mena Molina

Jcmena80@gmail.com

RESUMEN

El presente artículo académico describe la necesidad de mejorar la seguridad y control en los accesos no autorizados a las redes inalámbricas de la organización sin fines de lucro (OSFL) mediante la implementación de un servidor Radius.

En la vulnerabilidad se identificó el problema de accesos no autorizados a las redes inalámbricas así como sus consecuencias con el fin de mejorar las seguridades y buscar conceptualizar las variables identificadas dentro de la implementación, con la finalidad de tener mayor conocimiento para abordar la problemática.

En los resultados de la investigación y aplicación se determinó que después de implementar estas seguridades en las redes inalámbricas de la OSFL, se logró tener un mayor control de los accesos a las redes sobre clientes inalámbricos, minimizando el riesgo de robos de información y ataques a los diferentes recursos que están en la red LAN de la organización, y así cubrir con las falencias de seguridad dentro de la redes inalámbricas.

Palabras clave: Radius, redes Inalámbricas, seguridades, vulnerabilidad.

1. INTRODUCCIÓN

El problema radica en el control de acceso a las redes inalámbricas de la OSFL ya que son redes con muy pocas seguridades, lo cual las hace muy vulnerables contra ataques a los diferentes recursos como servidores, equipos de cómputos etc., Para ello se plantea la siguiente interrogante ¿Qué mecanismos se pueden utilizar para controlar y evitar los accesos no autorizados a las redes inalámbricas de la OSFL mediante la implementación de un servidor Radius?, El objetivo del presente trabajo pretende proporcionar seguridades a las redes inalámbricas para controlar los accesos no Autorizados a través de la implementación de un servidor Radius sobre un sistema operativo Windows Server 2016, esto permitirá gestionar la autenticación, Autorización y arqueo de usuarios no autorizados sobre un determinado recurso, brindando la adecuada seguridad de la información y así prevenir cualquier eventualidad que interrumpan las actividades de la organización .

1.1 Objetivo General

Proporcionar seguridades a las redes inalámbricas de la OSFL para controlar los accesos no Autorizados a través de la implementación de un servidor Radius.

1.2 Objetivos Específicos

- Examinar componentes de un servidor Radius e infraestructura de la organización.
- Facilitar el uso de los protocolos de autenticación mediante la investigación y descripción de sus conceptos.
- Controlar los accesos no autorizados a las redes inalámbricas de la OSFL.
- Implementación de un servidor Radius sobre un sistema operativo Windows Server 2016 y configuración de políticas de control de acceso a las redes inalámbricas del OSFL.

MARCO TEÓRICO

La organización sin fines de lucro brinda servicios a la comunidad (permisos de funcionamiento de locales comerciales, atención a solicitudes de simulacros, cursos y capitaciones a la ciudadanía y atención de emergencias), la cual proporciona internet a los empleados administrativos y visitantes mediante los diferentes puntos de acceso, pero posee un bajo control en los accesos no autorizados a las redes inalámbricas, las cuales son muy vulnerables contra ataques a los diferentes recursos existentes como servidores, equipos de cómputos o base de datos etc.,

A continuación la conceptualización de las herramientas utilizadas en este proyecto de investigativo

2. FUNDAMENTACIÓN TEÓRICA

2.1 Redes Inalámbricas

Una red inalámbrica conecta los ordenadores sin utilizar cables de red. Las computadoras usan comunicaciones de radio para enviar datos entre sí. Puede comunicarse directamente con otros equipos inalámbricos o conectarse a una red existente a través de un dispositivo AP inalámbrico (Intel, 2019).

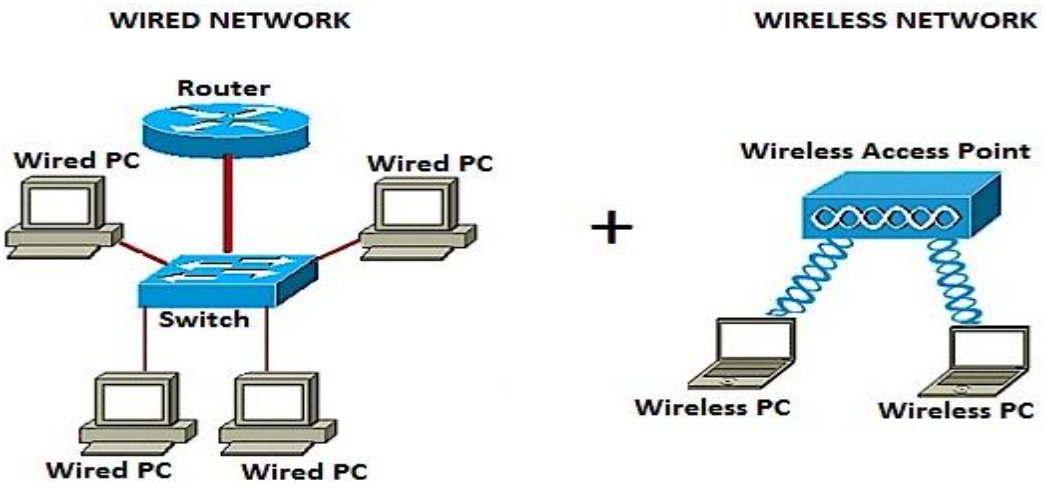

Figura 1: Redes Inalámbricas

Fuente: (Cisco)

2.2Firewall

Un firewall es un dispositivo de seguridad de red que monitorea el tráfico de red entrante y saliente y decide si permite o bloquea el tráfico específico en función de un conjunto definido de reglas de seguridad (Cisco, 2019).

2.3Seguridad Informática

> Podemos definir a la seguridad informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema (Gomez, 2014, pág. 38).

2.4Proxy

Los servidores proxy se suelen utilizar en redes de organizaciones y compañias, ya que permiten controlar los contenidos visitados en internet y asegurar que el uso que se hace del internet sea con fines laborales (Bellido, 2014)

2.5Amenazas

Una amenaza se puede definir como cualquier evento que puede afectar los activos de información y se relaciona, principalmente, con recursos humanos, eventos naturales o fallas técnicas. Algunos ejemplos pueden ser: ataques informáticos externos, infecciones con malware, una inundación, un incendio o cortes de fluido eléctrico (isotools, 2019).

2.6Vulnerabilidades

Las vulnerabilidades son por los general fallos de diseño de procedimientos o de recursos, las vulnerabilidades existen no se fabrican, una vulnerabilidad es cualquier fallo de diseño que permite que una amenaza pueda afectar a un recurso (Romero et al,. 2018).

2.7 RADIUS

El protocolo Radius (definido por los RFC 2865 y 2866) es un sistema cliente/servidor que permite gestionar de forma centralizada las cuentas de usuario y los derechos de acceso asociados (Carpentier, 2016, pág. 159).

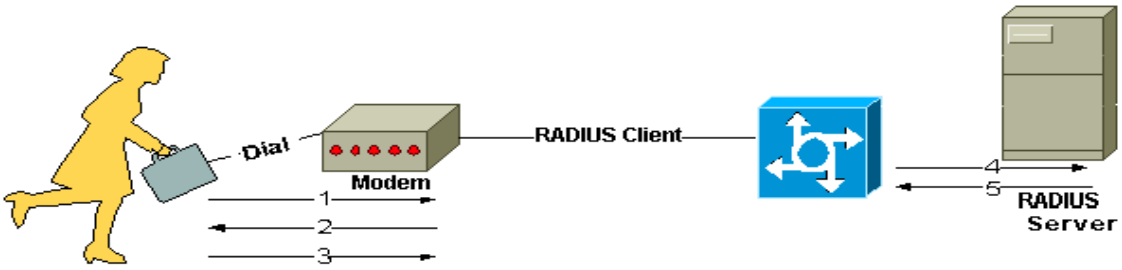

Figura 2: Cómo el Radius trabaja

Fuente: (Cisco)

2.1 Protocolo AAA

Para algunos autores el "AAA (Autenication, Authorization, Accounthing) provee una mejor solución al hacer que todos los dispositivos accedan a la misma base de datos de usurario y contraseñas en un servidor central" (Ariganello, 2016).

2.9 TACACS

Es un protocolo de autenticación remota privativo de Cisco, comúnmente usado en redes Unix, que se usa para comunicarse con un servidor de autenticación (Wikipedia, 2018).

2.10. Kerberos

El protocolo Kerberos proporciona autenticación de tercer interlocutor, en la que los usuarios demuestran su identidad ante un servidor centralizado, llamado servidor Kerberos o centro de distribución de claves (KDC), el cual expide tickets para los usuarios (IBM, 2019).

3. METODOLOGÍA

En el diseño del siguiente artículo es causi-experimental. Son una derivación de los estudios experimentales, en los cuales la asignación de los pacientes no es aleatoria aunque el

factor de exposición es manipulado por el investigador (Segura, 2019). El tipo de enfoque del artículo es cuantitativo. El enfoque cuantitativo es un procedimiento que se basa en la utilización de los números para analizar, investigar y comprobar tanto información como datos (Sanz, 2017). El alcance toma como base el estudio exploratorio, realizando una amplia documentación acerca de cada uno de los componentes y factores que contribuyen en la implementación de un servidor de autentificación Radius. Los estudios exploratorios se realizan cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes (Hernández Sampieri, 2014, pág. 79).

3.1 Métodos / Técnicas de Recolección

Una vez realizado el análisis de acuerdo a la naturaleza del artículo la metodología empleada fue el método deductivo. Se habla de método dedudctivo para referirse a una forma especifica de pensamiento o razonamiento, que extrae conclusiones lógicas y válidas a partir de un conjunto dado de premisas o proposiciones (Enciclopedia de Conceptos, 2018). La investigación no tiene sentido sin las técnicas de recolección de datos (Maya, 2014). Debido a lo cual la técnica de recolección de datos empleado en este artículo son: la observación, reportes de la solución implementada, log del servidor y el diagrama de flujo. El diagrama de flujo es una representación pictórica de los pasos en proceso, útil para determinar cómo funciona realmente el proceso para producir un resultado (slideshare, 2018).

El software que se utilizó para obtener los indicadores de rendimiento de la red es el IAS Log Viewe, Cisco WLC y el Fortianalyzer que son aplicaciones de análisis de trafico de red y permiten monitorear en tiempo real, mediante la utilización de protocolo Snmp, los usuarios y aplicaciones que consumen recursos de red en un determinado tiempo, la función principal de estos software es monitorear toda la red en busca de datos para generar estadísticas.

3.2 Diagrama de Flujo de Portal Cautivo

El objetivo del siguiente diagrama de flujo del portal cautivo es poder contrastar el proceso de autenticación del usuario, y así poder tomar como ejemplo para controlar los accesos no autorizados a las redes inalámbricas mediante la instalación y configuración de RADIUS Server en OSFL.

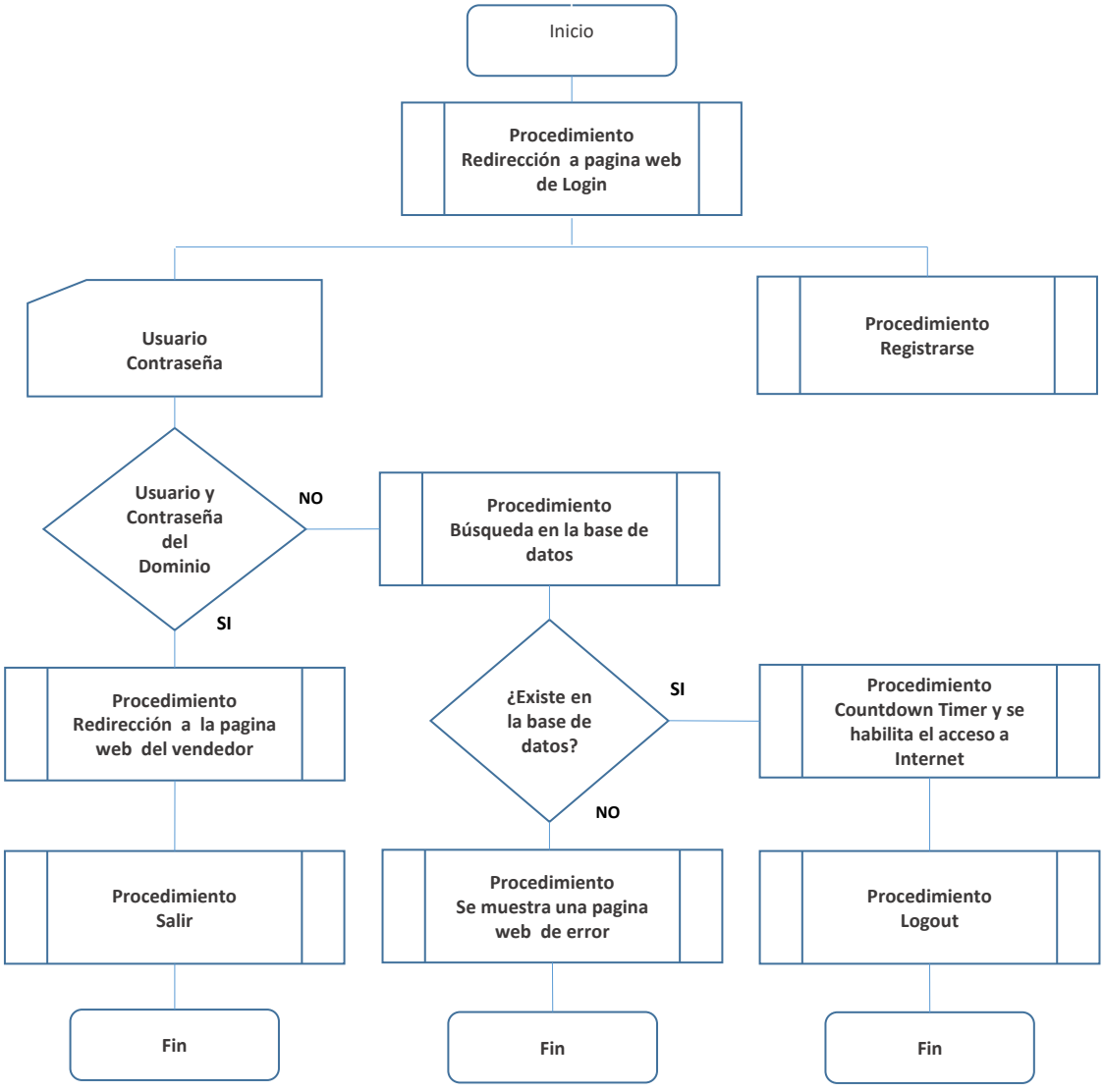

Figura 3: Diagrama de portal Cautivo

Fuente: (EPN)

Durante la implementación del sistema de autenticación inalámbrica se utilizó un esquema de red como el que muestra la figura 4, compuesta por un punto de acceso inalámbrico, un switch de acceso capa 2, una Wireless LAN Controller (WLC), un cable Ethernet Cat 6ª para el acceso a la red LAN, un servidor Radius y varios usuarios con tarjetas de red inalámbrica. La arquitectura se la puede observar en la siguiente figura.

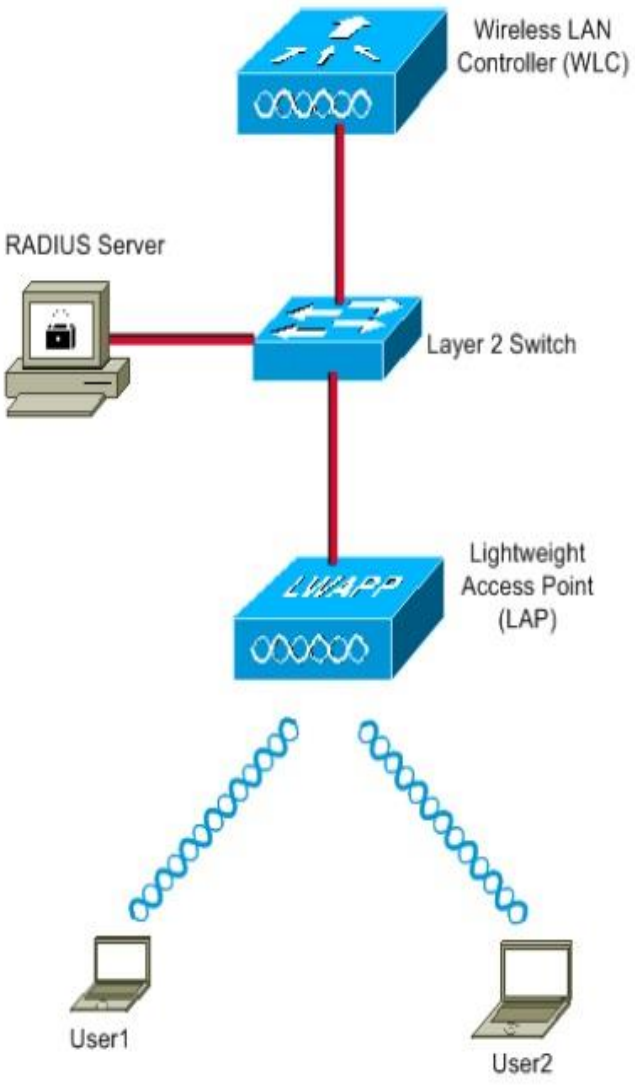

Figura 4: Diagrama de red
Fuente: (Cisco)

En la figura 4 muestra como los usuarios inalámbricos se conectan a un punto de acceso a través de una tarjeta de red inalámbrica, el punto de acceso sirve como medio para que los clientes inalámbricos se conecten con la wireless LAN Controller, en donde están creadas todas las red inalámbricas y estas a su vez con el servidor de seguridad Radius previamente configurado para administrar la autenticación de los clientes.

4. RESULTADOS

La siguiente grafica muestra el ancho de banda del enlace principal antes de la implementación del servidor Radius, esta grafica fue obtenida el 3 de diciembre del 2018.

Ancho de Banda de Enlace Principal de OSFL Proporcionada por el ISP

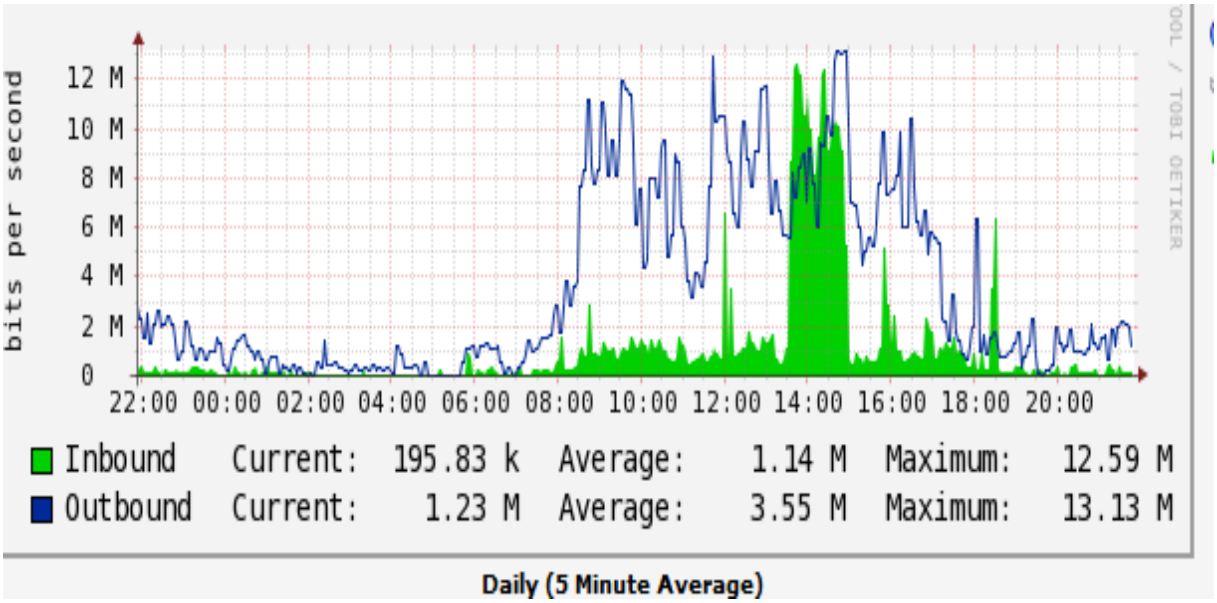

Figura 5: Reporte de ancho de Banda

Fuente: CNT

La siguiente grafica muestra el ancho de banda del enlace principal después de la implementación del servidor Radius, esta grafica fue obtenida el 3 de febrero del 2019.

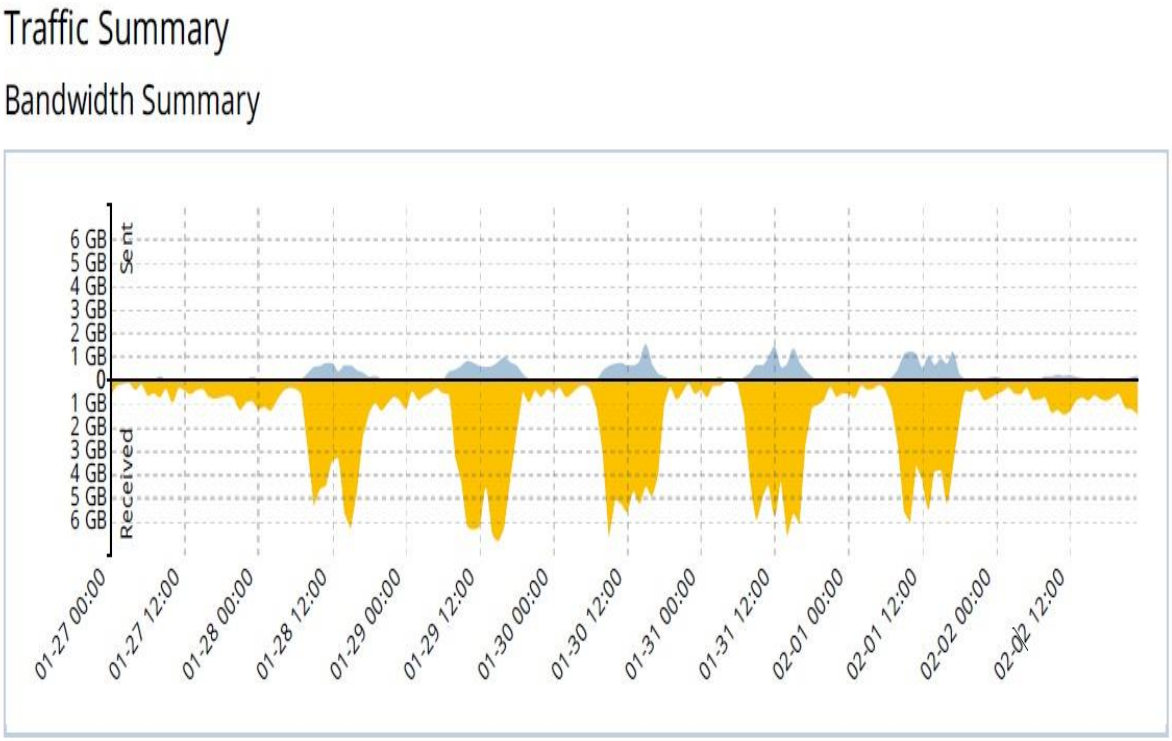

Figura 6: Bandwidth and Applications Report
Fuente: FortiAnalizer-200D

La Figura 5 muestra el ancho de banda del enlace principal de 15MB de la red de OSFL antes de implementación del servidor Radius, se pudo observar que la saturación llegaba a 13.3 MB durante una jornada laboral, esto era ocasionado por conexiones sin control y de forma desmedida. En la figura 6 muestra el ancho de banda del enlace principal luego de la implementación del servidor Radius, se observó que el ancho de banda de Subida y bajada permanecen equilibrando durante varios días y contrastado con la Figurar 5 se redujo a la

mitad el consumo general del enlace, lo cual hace que calidad del servicio sea la óptima y se evita la saturación del mismo.

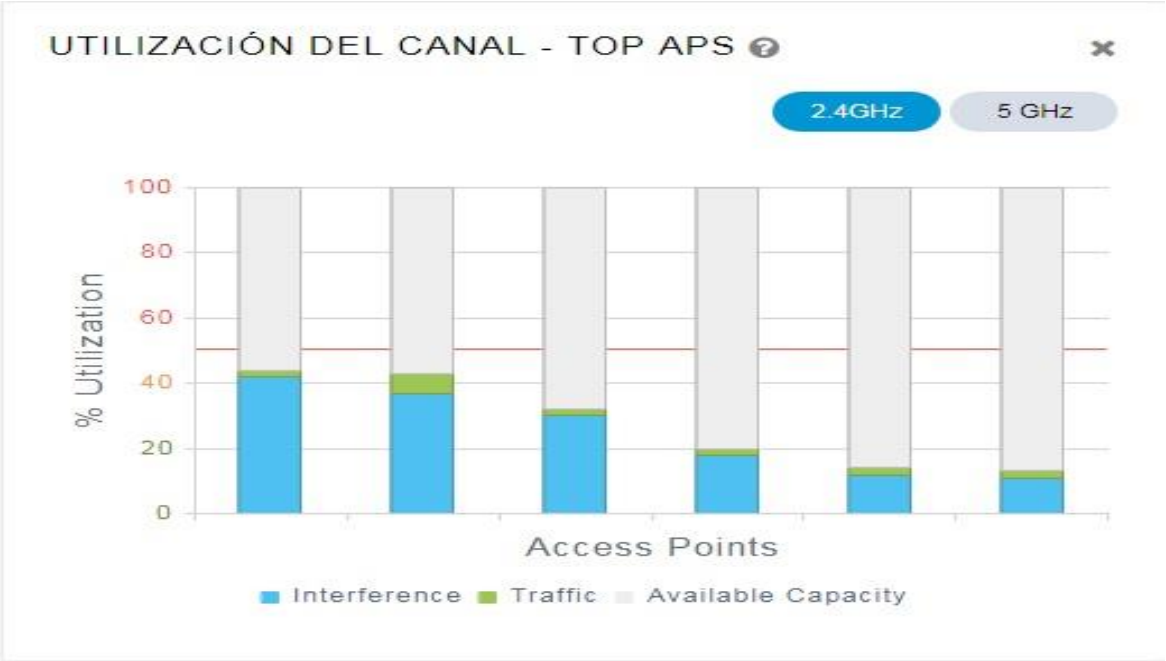

Figura 7: Rendimiento de AP

Fuente: Controlador Inalámbrico Cisco Serie 2500

En la Figura 7 se muestra como se redujo el tráfico en las diferentes AP luego de la implementación del servidor Radius y sus políticas para restringir los accesos no autorizados, y que tan solo dispositivos de la organización y los previamente autorizados tenga acceso a red Inalámbrica y demás recursos.

En cuanto a las políticas de seguridad implementadas, se puedo obtener buenos resultados esto con relación a la integración de usuario del dominio con el Servidor Radius, debido a la facilidad en la administración de las claves de las redes inalámbricas, y con respecto a limitar

el número de conexiones por usuario se logró descongestionar las redes y tener un mayor control de los usuario inalámbricos.

Para efectos de la presente investigación, se toma como datos las solicitudes rechazadas y aceptada por el servidor Radius, con estos datos obtenidos de las 4 últimas semanas se genera la siguiente tabla.

Tabla 1. Resultados de intentos de conexión que recibe el servidor Radius después de la implementación, se observa que acepta solo las conexiones de usuarios del dominio y las demás las rechaza.

	Número de Solicitudes de conexión			
	Semana 1	**Semana 2**	**Semana 3**	**Semana 4**
Aceptadas	123	30	141	556
Denegadas	7760	5300	5970	4761

Fuente: Elaboración Propia

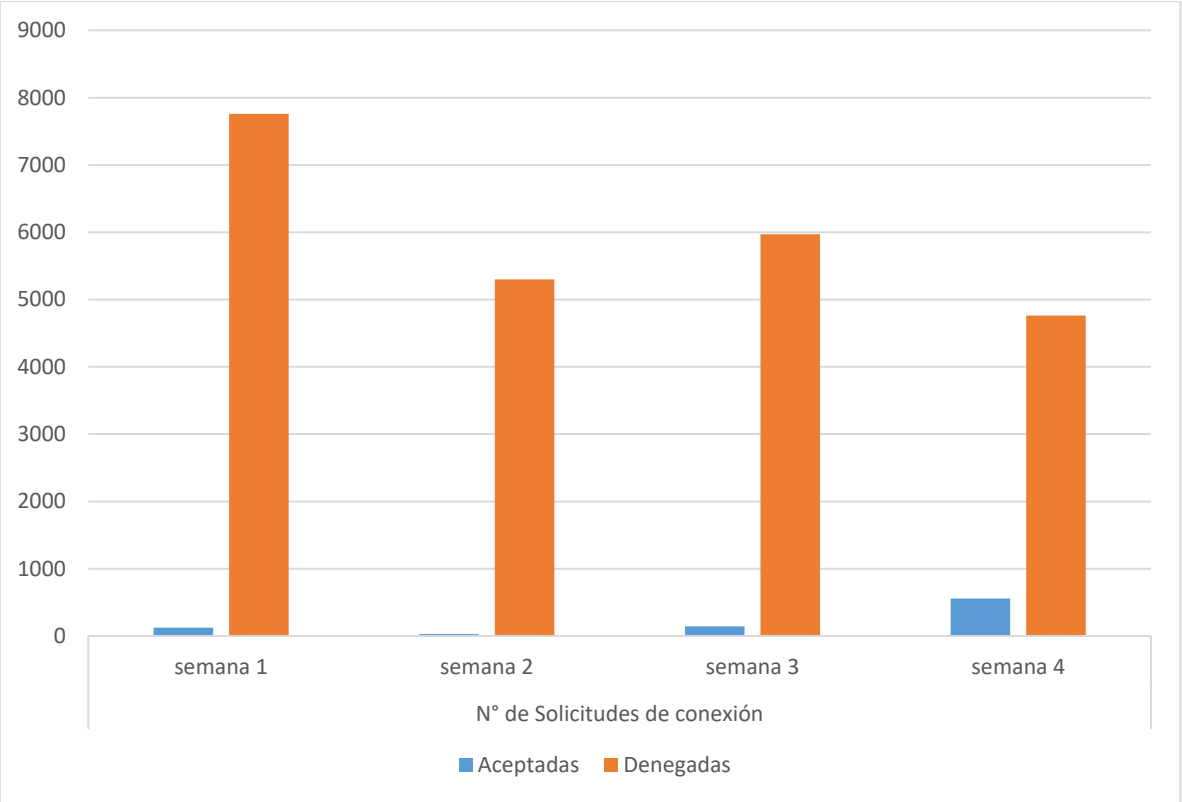

Figura 8: Numero de intentos de Conexiones a la redes inalámbricas de la OSFL

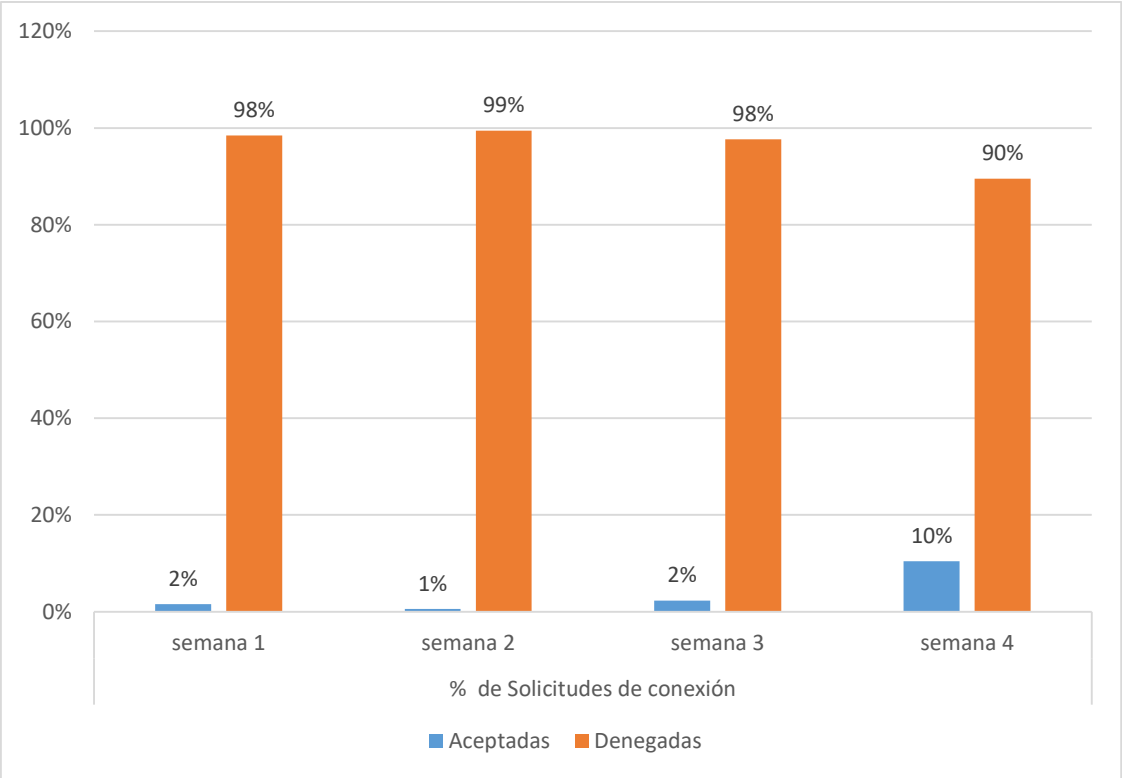

Figura 9: Porcentaje de Intentos de conexión a las redes inalámbricas de la OSFL.

5. CONCLUSIONES

- ✓ Una vez que se examinó los componentes de un Servidor Radius e infraestructura de la organización se pudo definir qué políticas de seguridad eran las más indicadas para corregir las falencias en los accesos a las redes inalámbricas, y así dotar de una solución adecuada a la organización.
- ✓ Realizado el análisis de la situación actual de las redes inalámbricas en el OSFL y apoyándonos en las investigaciones hechas sobre los conceptos relacionados con la autentificación y servidores, se decidió instalar el servidor Radius sobre la infraestructura actual que fue sobre un sistema operativo Windows Server 2016, y así facilitar la administración de las políticas de seguridad implementadas.
- ✓ A partir de la implementación del sistema de autenticación y autorización RADIUS sobre un sistemas Operativo Windows Server 2016, se logró tener un mayor control de los accesos no autorizados a las redes inalámbricas de OSFL, logrando denegar un 90% de solicitudes de conexión mientras que el 10% de solicitudes aceptadas son de usuarios autorizados como se muestra en la gráfica 7 durante la 4 últimas semanas, logrando cubrir con las falencias de seguridad que se encontraban en las redes inalámbricas, obteniendo buenos resultados después de la investigación e implementación.
- ✓ La seguridad y control en las redes Inalámbricas del OSFL, se beneficiaron de forma positiva, debido a que se implementaron políticas de seguridad como: permitir que solo usuarios del dominio puedan conectarse a la red inalámbrica, limitar el número de conexiones por usuario y el uso de protocolos avanzados de seguridad que nos permite encriptar los mensajes que viajan entre servidor y cliente Inalámbrico, con esto se logró minimizar el riesgo de robos de información y ataques a los recursos que están en la red LAN de la organización.

Referencias

Ariganello, E. (2016). *Redes Cisco. Guía de estudio para la certificación CCNA Routing y Switching.* Madrid: Ra-Ma.

Bellido, E. (2014). *Equipos de interconexión y servicios de red.* Malaga: IC Editorial.

Carpentier, J.-F. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas.* Ediciones ENI.

Cisco. (29 de Noviembre de 2018). *Agregue una red inalámbrica a una red alámbrica existente usando un unto de acceso de red inalámbrica (el WAP)*. Obtenido de Cisco: https://www.cisco.com/c/es_mx/support/docs/smb/wireless/cisco-small-business-100-series-wireless-access-points/smb5531-add-a-wireless-network-to-an-existing-wired-network-using-a.html

Cisco. (2019). *¿Cómo el RADIUS trabaja?* Obtenido de Cisco: https://www.cisco.com/c/es_mx/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.pdf

Cisco. (2019). *¿Qué es un firewall?* Obtenido de Cisco: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

Cisco. (2019). *Diagrama de la red.* Obtenido de Cisco: https://www.cisco.com/c/es_mx/support/docs/wireless-mobility/wireless-vlan/71683-dynamicvlan-config.pdf

Enciclopedia de Conceptos. (2018). *Método Deductivo*. Obtenido de Enciclopedia de Conceptos: https://concepto.de/metodo-deductivo-2/

EPN. (s.f.). *Dideño e implentación de un portal cautivo que permita la venta de tickets de internet para un hotspot, emplenado Herramientas de software libre* . Obtenido de bibdigital.epn.

Gomez, Á. (2014). *Enciclopedia de la Seguridad Informatica.* Alafaomega.

Hernández Sampieri, R. (2014). Metodología de la investigación. Mexico: Mc Graw Hill.

IBM. (2019). *Protocolos del servicio de autenticación de red*. Obtenido de IBM: https://www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_73/rzakh/rzakhprotocol.htm

Intel. (2019). *Redes inalámbricas Visión general*. Obtenido de Intel: https://www.intel.la/content/www/xl/es/support/articles/000006856/network-and-i-o/wireless-networking.html#1

isotools. (2019). *La norma ISO 27001: Aspectos claves de su diseño e implantación .* Obtenido de isotools: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

Maya, E. (2014). *Métodos y técnicas de investigación.* Obtenido de arquitectura: http://arquitectura.unam.mx/uploads/8/1/1/0/8110907/metodos_y_tecnicas.pdf

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Álava, C. M., . . . Castillo, M. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* Alicante: 3 ciencias.

Sanz, R. (30 de Abril de 2017). *¿Qué es el método cuantitativo?* Obtenido de Cursos: https://cursos.com/metodo-cuantitativo/

Segura, A. (Julio de 2019). *Diseños Causi-experimentales*. Obtenido de Facultad Nacional de Salud Pública. Universidad de Antioquia: http://www.sld.cu/galerias/pdf/sitios/renacip/disenos_cuasiexperimentales.pdf

slideshare. (30 de Noviembre de 2018). *Las técnicas de recolección de datos*. Obtenido de slideshare: https://es.slideshare.net/JuanSebastianGarciaM/las-tcnicas-de-recoleccin-de-datos

Wikipedia. (4 de Noviembre de 2018). *TACACS*. Obtenido de Wikipedia: https://es.wikipedia.org/wiki/TACACS