APLICABILIDAD DE CONTROLES DE SEGURIDAD INFORMATICA QUE GARANTICE LA EFECIENCIA DE LA ADMINISTRACION DEL SERVICIO DE RED “WIFI” DE LA COOPERATIVA UTRAHUILCA

MANUEL RICARDO GONZALEZ CHARRY

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
NEIVA - HUILA
2018

APLICABILIDAD DE CONTROLES DE SEGURIDAD INFORMATICA QUE GARANTICE LA EFECIENCIA DE LA ADMINISTRACION DEL SERVICIO DE RED “WIFI” DE LA COOPERATIVA UTRAHUILCA

MANUEL RICARDO GONZALEZ CHARRY

Trabajo de grado para optar el título de Especialista en Seguridad Informática

Director
ING. JUAN JOSE CRÚZ GARZÓN

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
NEIVA - HUILA
2018

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

NEIVA, 03 Mayo de 2018

DEDICATORIA

Dedico este trabajo a todas las personas que me apoyaron permitiendo crecer profesionalmente. A mi madre María del pilar Charry Rubiano, por su apoyo incondicional y su cariño, a mi novia Ana Tulia Sánchez por enseñarme que se puede lograr más cosas cuando uno se las propone y no desfallecer en el camino. Gracias a ellas cumplo mi meta.

AGRADECIMIENTOS

Agradezco el apoyo de mi madre y mi novia por confiar en mí para poder culminar con esta etapa profesional.

Al ing. Juan José Cruz, por la colaboración y su guía para la elaboración de esta tesis.

A la Cooperativa Utrahuilca, por permitirme implementar esta tesis la cual está en funcionamiento.

Agradezco a la Universidad Abierta y a Distancia - UNAD por permitir formarme como un mejor profesional ampliando mis conocimientos y mejorar la calidad de aprendizaje en el país.

Ing. Manuel Ricardo González Charry

CONTENIDO

pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

RESUMEN

Este proyecto tiene como finalidad documentar e implementar la aplicabilidad de controles de seguridad informática que garantice la eficiencia de la administración del servicio de red “WIFI” de la Cooperativa UTRAHUILCA. Es una empresa asociativa sin ánimo de lucro, especializada en ahorro y crédito enfocado en la economía solidaria con prácticas de principios y valores cooperativos.

En el proceso de ejecución, se encontró que necesita un elemento de mejora en el funcionamiento de la red WiFi de la Cooperativa, mediante de uso de portal cautivo el cual se encontrará seguro con un certificado SSL y la implementación de un web Application firewall, que será protegido de ataques y con el proxy Squid, esta procederá a bloquear los sitios no categorizados o malware; siendo así una red segura.

Palabras Clave: WIFI, RADIUS, SERVIDORES, PROXY, PORTAL CAUTIVO, SSL, WAF, SQUID

INTRODUCCIÓN

En la actualidad el crecimiento de los sistemas informático permite mayor interacción y realización de transacciones desde cualquier dispositivo, además agilizan un sin número de operaciones; pero, así mismo los delincuentes informáticos no se detienen y se provecha de cualquier debilidad en los sistemas, permitiendo sustraer información vital de cualquier organismo.

La seguridad en la WIFI se convierte en un problema si no se cuenta con la medida necesaria para controlar los accesos a la red. Teniendo en cuenta lo anterior, este proyecto tiene como objetivo asegurar la WIFI de la Cooperativa Utrahuilca, además, busca permitir el acceso a sus asociados para tener información confiable, ya que la información no se encuentra con seguridad y las vulnerabilidades que se descubren, la gran mayoría, son de ataques internos o por simple desconocimiento del tema.

La seguridad informática, es totalmente indispensable y necesaria en esta era digital, donde toda la información se encuentra expuesta en la nube y al ser así se requiere la protección de la misma; en la Cooperativa Utrahuilca se requiere que dicha información sea asegurada y esté disponible a sus asociados, y para ello se hace necesario una implementación de seguridad ya que no cuentan con ello.

1. TITULO

APLICABILIDAD DE CONTROLES DE SEGURIDAD INFORMÁTICA QUE GARANTICE LA EFECIENCIA DE LA ADMINISTRACIÓN DEL SERVICIO DE RED “WIFI” DE LA COOPERATIVA UTRAHUILCA EN NEIVA, HUILA.

AREA: SEGURIDAD INFORMATICA, RED WIFI

2. DEFINICION DEL PROBLEMA

2.1 ANTECEDENTES DEL PROBLEMA

Desde el principio de la historia el hombre ha tratado de encriptar la información de sus mensajes, como el clave morse o como la maquina enigma usada en la segunda guerra mundial la cual permitió descifrar y cifrar los mensajes para que el enemigo si llegara a interceptar el mensaje no pudiera cifrarlo, sólo se podía descifrar con la misma máquina que se creó el mensaje.

La Universidad Nacional a Distancia UNAD ha crecido en conocimiento respecto a su desarrollo y aplicación de conocimiento en Colombia, de esta manera, se resalta su trabajo en la implementación desde trabajos de investigación que promueven la práctica de la seguridad informática en el territorio nacional.

De esta manera, se presentan algunos trabajos de investigación realizados por la UNAD desde seguridad informática: "*Propuesta de actualización, apropiación y aplicación de Políticas de seguridad informática en una empresa Corporativa, propolsinecor*"[1], aquí el concepto sobre seguridad Informática que emplea el ingeniero Olmedo Patiño es: "la aceptación clara de cada uno de los usuarios del sistema informático de la compañía, en conocer las PSI, y/o herramienta que permite adoptar una cultura de seguridad informática, orientada a proteger el activo informático y estratégico de la compañía, los cuales deben estar alineados con los objetivos del negocio y los criterios de seguridad informática considerado

por El Information Technology Evaluation Criteria (ITSEC)"(Romero2003 p.35)".

[1]Olmedo, Luis Patiño. UNAD. San Juan de Pasto. 2014. {En línea}. {Consultado el 25 de agosto de 2017}. Disponible en: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/2742/1/129732 10.pdf.

Otra investigación, es el "*Análisis de riesgos de la Seguridad de la información para la institución Universitaria Colegio Mayor del Cauca*"[2], donde Solarte al citar sus fuentes indica que Seguridad Informática se puede entender como "un estado específico de la misma sin importar su formato, que indica un nivel o un determinado grado de seguridad de información, por ejemplo, que está libre de peligro, daño o riesgo, o por el contrario que es vulnerable y puede ser objeto de materialización de una amenaza"[3]; además, agrega que: "la seguridad de la información es importante en negocios tanto del sector público como del privado para proteger las infraestructuras críticas"[4].

En la búsqueda realizada sobre los trabajos realizados desde la seguridad informática se encontró que se han realizado diversas acciones en diversas entidades del territorio nacional, y esta investigación quiere hacer un aporte desde la integración de los dispositivos WIFI.

Contexto Local

En Colombia, el 2012 fue un año bastante movido en materia de seguridad informática debido a los constantes ataques a redes sociales y además por un crecimiento significativo de virus especializados para dispositivos móviles5 Y desde esta fecha el reto es mayor, actualmente, el 80% de los ataques son intentos de conexiones Netbios (Worms/Virus) y el18% son herramientas automatizadas de scanning.

---

[2] Solarte, Francisco Solarte. UNAD. Popayán. 2014 {En línea}. {Consultado el septiembre de 2017}. Disponible en: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/2655/3/76327474.pdf

[3] Ibíd.

[4] Op. cit. Pág. 19-20

[5] Arce, Acosta & Posada. Estado Del Arte de La Seguridad Informática. Universidad de Cartagena. 2013 {En línea}. {Consultado en agosto de 2017}. Disponible en: https://es.scribd.com/document/134099136/Estado-Del-Arte-de-La-Seguridad-Informatica

En el análisis y en la revisión documental realizada para el desarrollo de este proyecto, se encontró que en el contexto local no se han escrito proyectos de investigación que se especialicen en este tema y en este tipo de empresas, por lo cual se considera que este proyecto postula un conocimiento nuevo para esta entidad, es válido por la necesidad que presenta y es útil porque su aplicabilidad es pertinente para la seguridad de los usuarios de la Cooperativa Utrahuilca.

2.2 FORMULACIÓN DEL PROBLEMA

En la actualidad, la cooperativa Utrahuilca cuenta con 10 puntos de acceso dentro las instalaciones del edificio, cuenta con balanceo de carga, pero su administración no está centralizada. El nombre de red Utrahuilca_piso4, está sementada en una VLAN independiente.

Esta red no cuenta con la administración adecuada sin ningún control, dejando que el canal de banda ancha se sature por la cantidad de equipos conectados. Teniendo en cuenta lo anterior, lo más recomendable para esta situación es cifrar la conexión con WPA2 el cual se encuentra definido en los estándares de la IEEE 802.11 para permitir y garantizar el acceso a la red.

Teniendo en cuenta lo anterior, para los sistemas de información donde su uso es constante a través de dispositivos móviles ¿Cómo y qué controles de seguridad informática serán aplicados para garantizar la eficiencia de la administración del servicio de red “WIFI” de la Cooperativa Utrahuilca de Neiva en el año 2018?

2.3 DESCRIPCION DEL PROBLEMA

Utrahuilca, es una cooperativa especializada en ahorro y crédito la cual aplica la filosofía de la economía solidaria donde se ve los principios y valores cooperativos,

siendo una empresa asociativa sin ánimo de lucro creada como organización jurídica con formada por asociados. Ubicada en el sur colombiano con diferentes sedes alrededor del país prestando los servicios de ahorro y crédito a nivel nacional.

Para poder llegar a todos sus asociados deciden implementar zonas WiFi dentro de su agencia para otorgar libre acceso para ellos, ayudando a mejorar la disponibilidad de la oficina agilizando información y permitiendo evitar el congestionamiento de la agencia.

Para ello es necesario implementar controles de seguridad en la red de datos de la cooperativa Utrahuilca con la finalidad de mitigar los riesgos de intrusión al sistema, todo ingreso será por medio de autenticación.

3. JUSTIFICACION DEL PROYECTO

El presente trabajo se realizó para prestar un mejor servicio por medio de la WIFI para los asociados de la cooperativa Utrahuilca, también para asegurar la información que está expuesta a sus asociados, garantizando la alta disponibilidad y dando soluciones de manera pertinente y eficiente.

Como ingeniero de sistemas, entiendo que la información es vital, porque en las empresas y en la actualidad el crecimiento de la tecnología es enorme y representa retos de seguridad por implementar para minimizar las vulnerabilidades, por esas razones se realiza esta aplicabilidad de seguridad para la información de los usuarios de esta Cooperativa.

Finalmente, este trabajo es necesario para dar conocer todo el proceso de este tipo de implementación de controles, paso a paso desde la teoría a la práctica, debido a que sobre este tema hay escasa información académica en esta región del país. Además, porque permite desarrollar de manera práctica la configuración de un portal cautivo para garantizar la seguridad informática de la Cooperativa Utrahuilca; y de esta manera, sus asociados no presenten dificultades o vulnerabilidades en sus datos de sistema.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Aplicar controles de seguridad informática para garantizar la eficacia de la administración del servicio de red “WIFI” de la Cooperativa Utrahuilca de Neiva.

4.2 OBJETIVO ESPECIFICO

Debido a la falta de controles de seguridad informática en la red WIFI de la Cooperativa Utrahuilca, se propone hacer lo siguiente:

1. Implementar un sistema de seguridad basado en protocolo de Autenticación, Autorización y conteo de sesiones para la red WiFi de la Cooperativa Utrahuilca.

2. Implementar un servidor RADIUS para la administración de los servicios de autenticación, autorización y conteo de registros de acceso a la red inalámbrica de la cooperativa Utrahuilca.

3. Configurar un portal cautivo, para re-direccionar el tráfico HTTPS permitiendo el ingreso con autenticación.

4. Implementar SQUID como proxy para administrar los sitios que se podrán ingresar.

5. Implementar Web Application Firewall para controlar el acceso a la aplicación web del portal cautivo evitando ataques de inyección.

5. MARCO REFERENCIAL

5.1 MARCO TEÓRICO

5.1.1 Red inalámbrica:

Las redes inalámbricas se llaman así para distinguirlas de las redes tradicionales por cable o las más modernas de fibra óptica. En una red inalámbrica los datos se transmiten por el aire usando distintas tecnologías.[6]
Ventajas:

- Fácil instalación abajo costo de implementación.
- No es necesario cableado para conectar hacia los dispositivos.
- Mejor movilidad y productividad se puede trabajar solo donde se encuentre el área de cobertura de la red inalámbrica.
- Su topología permite funcionar de una manera sencilla.

Las organizaciones utilizan las redes inalámbricas para permitir el ingreso a sus aplicaciones dejando la molestia del cableado y permitiendo reducir costos.

Desventajas:

- La conexión por red inalámbrica puede descifrarse si no se cuenta con las medidas de seguridad pertinentes.
- Las redes inalámbricas son un poco instables debido a ondas electromagnéticas o dispositivos electrónicos cercanos.
- Algunas veces puede verse afectada la señal por objetos.

[6] Gutiérrez, Ángel. Red inalámbrica - Lo que necesitas saber. 2012 {En línea}. {Consultado el agosto de 2017}. Disponible en: https://www.aboutespanol.com/red-inalambrica-lo-que-necesitas-saber-3507889

La autenticación que maneja las redes inalámbricas son por protocolos los cuales de ellos son WEP, WPA o WPA2. Para la seguridad de esto se usa los protocolos de la IEEE 802.1 lo cual encripta lo que se digita para autenticarse y tener acceso a la red.

5.1.2 WEP

Privacidad equivalente a cableado o Wired Equivalent Privacy es un sistema de cifrado estándar de la IEEE 802.11 en 1999, perteneciente a las redes inalámbricas permite cifrar los datos. Su cifrado está definido por un algoritmo RC4 de 64 bits, su funcionamiento es por onda radial; con una clave secreta de 40 o 104 bits, combinada con un Vector de Inicialización (IV) de 24 bits para encriptar el mensaje de texto M y su checksum – el ICV (Integrity Check Value)[7]

A continuación, algo de historia sobre WEP que expone Lehembre en su artículo Seguridad de WEP, WAP y WAP2: el protocolo WEP no fue creado por expertos en seguridad o criptografía, así que pronto se demostró que era vulnerable ante los problemas RC4 descritos por David Wagner cuatro años antes. En 2001, Scott Fluhrer, Itsik Mantin y Adi Shamir (FMS para abreviar) publicaron su famoso artículo sobre WEP, mostrando dos vulnerabilidades en el algoritmo de encriptación: debilidades de no-variación y ataques IV conocidos. Y Luego, los ataques KoreK en 2004 (ataques generalizados FMS, que incluían optimizaciones de h1kari), y el ataque inductivo invertido Arbaugh, permitieron que paquetes arbitrarios fueran desencriptados sin necesidad de conocer la clave utilizando la inyección de paquetes.

[7] Lehembre, Guillaume. Seguridad de WEP, WPA y WPA2.hakin9 Nº 1/2006. Francia. {En línea}. {Consultado en abril de 2017}. Disponible en: http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf

Entonces, la incorporación de la inyección de paquetes mejoró sustancialmente los tiempos de crackeo de WEP, requiriendo tan sólo miles, en lugar de millones, de paquetes con suficientes IVs únicos – alrededor de 150,000 para una clave WEP de 64-bits y 500,000 para una clave de 128-bits. Y actualmente no es muy recomendada.

5.1.3 WPA

Acceso WiFi protegido o WiFi Protected Access es la mejora del cifrado WEP ya que corrige las falencias que poseía este protocolo. También implementa la norma IEEE 802.11i, este protocolo se usa como servidor de autenticación (RADIUS) la cual entrega contraseñas Diferentes para cada usuario uno de los protocolos más relevantes es TKIP - Protocolo de Integridad de Clave Temporal o Temporal Key Integrity Protocol el cual se usa para evitar ataques de recuperación de clave.

5.1.4 WPA2

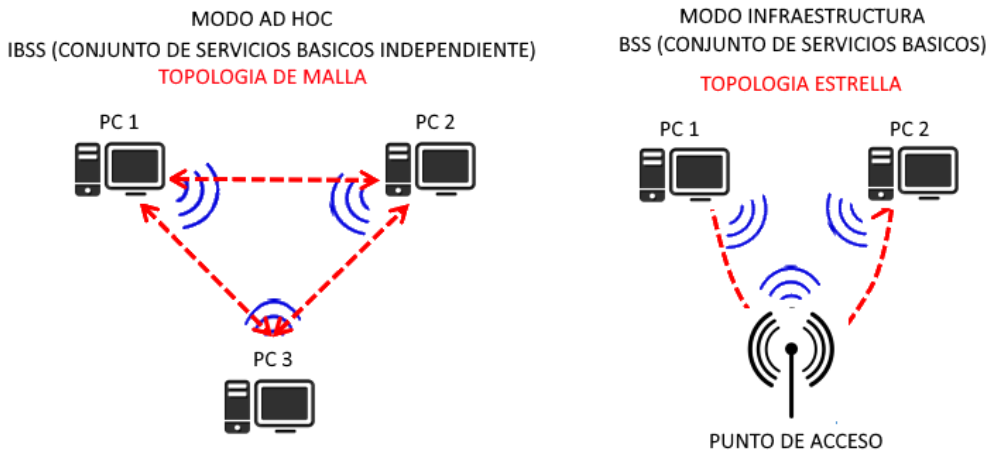
Acceso WiFi protegido 2 o WiFi Protected Access 2 es la mejora del cifrado WAP ya que corrige las falencias que poseía este protocolo con la norma IEEE 802.11i actualmente su Cifrado es AES (Avance Encriptaron Standard).

Este tipo de cifrado es recomendable para las organizaciones por su interoperabilidad.

5.1.5 Topología de red del 802.11

implementa en su arquitectura áreas conocida como BSA Area Básica de Servicio que es la que da el acceso del Access Point este dispositivo crea un BSS Set De servicio Básico sistemas de distribución.

Figura 1. Topologías de red 802.11



Fuente: El autor

5.2 MARCO CONCEPTUAL

Teniendo en cuenta los referentes teóricos vistos al inicio de este capítulo y los trabajos de investigación previos desarrollados por la Universidad Nacional a Distancia (UNAD), los siguientes conceptos para efectos de este proceso de investigación y de implementación, se entienden de la siguiente manera:

5.2.1 Seguridad informática

La seguridad informática se ocupa de diseñar las normas, protocolos, procedimientos, métodos y técnicas con la finalidad que el sistema de información sea seguro y confiable.

La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore y signifique un riesgo para la misma.

Según Ribagorda Gamacho, la seguridad de la información es una disciplina de reciente aparición y trata de la protección de ésta frente a revelaciones -accidentales o intencionadas-, a usuarios no autorizados, frente a modificaciones indebidas o frente a destrucciones[8]; además, agrega que esto implica la protección de datos personales que trata de mantener el derecho de los individuos para determinar cuándo, cómo, a quién, qué y para qué información sobre ellos puede ser cedida a terceros.

Así mismo, expone la necesidad de una autentificación de los Usuarios y lo considera como una actuación mediante la que el usuario corrobora ser quien se supone que es, esto como un mecanismo valioso en la seguridad informática. [9]

5.2.2 Vulnerabilidades

Lo sistemas no son 100% seguros por ello se deben realizar pruebas para detectar falencias en su programación puertos abiertos errores en su código siempre es necesario realizar pruebas de instrucción para encontrar falencias en este caso usar un protocolo de red robusto para el cifrado y cifrado en la programación del sitio cautivo con certificados de seguridad.

5.2.3 Radius

conocido como remote authentication dial-in user server este protocolo de autenticación nos permite gestionar el acceso a la red, permite grabar los registros

[8] Ribagorda, Arturo. La protección de datos personales y seguridad de la información. Escuela Politécnica Superior. Universidad Carlos III. Revista Jurídica de Castilla y León. N.º 16. SEPTIEMBRE 2008. Pág. 373-399.

[9] Ibíd. Pág. 383

de usuarios esquemas de autenticación son PAP, CHAP o EAP donde autorizara el acceso al ISP y permite el consumo de la red.

5.2.4 Proxy

Es un programa o un dispositivo que se encuentra en un servidor que permite la interacción entre cliente y servidor para las solicitudes para ingreso a sitios web también almacena información de esos sitios para que su ingreso sea más rápido también se puede restringir el acceso a ciertas paginas para bloquear puertos a sitios vulnerables con el fin de no afectar los usuarios.

5.2.5 Autenticación

se determinará si el usuario tiene acceso para ingresar a la red se maneja a través de credenciales.

5.2.6 Autorización

Permite entrar a módulos específicos según el perfil del usuario cuando ya ha conseguido autenticarse.

5.2.7 Pautas para Seguridad

A continuación, se presentan las pautas de seguridad a tener en cuenta en el interior de la investigación y la implementación de los elementos de seguridad en la WiFi.

- Proteger el sitio web con Secure Sockets Layer (SSL) para utilizar conexiones más seguras en el sitio web este certificado proveerá seguridad

para la entidad como para el cliente al momento de dar información personal es muy necesario para los servidores públicamente expuestos al internet.

- Verificar la programación del sitio no permitir el uso de caracteres especiales en las cajas de texto del sitio esto puede prevenir las inyecciones de SQL al sitio.
- Protección de ataques de denegación de servicio o DDoS con Cloudflare este no permitirá que se envíen peticiones constantes desde un mismo sitio, sino que lo restringirá.
- La seguridad física es vital al resguardar información en el datacenter solo deberá ingresar personal autorizado a esta área e igualmente desde la red local no se debe tener acceso al servidor web.
- Se debe realizar pruebas de instrucción al sitio web con herramientas tales como brute force, sqlmap, XXS, nessus con el fin de explorar las vulnerabilidades y cerrarlas.
- La incorporación de certificados digitales permitirá mejorar la seguridad servidor <-> cliente.
- El servidor debe ser monitoreado constantemente ver los logs de transacciones de la base de datos como el servicio web.
- Incorporación de Firewall con WAF esto con el fin de llegar a analizar las posibles intrusiones al sitio web el WAF Nos informara que ha tratado de Ingresar al sitio.
- En la red local donde se encuentra el servidor es de vital importancia contar con antivirus esto para que no se prologuen alguna infección que pueda perjudicar al sitio web.
- Se debe contar con una réplica fuera de la ciudad o en la nube en caso de una catástrofe caída total del sitio la réplica deberá entrar en línea para ello es recomendable el uso de balanceador de carga.
- Las claves de acceso deberán ser cifradas para no permitir robo de ella.

- La alta disponibilidad del sitio se encargará de no permitir cambios de la página web en caso de que un extraño quiera cambiar la integridad del sitio. la alta disponibilidad recupera el sitio original.
- Realizar escaneos a la red y cerrar los puertos vulnerables e innecesarios del sitio esto para minimizar el riesgo de intrusiones.
- Restringir el sitio a través de VPN esto para usar un canal dedicado sin permitir acceso a ningún intruso son más seguros para manejar información delicada.
- Los permisos a los archivos del sitio web solo otorgar privilegios a personal autorizado.
- Cambiar la configuración por defecto del servidor web ya que instalan usuarios admin el cual deberá ser modificado para mayor seguridad.

5.2.8 ISO 27001

Es un estándar internacional para los sistemas de gestión de la seguridad de la información (SGSI) que proporciona un marco de gestión de la seguridad de la información. Permite elegir los controles de seguridad adecuados para la protección de información de la empresa.

Características:

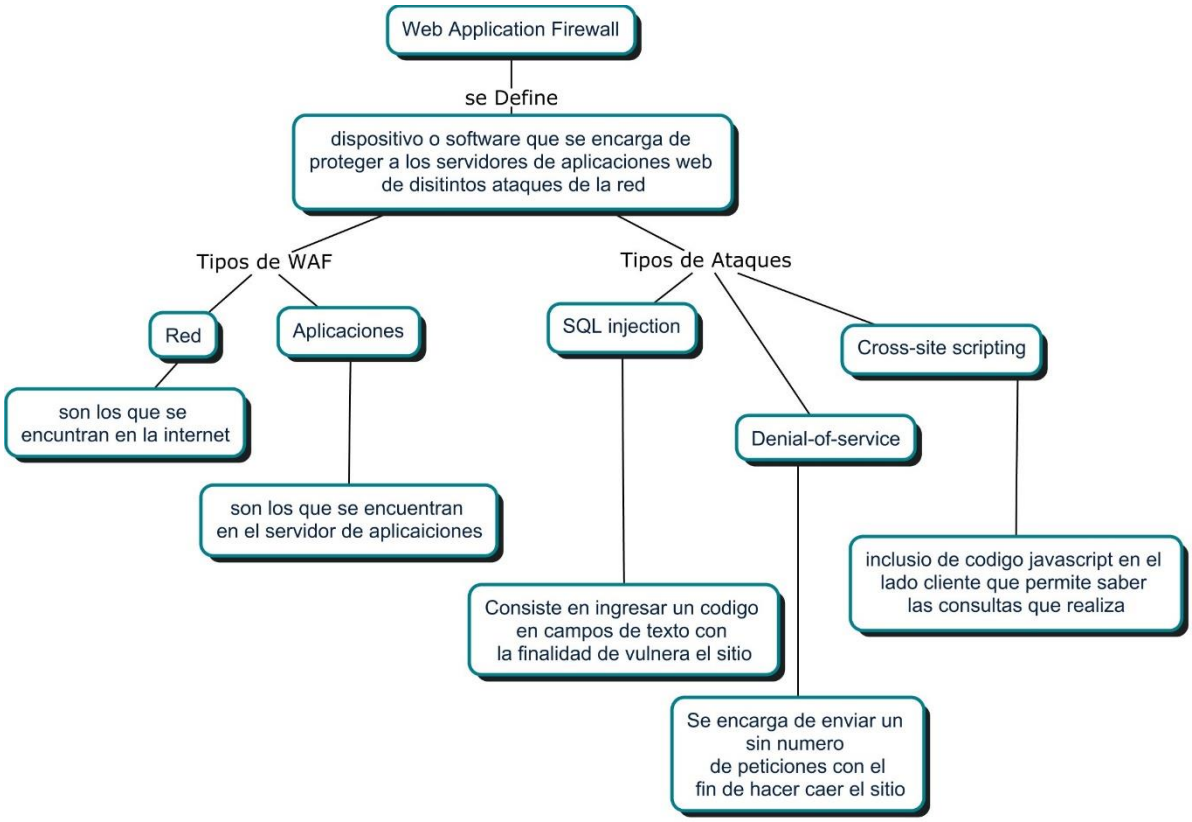
- Confidencialidad: se protege la información para que no sea utilizada por terceros.

- Seguridad de la información: resguardo y protección de la información solo se permite acceso a personas autorizadas.

- Sistemas de gestión de la seguridad de la información: permite Monitorear, Revisar y mejorar seguridad de información.

5.2.9 WAF

Figura 2. Cortafuego de Aplicación Web.



Fuente: El autor

5.3 MARCO HISTORICO

5.3.1 Antecedentes.

La cooperativa Utrahuilca, en el 2013 decide por parte del área de tecnología el uso de WiFi para facilitar el uso de los dispositivos portátiles dentro de las instalaciones ya que en un inicio se arrancó con 1 punto de acceso esto para pruebas piloto y ver como evolucionaba al saber que se quedaron sin recursos debido a la falta de filtrado de contenido ya que se consume la banda ancha por Videos y juegos.

La solución de centralizar y permitir el máximo provecho a la banda ancha con portal administrable ya que se permite que sea amigable para los usuarios, pero esto no ha sido posible.

5.4 MARCO LEGAL

La ley 1273 de 2009 de delitos informáticos en Colombia nombrada como la protección de la información y de los datos, donde castiga con penas de prisión y multas a los individuos que incurran en estos delitos:

Acceso abusivo a un sistema, informático, interceptación de datos informáticos, por usos de malware, robo de datos personales, suplantación de sitios web (Phishing), robo de bases de datos, transferencias de activos.

Hackers incurren en estas modalidades delictivas ya que se hacen de lo más importante la información para robos y suplantaciones.

Por ello las empresas que poseen la información deben garantizar la confidencialidad de la misma y tener una buena infraestructura en seguridad con el

fin de que no estén vulnerables ante estos ataques. Por ahora los más afectados son el sector financiero y las redes sociales.

El contenido de la ley es la siguiente:

CAPÍTULO. I.

Artículo 269A: Acceso abusivo a un sistema informático
Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.
Artículo 269C: Interceptación de datos informáticos.
Artículo 269D: Daño Informático
Artículo 269E: Uso de software malicioso
Artículo 269F: Violación de datos personales.
Artículo 269G: Suplantación de sitios web para capturar datos personales.

CAPITULO. II.

Artículo 269I: Hurto por medios informáticos y semejantes.
Artículo 269J: Transferencia no consentida de activos.

6. DISEÑO METODOLÓGICO

6.1 TIPO DE INVESTIGACIÓN

Esta investigación es de tipo aplicada porque desde la identificación de un problema en la red WIFI se propone y ejecuta una solución desde la aplicación de controles para el uso correcto de la red dentro de una cooperativa.

Teniendo en cuenta lo anterior, se realiza un estudio para determinar el funcionamiento de la red WIFI, el tipo de información consultada se toman los datos de los funcionarios y de algunos asociados para desarrollar una implementación de un sistema de control.

6.1.1 Alcance del Proyecto

Se realizó este proyecto de investigación e implementación del mismo permite que los asociados y empleados de la cooperativa Utrahuilca se beneficien con mayor eficiencia en la seguridad de sus datos al usar la red WIFI de la empresa. Además, este proyecto permite que otros estudiantes de seguridad informática conozcan un ejemplo de aplicación de controles a la red WIFI y de esta manera permite afianzar conocimientos para posteriores aplicabilidades.

Según la información obtenida, esta sirve de insumo para controlar los accesos a la red WIFI convirtiendo la navegación a la red más segura. Es decir, se implementa al acceso de la red WiFi en la cooperativa Utrahuilca con finalidad de permitir un mejor manejo de este recurso y asegurando su uso permitiendo el acceso a la información de manera controlada.

6.2 METODOLOGIA DE DESARROLLO

6.2.1 Procedimiento

Se tomaron las respuestas de la encuesta con la finalidad de examinar el problema de manera detallada e implementar la solución, esta información se socializó con los funcionarios de la cooperativa de la agencia Neiva ubicada en Neiva (Huila).

Para profundizar en el tema se consultaron fuentes secundarias como páginas web documentos sobre el problema y se seleccionó la mejor solución para el problema de seguridad WIFI.

6.3 HIPOTESIS

Teniendo en cuenta la situación presentada por la Cooperativa y los recursos al alcance, se plantea que un portal cautivo y sus controles pueden optimizar la red WIFI de la Cooperativa Utrahuilca.

VARIABLES E INSUMOS

Variable 1: eficiencia de servicio red wifi en Utrahuilca
Medida: critica, alta, media, baja.
Dimensión:

- Administración de Red Wifi.
- Identificación de usuarios red wifi.
- Utilizar canales sin Interferencia.
- Actualización de firmware.

6.4 TÉCNICAS DE ANÁLISIS Y PROCESAMIENTO DE DATOS

Por medio de la encuesta donde participaron 250 funcionarios que utilizaron la red WIFI, esto se realizó de esta manera debido a que esta muestra era más oportuna que si se preguntaba a los asociados. Posteriormente, se realizó una tabulación de a información en donde se elaboraron unas gráficas y estas permitieron analizar los resultados de las encuestas.

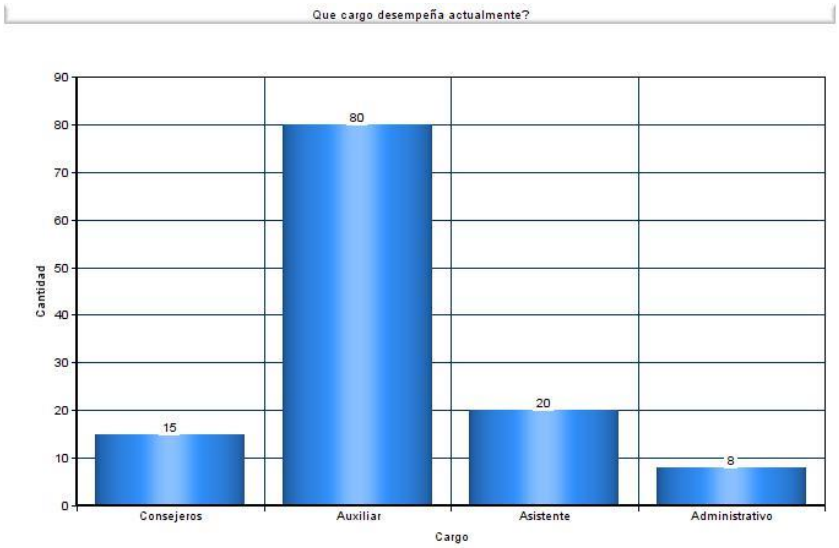
Figura 3. Encuesta.

Fuente: Manuel Charry

6.5 ANÁLISIS DE RESULTADOS DE LA INFORMACIÓN

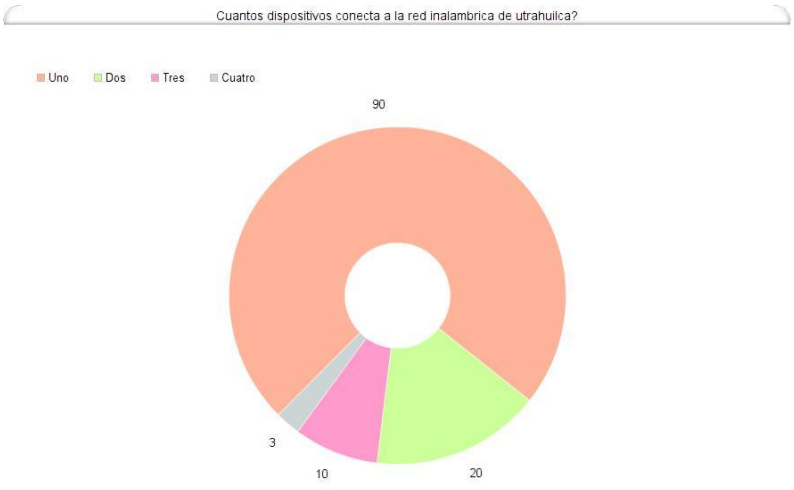
Se obtuvieron los siguientes datos después de tabular por pregunta, y los resultados son los siguientes:

Figura 4. Pregunta 1. Cargo que desempeña



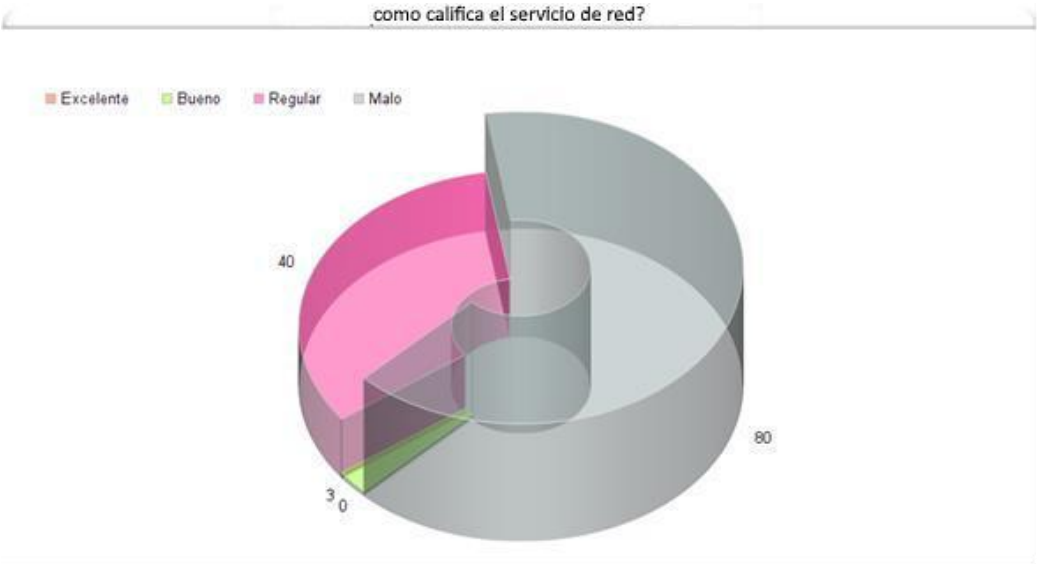
Fuente: El autor

Figura 5. Pregunta 2. Cantidad de dispositivos conectados a la red Utrahuilca



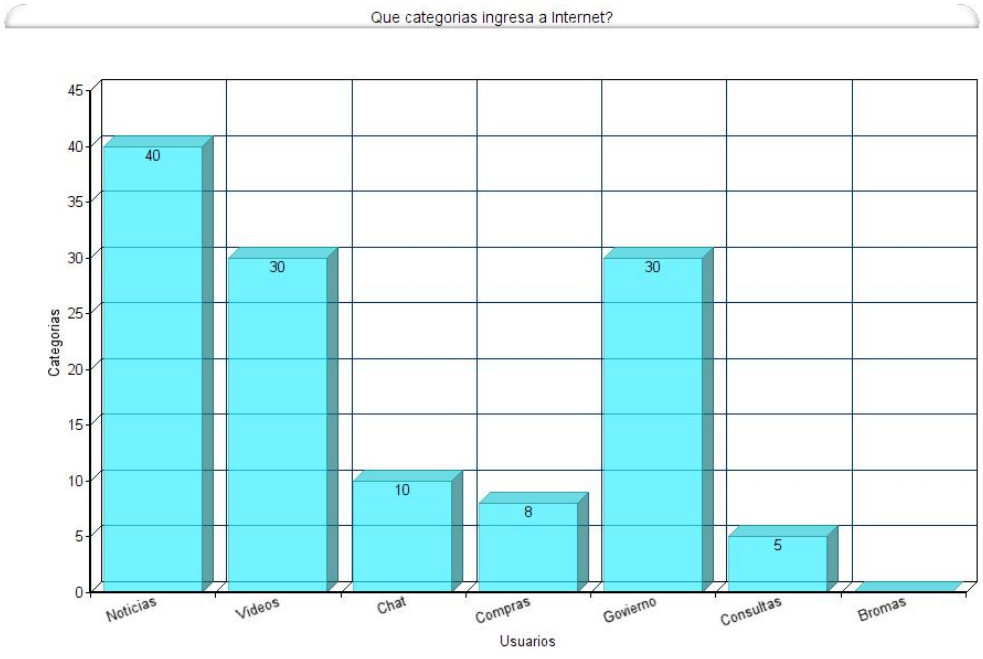
Fuente: El autor

Figura 6. Pregunta 3. Calificación del servicio



Fuente: El autor

Figura 7. Pregunta 4. Categorías de ingreso a internet



Fuente: El autor

Figura 8. Pregunta 5. Percepciones sobre la seguridad en la red

Fuente: El autor

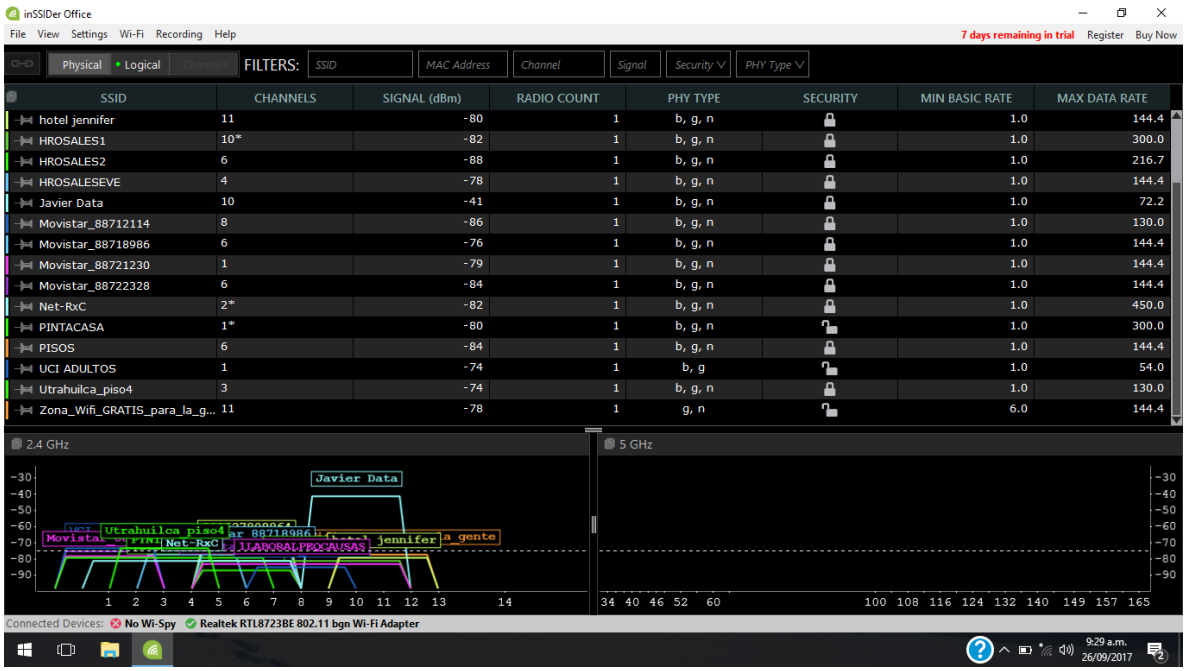
Luego de realizar el muestreo con los resultados obtenidos, el servicio de red inalámbrica de la cooperativa Utrahuilca, se determinó que no cumple con la satisfacción de sus usuarios.

7. ESQUEMA TEMATICO

Se Realizó un análisis exhaustivo a las redes inalámbricas cercanas esto encontrar las redes que estará interfiriendo en la red de igual manera realizar cambio de canal e igual manera solucionar la deficiencia en la señal y para ello utilizamos la herramienta inSSIDer la cual funciona bajo Windows que nos permite detectar por ambiente grafico todas las redes que se encuentran cercanas para encontrar un mejor canal para evitar interferencias en la señal.

Se Realizó pruebas cerca al punto de acceso y encontramos los siguientes problemas:

Figura 3. Verificación de señales redes inalámbricas inSSIDer



Fuente: El autor

Figura 4.Identificacion de canal red inalámbrica Utrahuilca

Fuente: El autor

Podemos identificar que Utrahuilca se encuentra en el canal 3 donde se encuentra la gran mayoría de redes la cual interviene con la intensidad de la señal procedemos a realizar el cambio a canal 4 y con ello podemos ver un gran cambio en la red.

InSSIDer nos permite un análisis más profundo donde muestra que podemos cambiar el tipo de protocolo de 802.11b que es el actual a 802.11n el cual mejora significativamente el rendimiento de la red y optimizándola donde se detecta las posibles ondas electromagnéticas que intervienen en nuestra red.

8. IMPLEMENTACION DE SEGURIDAD

La implementación del sistema de seguridad se da gracias a la infraestructura que posee la cooperativa Utrahuilca permitiendo su instalación y configuración en uno de sus servidores de manera virtualizado, bajo VMware versión 12, su sistema operativo Linux Ubuntu Server 17.04.3 el cual se utilizara para la realización del proyecto en cuestión.

Ventajas:

- su implementación permite un uso más administrable para contraseñas de ingreso a la red de la cooperativa permitiendo que toda la data que se consulta sea segura evitando asi infecciones e inyecciones al sistema tanto como los funcionarios y/o asociados.
- Su contraseña es completamente cifrada para el ingreso al portal.
- Una mayor administración de los ingresos a los sitios web que frecuentan los funcionarios y/o asociados.
- Contraseñas personalizadas para el ingreso al portal cautivo.
- Detección de ataques de inyección en tiempo real y monitoreo.

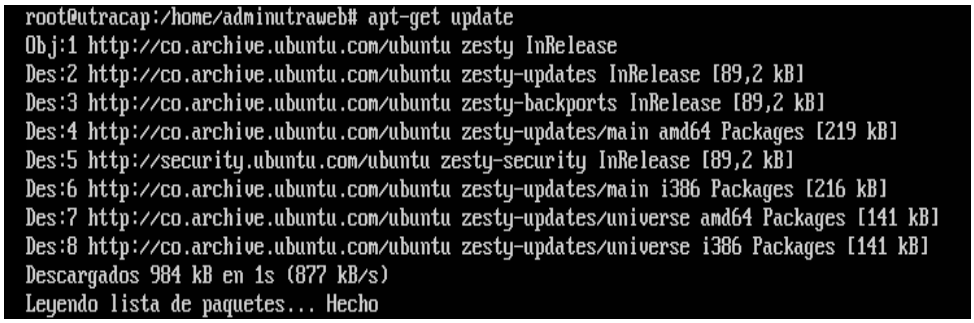
La implementación mejora de manera significativa el uso de los recursos de la cooperativa brindando un mejor servicio a sus funcionarios y/o asociados.

a continuación, se detallará el trabajo realizado:

8.1 INSTALACIÓN SERVIDOR RADIUS

Antes de iniciar el proceso de instalación del servidor Radius procedemos a actualizar el servidor Linux Ubuntu para ello digitamos apt-get update.

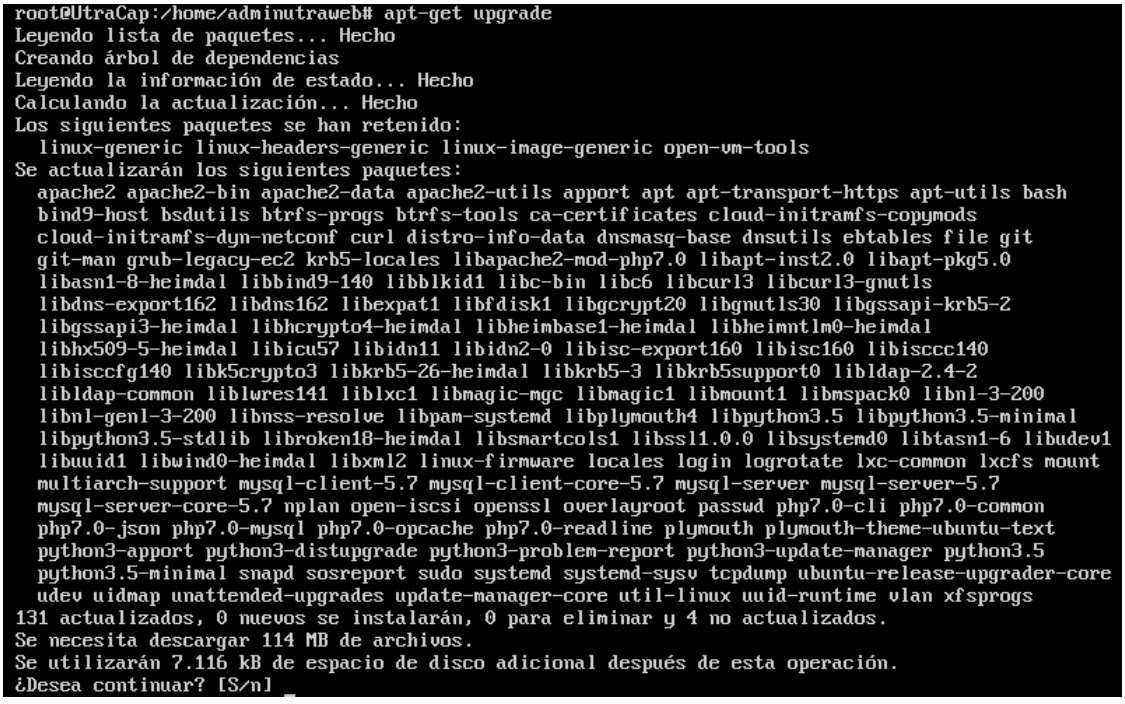
Figura 5.Actualizacion Linux Ubuntu Server



Fuente: El autor

Ahora a aplicar las actualizaciones el servidor Linux Ubuntu para ello digitamos apt-get upgrade

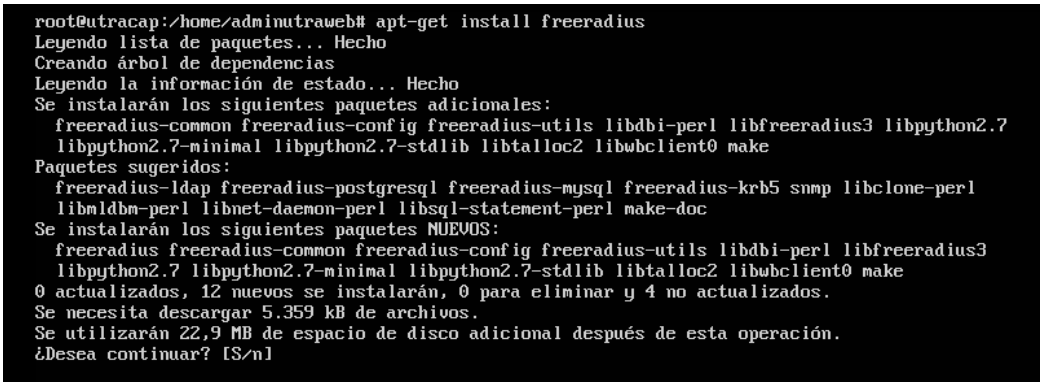
Figura 6. Actualización Linux Ubuntu Server 2



Fuente: El autor

Ahora procedemos a instalar el servidor Radius, utilizaremos el freeradius para la implementación propuesta para ello, ingresamos la siguiente línea de código apt-get install freeradius y presionamos enter.

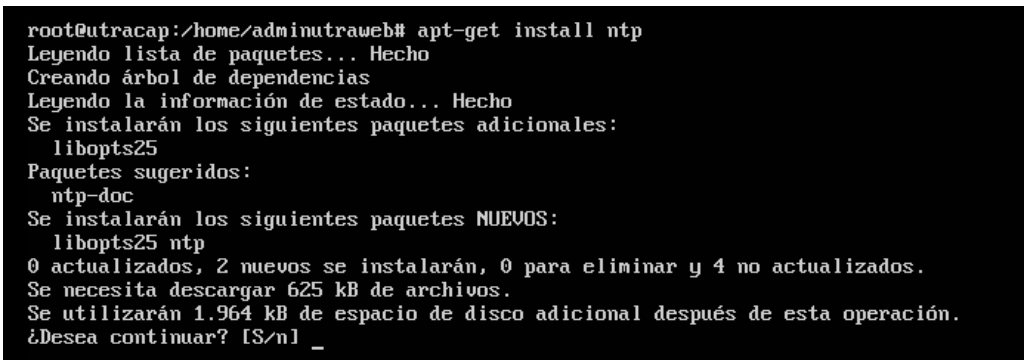
Figura 7.Instalación Servidor Radius (FreeRadius)



Fuente: El autor

Para que la sincronización sea exitosa utilizaremos el servicio de internet NTP el cual nos permitirá sincronizar los relojes de los sistemas de enrutamiento para detectar la red con latencia variable digitamos apt-get install ntp y presionamos enter.

Figura 8.Instalacion Servicio NTP

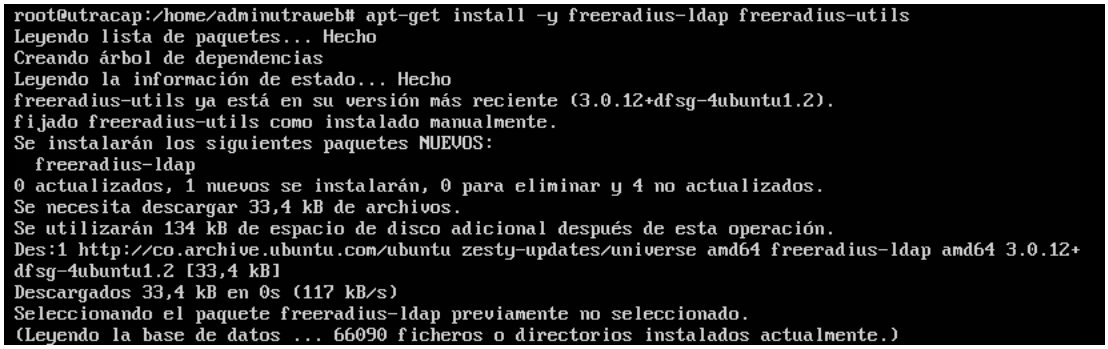


Fuente: El autor

8.2 CONFIGURACIÓN DE SERVIDOR RADIUS

Ahora para un mejor manejo realizamos la instalación con el protocolo ligero de acceso a directorios o LDAP para ello digitamos la línea apt-get install –y freeradius-ldap freeradius-utils y presionamos enter.

Figura 9.instalación de paquetes configuración Radius LDAP



Fuente: El autor

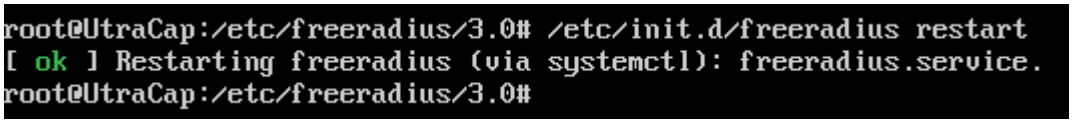
Luego de instalar los paquetes de configuración freeradius procedemos a Instalarlo para ello nos dirigimos a la siguiente ruta digitamos cd /etc/freeradius/3.0/ y buscamos el archivo users para crear nuestro usuario para ingreso digitamos la siguiente línea nano users y ahora digitamos en el editor de texto al final del documento mgonzalez Cleartext-Password := “Sistem2017”.

Figura 10. Creación de usuario en servidor radius.

Fuente: El autor

Luego de crear el usuario reiniciamos el servicio para que tome los cambios digitamos /etc/init.d/freeradius restart.

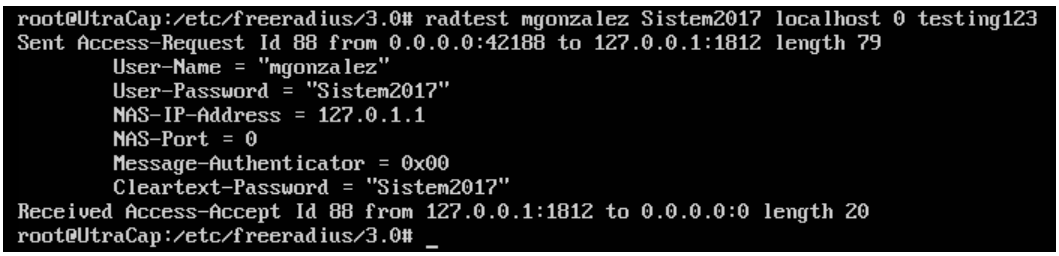
Figura 11.reinicio de servicio radius



Fuente: El autor

Para probar el funciónamelo del servidor radius digitamos la siguiente línea radtest mgonzalez Sistem2017 localhost 0 testing123.

Figura 12. Verificación de funcionamiento radius local.



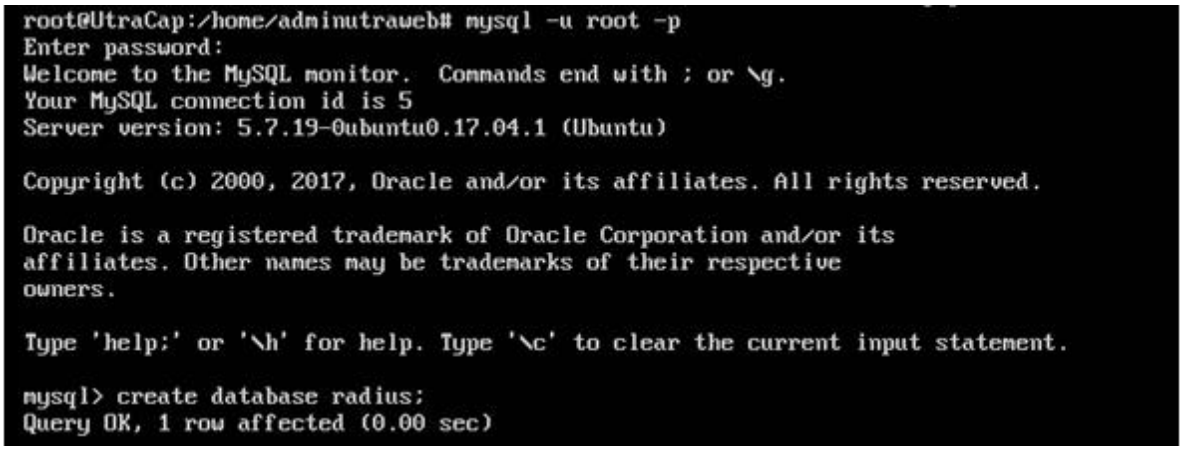
Fuente: El autor

Al realizar la verificación tenemos respuesta exitosa lo cual nos faltaría crear la base de datos donde se almacenara la información de los usuarios y sus respectivas contraseñas para su ingreso a través de un portal cautivo.

Para ello crearemos una base de datos con nombre radius primero iniciaremos el MYSQL con la siguiente línea mysql –u root –p y luego de ello escribimos la contraseña para ingresar al motor de base de datos MYSQL.

Ya dentro de MYSQL ingresamos la línea create database radius; y presionamos enter.

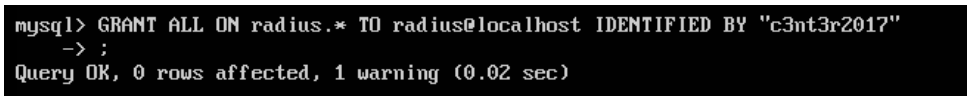
Figura 13.Creación de base datos radius



Fuente: El autor

Una vez creada la base de datos procedemos a crear el usuario que se vinculara al archivo sql.conf de freeradius, digitamos la siguiente línea GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY “c3nt3r2017”; y salimos de MYSQL con exit;

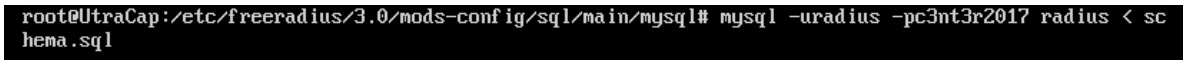
Figura 14.Creación de Usuario radius para base de datos radius



Fuente: El autor

Ahora replicamos el esquema que trae por defecto freeradius a nuestra base de datos anteriormente creada para ello nos dirigimos a la ruta cd /etc/freeradius/3.0/mods-config/sql/main/mysql una vez dentro de la ruta digitamos mysql –uradius –pc3nt3r2017 radius < schema.sql y presionamos enter.

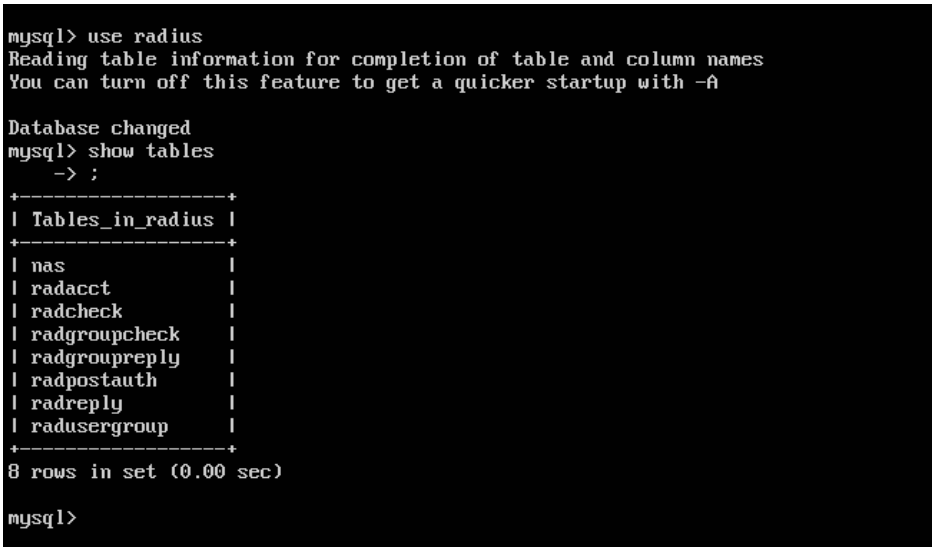
Figura 15.Creación de tablas para base datos radius



Fuente: El autor

Ahora verificamos la creación de las tablas dentro de la base de datos de radius dentro de MYSQL Seleccionamos la base de datos con Use radius y digitamos show tables mostrándonos las tablas creadas.

Figura 16.Verificación del esquema de radius SQL



Fuente: El autor

8.3 INSTALACIÓN SERVIDOR SQUID

Dentro de la cooperativa Utrahuilca tienen una solución de seguridad perimetral o UTM la cual se encarga del filtrado de contenido y otras funcionalidades como:

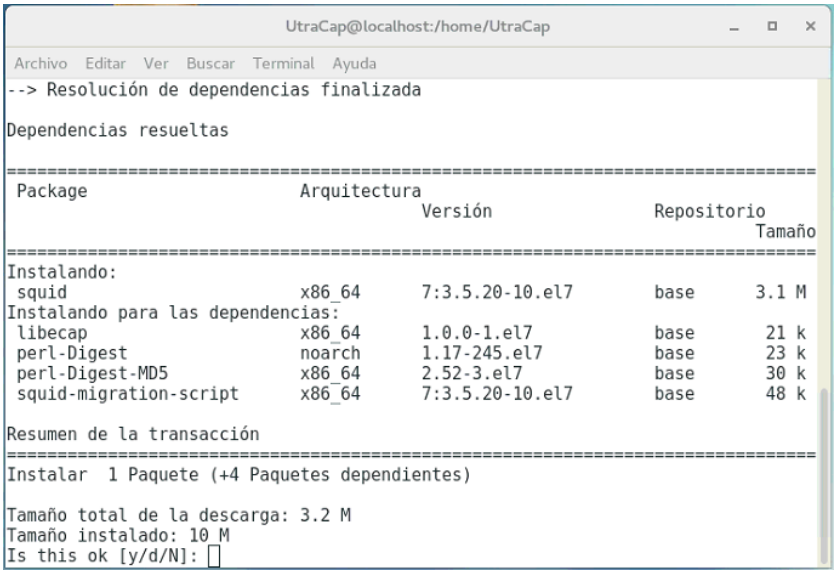
control de aplicaciones: realizando restricciones a aplicaciones web alojadas en internet donde pueden ser fraudulentas permitiendo el robo de informacion.

antivirus y anti spam: protección para evitar sitios con virus y que no ingresen a nuestro sistema.

por lo cual el Squid se encargara de almacenar las consultas realizada por el usuario en cache con el fin de acelerar y optimizar este proceso.

A continuación procedemos con su instalación con la siguiente línea de código para instalar el paquete de Squid **apt-get install squid**

Figura 17. Instalación Squid



Fuente: El autor

8.4 CONFIGURACIÓN DE SQUID

Ahora ingresamos a la ruta **cd.. /etc/squid/** y procedemos a modificar el archivo de configuración del Squid para ello digitamos **nano squid.conf**

En el puerto de proxy agregaremos **transparent**

Figura 18. Modificación a proxy transparente

```
# Squid normally listens to port 3128
http_port 3128 transparent
```

Fuente: El autor

Figura 19. Aumento de almacenamiento web cache

```
# Uncomment and adjust the following to add a disk cache directory.
cache_dir ufs /var/spool/squid 33300 16 256
```

Fuente: El autor

Figura 20. Inclusión de redes Utrahuilca

```
 GNU nano 2.3.1                        Fichero: squid.conf

#
# Recommended minimum configuration:
#

# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 10.0.0.0/8     # RFC1918 possible internal network
acl localnet src 172.16.0.0/12  # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network  - Vlan Utrahuilca
acl localnet src 192.10.0.0/21  # Vlan Wifi Cautivo
acl localnet src fc00::/7       # RFC 4193 local private network range
acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines
```

Fuente: El autor

Figura 21.reinicio de servicio squid

```
[root@localhost squid]# service squid restart
Redirecting to /bin/systemctl restart squid.service
[root@localhost squid]# service squid status
Redirecting to /bin/systemctl status squid.service
● squid.service - Squid caching proxy
   Loaded: loaded (/usr/lib/systemd/system/squid.service; disabled; vendor preset: disabled)
   Active: active (running) since jue 2017-11-23 16:57:16 -05; 1min 6s ago
  Process: 15788 ExecStart=/usr/sbin/squid $SQUID_OPTS -f $SQUID_CONF (code=exited, status=0/SUCCESS)
  Process: 15778 ExecStartPre=/usr/libexec/squid/cache_swap.sh (code=exited, status=0/SUCCESS)
 Main PID: 15790 (squid)
   CGroup: /system.slice/squid.service
           ├─15790 /usr/sbin/squid -f /etc/squid/squid.conf
           ├─15792 (squid-1) -f /etc/squid/squid.conf
           ├─15796 (logfile-daemon) /var/log/squid/access.log
           └─15797 (unlinkd)

nov 23 16:57:15 localhost.localdomain systemd[1]: Starting Squid caching proxy...
nov 23 16:57:16 localhost.localdomain cache_swap.sh[15778]: init_cache_dir /var/spool/squid...
nov 23 16:57:16 localhost.localdomain squid[15790]: Squid Parent: will start 1 kids
nov 23 16:57:16 localhost.localdomain squid[15790]: Squid Parent: (squid-1) process 15792 started
nov 23 16:57:16 localhost.localdomain systemd[1]: Started Squid caching proxy.
[root@localhost squid]#
```

Fuente: El autor

Como se puede observar, se configuró el proxy en modo transparente por lo cual no necesitara alguna configuración adicional para funcionar, por defecto en la configuración detectó la red vlan 192.168.0.0/16 la cual pertenece a la cooperativa y se adiciona la 190.10.0.0/21 que se usará para la red Wifi.

8.5 INSTALACIÓN DE SERVICIO WAF

Nos dirigimos al terminal y digitamos las siguientes líneas

yum -y install epel-release

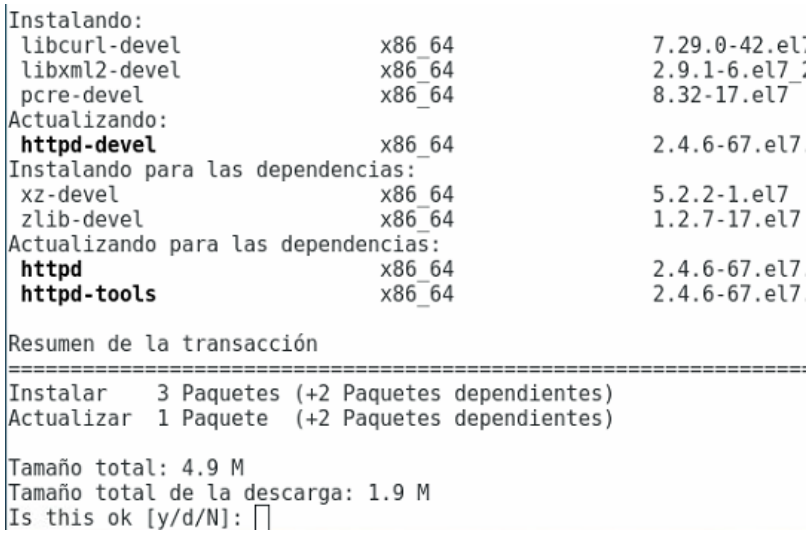
Figura 22. Instalación de epel

Fuente: El autor

Ahora instalamos los paquetes restantes del waf y digitamos las siguientes líneas

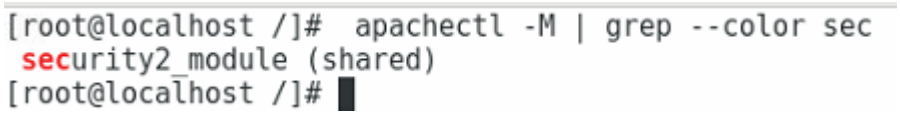
yum install gcc make httpd-devel libxml2 pcre-devel libxml2-devel curl-devel git

Figura 23.instalación de paquetes Waf



Fuente: El autor

Figura 24. Verificación funcionamiento de waf



Fuente: El autor

Ahora verificamos y activamos la opción de **SecRuleEngine** de **Off** a **On**

Figura 25.Configuración de Waf mod_security

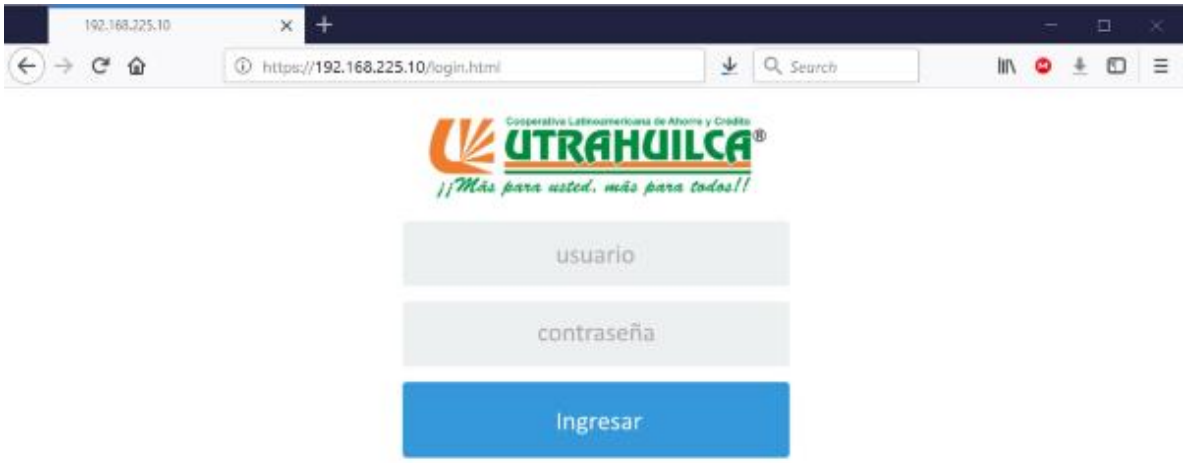
Fuente: El autor

Para verificar su funcionamiento se encuentra en la ruta **/var/log/httpd/modsec_audit.log**

8.6 CONFIGURACIÓN DE PORTAL CAUTIVO

El servidor tiene el siguiente portal cautivo como cliente donde ya se encuentra dentro de la solución y se encuentra configurado para el acceso de WiFi donde solo los usuarios registrados tendrán acceso al sistema.

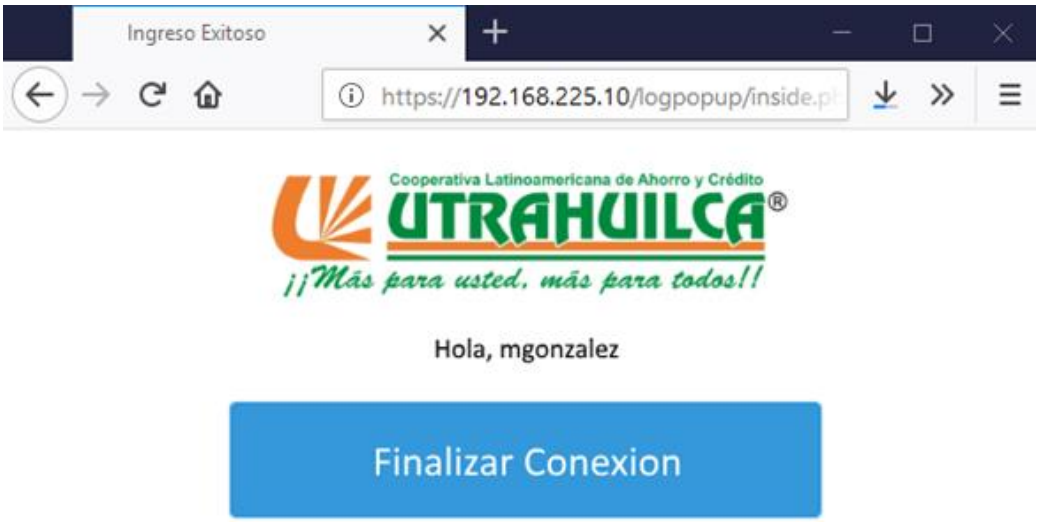
Figura 26.Portal Cautivo Utrahuilca



Fuente: El autor

Cuando el usuario establezca conexión con la wifi y trate de navegar a cualquier sitio será re-direccionado automáticamente al portal cautivo donde se solicitara el usuario y contraseña una vez los datos sean correctos el usuario podrá tener acceso a la red.

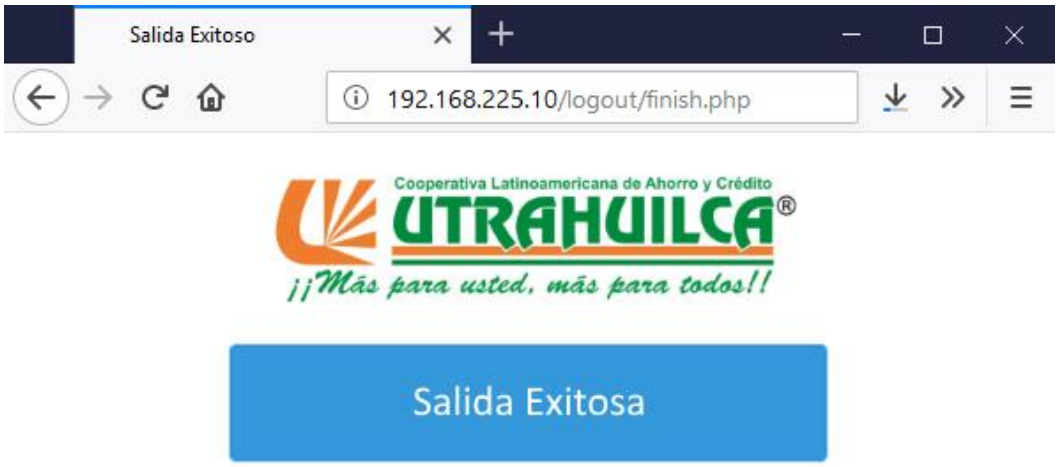
Figura 27.Ingreso Exitoso de portal cautivo



Fuente: El autor

el portal cautivo gracia al gateway, utilizara las reglas de filtrado del firewall, el cual denegara el acceso a la red a usuario sin autorización.

Figura 28.Salida Exitosa de portal cautivo



Fuente: El autor

El gateway valida con el s servidor de autenticación para determinar si el usuario existe verificando en el servidor Radios ya siendo exitosa esta transacción tendrá acceso a la red.

Para verificar las conexiones existentes mediante el portal cautivo nos dirigimos al servidor Radius y en el terminal digitamos la línea **freeradius –X**, a continuación, se presenta un ejemplo de esto:

8.7 RESULTADOS E IMPACTOS ESPERADOS

Al aplicar este proyecto se pudo lograr el aumento de la seguridad de los sistemas informáticos en la cooperativa Utrahuilca, de esta manera, actualmente la Cooperativa Utrahuilca, cuenta con una aplicabilidad integrada al sistema, que permite al usuario tener acceso a una información confidencial, desde la integralidad de la información garantizada, en donde se bloqueará cualquier información inapropiada que pueda incomodar al usuario o dañar su dispositivo móvil.

La Cooperativa Utrahuilca, es la primera en su tipo de organización en Neiva, que tiene un sistema de seguridad de este tipo y producto de un ejercicio de aprendizaje desde la especialización de Seguridad informática, algo que le permite tener tráfico pesado en la red de una manera confiable y amigable con el usuario.

La disponibilidad nos permitirá tener acceso seguro a los datos e informacion para los usuarios autorizados aquello que tengan el ingreso al sistema donde ya se restringen virus y sitios maliciosos en la red.

La integridad ya siendo una red monitoreada podemos idenficar si es alterada la informacion que sea enviada por y para el usuario mejorando el nivel de encriptación del acceso al portal.

Actualmente, la Cooperativa tiene control total sobre la red WiFi, y se ha centrado en la mejora continua desde el servicio que tenían antes y se implementó una forma de disponibilidad del servicio, garantizando el mejor uso de la red a través de autenticación de usuario, con ello se podrá llevar un mejor control de igual manera se puede llevar gestión sobre el uso de red con informes del sistema.

Se espera que este tipo de aplicabilidad contribuya en la seguridad de los usuarios y en los dispositivos móviles, no sólo en la Cooperativa Utrahuilca, sino también en otras entidades que necesitan de canales seguros para el empleo de su información; es decir, que este ejercicio académico llegue a las personas que día a día se conectan a las redes desde la WIFI.

9. PROPONENTES DEL PROYECTO

9.1 PRIMARIOS

Manuel Ricardo González Charry, Ingeniero de Sistemas egresado de la Universidad Cooperativa de Colombia y estudiante de la especialización de Seguridad Informática. Su experiencia profesional está enfocada al desarrollo de software, actualmente trabaja en la Cooperativa Utrahuilca como Desarrollador y es asistente de infraestructura de esta entidad.

9.2 SECUNDARIOS

Docente
JUAN JOSE CRUZ GARZON, Ingeniero de Sistemas, Especialista en Seguridad Informática. 8 años de Experiencia General. Docente Ocasional en el Programa de la Especialización Informática UNAD.

Director
SALOMÓN GONZÁLEZ, Ingeniero de Sistemas, Especialista en Seguridad Informática. Docente en el Programa de la Especialización Informática UNAD.

10. RECURSOS

10.1 RECURSOS MATERIALES

Este proceso lo realiza el ingeniero Manuel Ricardo González Charry quien se encarga de implementar este proyecto según lo pactado contando con la asesoría del Ingeniero Salomón González García y Juan José Cruz Garzón.

10.2 RECURSOS INSTITUCIONALES

La cooperativa Utrahuilca desde la subgerencia, permite el espacio para realizar el trabajo, su infraestructura para la ejecución del proyecto cuya finalidad es la implementación y aplicación de controles de seguridad en su red WIFI.

10.3 RECURSOS FINANCIEROS

Se estima un valor de $ 10.540.000 (DIEZ MILLONES QUNIENTOS CUARENTA MIL PESOS M/CTE) Para la implementación del proyecto los cuales se detallan de la siguiente manera:

Tabla 1. Presupuesto oficial

RUBRO	DESCRIPCION	VALOR EN MILES DE $
Equipo Humano	Líder del proyecto	$ 2.000.000
Equipos y Software	Servidor	$ 5.700.000
Materiales y suministros		$ 2.240.000
Transporte		$600.000
TOTAL		$ 10.540.000

Fuente: El autor

Tabla 2. Descripción del equipo humano.

NOMBRE	TÍTULO	(#HORAS/SEMANA)
Manuel Ricardo González	Ingeniero de Sistemas	10 h/semana
TOTAL		$ 2.000.000

Fuente: El autor

Tabla 3. Descripción de compra de equipos.

DESCRIPCION	JUSTIFICACION	VALOR
Servidor HPE ProLiant DL560 Gen10	Servidor robusto para múltiples operaciones	$ 5.700.000
TOTAL		$ 5.700.000

Fuente: El autor

Tabla 4. Materiales y suministros

MATERIALES*	JUSTIFICACIÓN	VALOR
2 computadores	Equipos para desarrollo	$1.900.000
Resma		$15.000
Escritorio		$200.000
Bolígrafo		$5.000
Silla		$120.000
Internet	Consultoría	$ 100.000
TOTAL		$2.340.000

Fuente: El autor

Tabla 5. Transporte

DESCRIPCION	JUSTIFICACION	VALOR
Transporte	Casa- Oficina- Casa durante 6 meses. Casa-Biblioteca	$600.000
TOTAL		$ 600.000

Fuente: El autor

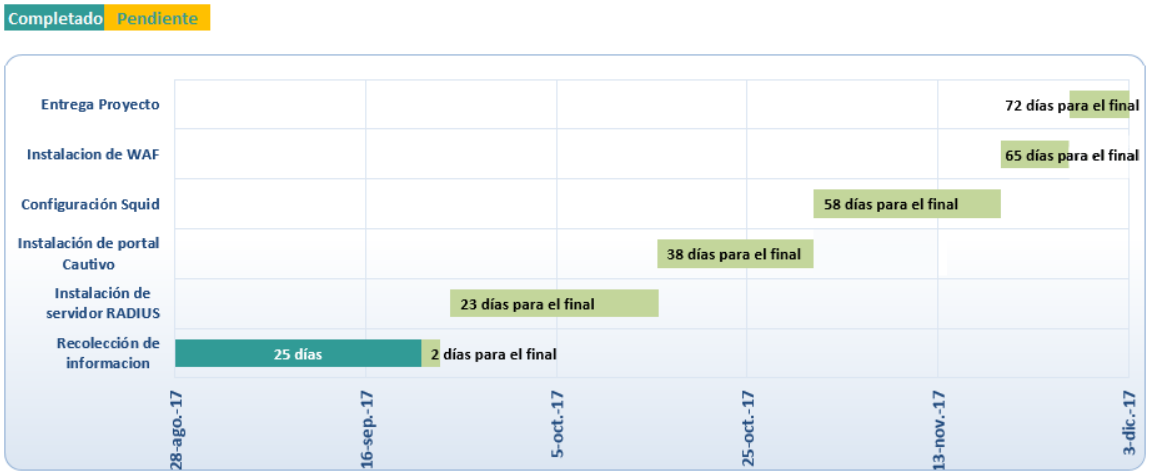
11. CRONOGRAMA

Tabla 5.Cronograma de Actividades.

ACTIVIDAD	MES 1	MES 2	MES 3	MES 4	MES 5	MES 6	MES 7	MES 8	MES 9	MES 10	MES 11	MES 12
Recolección de información												
Instalación de servidor RADIUS												
Instalación de portal Cautivo												
Configuración Squid												
Instalación de WAF												
Entrega de Proyecto												

Fuente: El autor

Figura 29.Grafica Cronograma de Actividades



Fuente: El autor

12. CONCLUSIONES

1. Con la implementación del sistema de seguridad basado en el protocolo de autenticación, autorización y conteo de sesiones para la red WIFI de la Cooperativa Utrahuilca; en el mes de noviembre se minimizaron la descarga de virus en los dispositivos móviles de los usuarios de la red WIFI a partir del bloqueo de proxy que se realizó mediante el portal cautivo.

2. De acuerdo a la aplicabilidad del servicio RADIUS se logró identificar el número de usuarios que acceden a la red WIFI y a empezar un primer momento de control desde el ingreso de cada uno de los usuarios. Se considera que este servidor es funcional y se recomienda su uso para implementar en otras entidades que necesiten este tipo de control.

3. La configuración del portal cautivo permite de manera efectiva el re-direccionamiento de los sitios HTTPS permitiéndoles a los usuarios una navegación segura.

4. Con la implementación de SQUID como proxy se logró administrar el acceso a los sitios considerados inseguros.

5. Al denegar las transacciones inseguras con el Web Application Firewall nos permite que nuestro sistema ingrese a sitios seguros y de igual manera verificar vulnerabilidades en la red de la empresa.

BIBLIOGRAFIA

- Tesis Online

Olmedo, Luis Patiño. Propuesta de Actualización, apropiación, aplicación de políticas de Seguridad Informática en una empresa corporativa, PROPOLSINECOR. UNAD. San Juan de Pasto. 2014. {En línea}. {Consultado el 25 de agosto de 2017}. Disponible en: http://stadium.unad.edu.co/preview/UNAD. php?url=/bitstream/10596/2742/1/129732 10.pdf.

Solarte, Francisco Solarte. UNAD. Popayán. 2014 {En línea}. {Consultado el septiembre de 2017}. Disponible en: http://stadium.unad.edu.co/preview/UNAD.ph p?url=/bitstream/10596/2655/3/7632474.pdf

Arce, Acosta & Posada. Estado Del Arte de La Seguridad Informática. Universidad de Cartagena. 2013 {En línea}. {Consultado en agosto de 2017}. Disponible en: https://es.scribd.com/document/134099136/Estado-Del-Arte-de-La-Seguridad-Informatica

Lasso, Claudia Andrea Urbano. Auditoría en seguridad informática en base de datos del grupo de trabajo de Infraestructura y soporte de tecnologías de la información del departamento para la prosperidad social. Bogotá. 2015 {En línea}. {Consultado en agosto de 2017}. Disponible en: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3717/1/27149612.pdf

Gutiérrez, Ángel. Red inalámbrica - Lo que necesitas saber. 2012 {En línea}. {Consultado el agosto de 2017}. Disponible en: https://www.aboutespanol.com/red-inalambrica-lo-que-necesitas-saber-3507889.

Lehembre, Guillaume. Seguridad de WEP, WPA y WPA2.hakin9 Nº 1/2006. Francia. {En línea}. {Consultado en abril de 2017}. Disponible en: http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf

Romero, Luis Alfonso. Seguridad Informática Conceptos generales. Universidad de Salamanca. 2016. {En línea}. {Consultado en abril de 2017} http://campus.usal.es/~derinfo/Activ/Jorn02/Pon2002/LARyALSL.pdf

- Artículos de Revistas

Ribagorda, Arturo. La protección de datos personales y seguridad de la información. Escuela Politécnica Superior. Universidad Carlos III. Revista Jurídica de Castilla y León. N. º 16. SEPTIEMBRE 2008. Pág. 373-399.

ESET. Guía de Seguridad en redes informáticas. {En línea}. {Consultado en mayo de 2017} https://www.welivesecurity.com/wpcontent/uploads/2014/01/documento_guia_de_wifi.pdf.

INFOMED. Principios fundamentales de la Seguridad Informática. Revista de información a Directivos. Cuba. {En línea}. {Consultado en Julio de 2017} http://www.sld.cu/sitios/infodir/temas.php?idv=1346

FORMATO RAE

1. Información General	
Tema	SEGURIDAD INFORMATICA EN REDES WIFI
Titulo	APLICABILIDAD DE CONTROLES DE SEGURIDAD INFORMATICA QUE GARANTICE LA EFECIENCIA DE LA ADMINISTRACION DEL SERVICIO DE RED “WIFI” DE LA COOPERATIVA UTRAHUILCA. NEIVA, HUILA
Tipo de proyecto	APLICADO
Autor (es)	Manuel Ricardo Gonzalez Charry
Director	Especialista en Seguridad Informática JUAN JOSE CRÚZ GARZÓN
Fuente Bibliográfica	Baca, Gabriel Urbina. Introducción a la seguridad informática. Grupo Editorial Patria. ISBN. 9786077443445. 361 Pág. 2016 Machado, María José Pinilla. Dificultades terminológicas en el proceso de traducción de un texto de seguridad informática. Revista Tonos Digital; Murcia N.º 31, (Jun 2016): 1-22. Muñoz, Mirna; Rivas, Lizbeth. Estado actual de equipos de respuesta a incidentes de seguridad informática/Present state of Response Teams computer security incidents. Revista Ibérica de Sistemas e Tecnologias de Informação; Lousada N.º E3, (Mar 2015): 1-15. Olmedo, Luis Patiño. Propuesta de Actualización, apropiación, aplicación de políticas de Seguridad Informática en una empresa corporativa, PROPOLSINECOR. UNAD. San Juan de Pasto. 2014. {En línea}. {Consultado el 25 de agosto de 2017}. Disponible en: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/2742/1/129732 10.pdf. Ribagorda, Arturo. La protección de datos personales y seguridad de la información. Escuela Politécnica Superior. Universidad Carlos III. Revista Jurídica de Castilla y León. N. º 16. SEPTIEMBRE 2008. Pág. 373-399. Solarte, Francisco Solarte. UNAD. Popayán. 2014 {En línea}. {Consultado el septiembre de 2017}. Disponible en:

	http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/2655/3/7632474.pdf
Año	2018
Resumen	Este proyecto tiene como finalidad documentar e implementar la aplicabilidad de controles de seguridad informática que garantiza la eficiencia de la administración del servicio de red “WIFI” de la Cooperativa UTRAHUILCA, Neiva. Se desarrolló en una empresa asociativa sin ánimo de lucro localizada en el departamento del Huila, especializada en ahorro y crédito enfocado en la economía solidaria con prácticas de principios y valores cooperativos. En el proceso de ejecución, se encontró que la Cooperativa necesitaba un elemento de mejora en el funcionamiento de la red WiFi, mediante de uso de portal cautivo el cual se encuentra seguro con un certificado SSL y la implementación de un web Application firewall, que permite estar protegido de ataques y con el proxy Squid, esta tiene la función de bloquear los sitios no categorizados o malware, siendo así una red segura. Durante el proceso de investigación, se realizó una serie de encuestas, y un análisis de los resultados; además, se verificó la red WIFI y a partir de la información recolectada se configuró un servidor RADIUS con portal cautivo, servidor Proxy SQUID, y un servidor WAF.
Palabras Claves	WIFI, RADIUS, SERVIDORES, PROXY, PORTAL CAUTIVO, SSL, WAF, SQUID
Contenidos	Estos son los temas que se desarrollan desde el diseño y funcionamiento del portal cautivo para la seguridad de la WIFI de la Cooperativa Utrahuilca: En una primera parte, están los antecedentes, la descripción del problema de investigación; luego se complementa con los elementos teóricos y normativos desde el tema en la seguridad informática. Posteriormente, se hace una presentación de la razón de este trabajo para mejorar la calidad del servicio y proteger al usuario. Además, se presenta un compendio de información desde

	cuadros y gráficos que muestran el paso a paso de la implementación del portal cautivo. En el desarrollo de este proceso se encuentra detalladamente cómo fue: la implementación de seguridad; la instalación y configuración de servidor Radius; la instalación y configuración de servidor SQUID; la instalación servicio WAF; la configuración de portal cautivo; y los resultados e impactos.

2. Descripción del Problema de Investigación

La Cooperativa Utrahuilca cuenta con 10 puntos de acceso dentro las instalaciones del edificio, y además cuenta con balanceo de carga, pero su administración no está centralizada. El nombre de red Utrahuilca_piso4, está sementada en una VLAN independiente. Sin embargo, esta red no contaba con la administración adecuada sin ningún control, dejando que el canal de banda ancha se saturara por la cantidad de equipos conectados. Teniendo en cuenta lo anterior, al iniciar el proceso, se recomendó cifrar la conexión con WPA2 teniendo en cuenta los estándares de la IEEE 802.11 para permitir y garantizar el acceso a la red.

Teniendo en cuenta lo anterior, se planteó la pregunta ¿Cómo y qué controles de seguridad informática aplicar para garantizar la eficiencia de la administración del servicio de red “WIFI” de la Cooperativa Utrahuilca de Neiva en el año 2018?

Otro elemento para agregar en la descripción del problema: durante el análisis y en la revisión documental realizada, se encontró que en el contexto local no se han publicado recientemente investigaciones que se especialicen desde el tema de la Seguridad Informática y en este tipo de empresas es necesario promover -desde el conocimiento- el proteger a los usuarios, por lo cual se considera que este proyecto postula un conocimiento nuevo para esta entidad y el departamento del Huila, es válido por la necesidad que presenta la entidad y es útil porque su aplicabilidad es pertinente para la seguridad de los usuarios de la Cooperativa Utrahuilca.

3. Objetivos

OBJETIVO GENERAL:

Aplicar controles de seguridad informática para garantizar la eficacia de la administración del servicio de red “WIFI” de la Cooperativa Utrahuilca de Neiva.

OBJETIVOS ESPECÍFICOS:

Implementar un sistema de seguridad basado en protocolo de Autenticación, Autorización y conteo de sesiones para la red WiFi de la Cooperativa Utrahuilca.

Implementar un servidor RADIUS para la administración de los servicios de autenticación, autorización y conteo de registros de acceso a la red inalámbrica de la cooperativa Utrahuilca.

Configurar un portal cautivo, para re-direccionar el tráfico HTTPS permitiendo el ingreso con autenticación.

Implementar SQUID como proxy para administrar los sitios que se podrán ingresar.

Implementar Web Application Firewall para controlar el acceso a la aplicación web del portal cautivo evitando ataques de inyección.

4. Referentes Teóricos

Se consultaron las monografías y trabajos de grados de la UNAD, de los especialistas Luis Patiño Olmedo, y Francisco Solarte; además se consultaron las fuentes descargadas desde Proquest y revistas indexadas como la revista Tono Digital, desde el aporte de María José Muñoz Pinilla y los aportes de Mina Muñoz y Lizbeth Rivas sobre la seguridad informática, elementos teóricos compartidos desde la revista Ibérica de Sistemas y tecnologías de información.

Referentes de normatividad

También, se incorporaron los elementos básicos de la normatividad Colombiana y Mundial. Ley 1273 de 2009 de delitos informáticos; Y la norma ISO 27001.

5. Referentes Teóricos y Conceptuales

.

Para este proyecto de investigación, se tuvieron en cuenta los siguientes conceptos: Seguridad de la información, las redes inalámbricas y la WEP, a continuación se presentan los elementos conceptuales desde donde se tuvieron en cuenta una serie de aportes de profesionales sobre el tema.

Según Ribagorda Gamacho, “la seguridad de la información es una disciplina de reciente aparición y trata de la protección de ésta frente a revelaciones -accidentales o intencionadas-, a usuarios no autorizados, frente a modificaciones indebidas o frente a destrucciones”

Según Ángel Gutierrez, las redes inalámbricas “se llaman así para distinguirlas de las redes tradicionales por cable o las más modernas de fibra óptica. En una red inalámbrica los datos se transmiten por el aire usando distintas tecnologías”

Según Lehembre la WEP o privacidad equivalente a cableado o Wired Equivalent Privacy “es un sistema de cifrado estándar de la IEEE 802.11 en 1999, perteneciente a las redes inalámbricas permite cifrar los datos. Su cifrado está definido por un algoritmo RC4 de 64 bits, su funcionamiento es por onda radial; con una clave secreta de 40 o 104 bits, combinada con un Vector de Inicialización (IV) de 24 bits para encriptar el mensaje de texto M y su checksum – el ICV (Integrity Check Value)”

6. Resultados y Conclusiones

Resultados:

Al aplicar este proyecto se pudo lograr el aumento de la seguridad de los sistemas informáticos en la cooperativa Utrahuilca, de esta manera, actualmente la Cooperativa cuenta con una aplicabilidad integrada al sistema que permite al usuario tener acceso a una información confidencial, desde la integralidad de la información garantizada, en donde se bloqueará cualquier información inapropiada que pueda incomodar al usuario o dañar su dispositivo móvil.

La Cooperativa Utrahuilca, es la primera en su tipo de organización en Neiva, que tiene un sistema de seguridad de este tipo y producto de un ejercicio de aprendizaje desde la especialización de Seguridad informática, algo que le permite tener tráfico pesado en la red de una manera confiable y amigable con el usuario.

La disponibilidad permitirá tener acceso seguro a los datos e informacion para los usuarios autorizados; es decir, tienen el acceso al sistema donde se restringen virus y sitios maliciosos en la red.

La integridad, ya siendo una red monitoreada se puede identificar si es alterada la informacion que sea enviada por y para el usuario mejorando el nivel de encriptación del acceso al portal.

Actualmente, la Cooperativa tiene control total sobre la red WiFi, y se ha centrado en la mejora continua desde el servicio que tenían en el año 2016 y se implementó una forma de disponibilidad del servicio, garantizando el mejor uso de la red a través de autenticación de usuario, con ello se podrá llevar un mejor control, de igual manera se puede llevar gestión sobre el uso de red con informes del sistema.

Se espera que este tipo de aplicabilidad contribuya en la seguridad de los usuarios y en los dispositivos móviles, no sólo en la Cooperativa Utrahuilca, sino también en otras entidades que necesitan de canales seguros para el empleo de su información; es decir, que este ejercicio académico llegue a las personas que día a día se conectan a las redes desde la WIFI.

Conclusiones:

Con la implementación del sistema de seguridad basado en el protocolo de autenticación, autorización y conteo de sesiones para la red WIFI de la Cooperativa Utrahuilca; en el mes de noviembre del 2017, se minimizaron las descargas de virus en los dispositivos móviles de los usuarios conectados a la red WIFI a partir del bloqueo de proxy que se realizó mediante el portal cautivo.

De acuerdo a la aplicabilidad del servicio RADIUS se logró identificar el número de usuarios que acceden a la red WIFI y a empezar un primer momento de control desde el ingreso de cada uno de los usuarios. Se considera que este servidor es funcional y se recomienda su uso para implementar en otras entidades que necesiten este tipo de control.

La configuración del portal cautivo permite de manera efectiva el re-direccionamiento de los sitios HTTPS permitiéndoles a los usuarios una navegación segura.

Con la implementación de SQUID como proxy se logró administrar el acceso a los sitios considerados inseguros.

Al denegar las transacciones inseguras con el Web Application Firewall permite que el usuario ingrese a sitios seguros y de igual manera verificar vulnerabilidades en la red de la empresa.