UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

"ANÁLISIS DEL MÉTODO DE DUPLICACIÓN DE SESIÓN POR MEDIO DE COOKIES. CASO DE ESTUDIO: PLATAFORMAS DE AUDIO Y VIDEO BAJO DEMANDA POR STREAMING"

PROYECTO DE TITULACIÓN

Previa a la obtención del Título de:

INGENIERO EN NETWORKING Y TELECOMUNICACIONES

AUTOR (ES):

BALLESTEROS CORREA SIMÓN CESAR.

SARMIENTO RONQUILLO FRANCISCO XAVIER.

TUTOR:

ING. EDUARDO ALVARADO UNAMUNO M.SC.

GUAYAQUIL – ECUADOR

2017

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE GRADUACIÓN

TÍTULO Y SUBTÍTULO:	**ANÁLISIS DEL MÉTODO DE DUPLICACIÓN DE SESIÓN POR MEDIO DE COOKIES. CASO DE ESTUDIO: PLATAFORMAS DE AUDIO Y VIDEO BAJO DEMANDA POR STREAMING.**		
AUTOR(ES) (apellidos/nombres):	**Ballesteros Correa Simón Cesar.** **Sarmiento Ronquillo Francisco Xavier.**		
REVISOR(ES)/TUTOR(ES) (apellidos/nombres):	**Ing. Francisco Álvarez M.sc.** **Ing. Eduardo Alvarado Unamuno M.sc.**		
INSTITUCIÓN:	**UNIVERSIDAD DE GUAYAQUIL**		
UNIDAD/FACULTAD:	**FACULTAD DE CIENCIAS MATEMATICAS Y FISICA**		
MAESTRÍA/ESPECIALIDAD:	**INGENIERIA EN NETWORKING Y TELECOMUNICACIONES**		
GRADO OBTENIDO:			
FECHA DE PUBLICACIÓN:		**No. DE PÁGINAS:**	
ÁREAS TEMÁTICAS:	**Networking Telecomunicaciones**		
PALABRAS CLAVES /KEYWORDS:	**Seguridad, Streaming, Magerit. Duplicidad.**		
El proyecto de titulación tiene como objetivo realizar un análisis del método de duplicación de sesión en plataformas Streaming de audio y video, para detectar los riesgos que se pueden acarrear en el momento que los atacantes pueden propagar las sesiones de usuarios en beneficio propio atentando a la confidencialidad de la información. El proyecto en mención tiene implementado un servidor Streaming de prueba para realizar los ataques de duplicidad de sesión demostrando a las organizaciones por medio de una práctica de laboratorio la amenaza que se puede cumplir al no tomar las medidas adecuadas para proteger los logueos del usuario.			
ADJUNTO PDF:	**[x] SI**	**[ ] NO**	
CONTACTO CON AUTOR/ES:	**Teléfono:** **0996787858** **0982266559**	**E-mail:** **simon.ballesterosc@ug.edu.ec** **francisco.sarmientor@ug.edu.ec**	
CONTACTO CON LA INSTITUCIÓN:	**Nombre:**		
	Teléfono:		
	E-mail:		

CARTA DE APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de titulación**, ANÁLISIS DEL MÉTODO DE DUPLICACIÓN DE SESIÓN POR MEDIO DE COOKIES. CASO DE ESTUDIO: PLATAFORMAS DE AUDIO Y VIDEO BAJO DEMANDA POR STREAMING.** Elaborado por el **Sr.** BALLESTEROS CORREA SIMON CESAR Y el **Sr.** SARMIENTO RONQUILLO FRANCISCO XAVIER, **Alumnos no titulados** de la Carrera de Ingeniería en Networking y Telecomunicaciones de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil, previo a la obtención del Título de Ingeniero en Networking y Telecomunicaciones, me permito declarar que luego de haber orientado, estudiado y revisado, la Apruebo en todas sus partes.

Atentamente

ING. EDUARDO ALVARADO UNAMUNO M.SC.

TUTOR

DEDICATORIA

Dedico este proyecto principalmente a Dios, por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional. A mis padres por ser ellos un pilar fundamental en todo el transcurso académico, quienes me demostraron siempre su cariño, apoyo y me alentaron para continuar cuando parecía que me iba a rendir. A mis hermanas Italia, Gabriela, Gloria, Mariuxi que me brindaron que fueron el sostén sin importar nuestras diferencias de opiniones. A mi novia Carol Pacheco quien me apoyo todo el tiempo incondicionalmente. A mi amigo Edwin Cevallos que desde lo más alto me bendice, y a todos aquellos que creyeron en mí en cada paso que daba hacia la culminación de mis estudios.

Simón Cesar Ballesteros Correa.

La presente tesis se la dedico primeramente a Jehová que me dio la fuerza la inteligencia y la salud para poder culminar mi carrera y ser un Profesional, en segundo a mis padres que no perdieron la esperanza y estar ahí siempre que los necesite con su apoyo moral y económico tercero a mis hermanos Fernando y Carlos. A toda mi familia que compartió día a día el trascurso de cada año mi carrera. A las personas que estuvieron presentes directa e indirectamente y aportaron a que este sueño de ser profesional sea una meta más cumplida.

Francisco Xavier Sarmiento Ronquillo.

AGRADECIMIENTO

Agradezco a Dios por protegerme durante todo el camino y darme las fuerzas para superar obstáculos y dificultades a lo largo de toda mi vida. A mis padres por brindarme la oportunidad y el apoyo para culminar una de mis metas profesionales. A mi primer tutor Ingeniero José Maridueña y a mi revisor Ingeniero Eduardo Alvarado por su valiosa guía y asesoramiento a la realización de este proyecto. A mis compañeros que fueron parte de mi equipo de trabajo Francisco, Erik, Milagros, a los Ingenieros Marlon Altamirano y Marcelo Rúales por la colaboración brindada durante este proyecto.

Simón Cesar Ballesteros Correa.

Agradezco primeramente a Jehová por protegerme en todo mi camino para poder culminar los obstáculos profesionales que he tratado en esta vida universitaria. Agradezco la confianza y la voluntad de mi madre Sra. Lucila Ronquillo, por qué siempre estuvo pendiente que no me falte el pan de cada día en mi mesa cuando llegaba muy tarde a mi hogar siempre estuvo como un faro para los navíos que llegue bien. A mi Padre Sr. Carlos Remigio Sarmiento por apoyarme a darme siempre sus consejos sus palabras de aliento y recordar sus palabras que el esfuerzo siempre va traer su recompensa. A mi primer tutor Ingeniero José Maridueña y a mi revisor Ingeniero Eduardo Alvarado que hicieron posible que este proyecto pueda ser terminado de la mejor manera y por la gran calidad humana que ha demostrado y como docente con sus buenas enseñanzas. A mi Equipo de trabajo Cesar, Ingeniero Marcelo.

Francisco Xavier Sarmiento Ronquillo

TRIBUNAL PROYECTO DE TITULACIÓN

Ing. Eduardo Santos Baquerizo, M.Sc.
DECANO DE LA FACULTAD
CIENCIAS MATEMÁTICAS Y FÍSICAS

Ing. José Jacinto Medina, M. Sc
SUBDIRECTOR CINT

Ing. Eduardo Alvarado Unamuno M. Sc
PROFESOR DIRECTOR DEL
PROYECTO DE TITULACIÓN

Ing. Francisco Álvarez, M. Sc
PROFESOR TUTOR REVISOR
DEL PROYECTO DE TITULACIÓN

Ab. Juan Chávez A.
SECRETARIO

DECLARACIÓN EXPRESA

“La responsabilidad del contenido de este Proyecto de Titulación, me corresponden exclusivamente; y el patrimonio intelectual de la misma a la UNIVERSIDAD DE GUAYAQUIL”

Ballesteros Correa Simón Cesar

Sarmiento Ronquillo Francisco Xavier

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

"ANÁLISIS DEL MÉTODO DE DUPLICACIÓN DE SESIÓN POR MEDIO DE COOKIES. CASO DE ESTUDIO: PLATAFORMAS DE AUDIO Y VIDEO BAJO DEMANDA POR STREAMING."

Proyecto de Titulación que se presenta como requisito para optar por el título de

INGENIERO EN NETWORKING Y TELECOMUNICACIONES

Autores:

Ballesteros Correa Simón Cesar
C.I. 2000082111

Sarmiento Ronquillo Francisco Xavier
C.I. 0914049556

Tutor: Ing. Eduardo Alvarado Unamuno, M.Sc

Guayaquil, Octubre de 2017

CERTIFICADO DE ACEPTACIÓN DEL TUTOR

En mi calidad de Tutor del proyecto de titulación, nombrado por el Consejo Directivo de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de

Guayaquil.

CERTIFICO:

Que he analizado el Proyecto de Titulación presentado por los estudiantes Ballesteros Correa Simón Cesar y Sarmiento Ronquillo Francisco Xavier, como requisito previo para optar por el título de Ingeniero en Networking y Telecomunicaciones cuyo tema es:

"ANÁLISIS DEL MÉTODO DE DUPLICACIÓN DE SESIÓN POR MEDIO DE COOKIES. CASO DE ESTUDIO: PLATAFORMAS DE AUDIO Y VIDEO BAJO DEMANDA POR STREAMING."

Considero aprobado el trabajo en su totalidad.

Presentado por:

Ballesteros Correa Simón Cesar — Cédula de ciudadanía N° 2000082111

Sarmiento Ronquillo Francisco Xavier — Cédula de ciudadanía N° 0914049556

Tutor: Ing. Eduardo Alvarado Unamuno, M.Sc

Guayaquil, Octubre de 2017.

UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

Autorización para Publicación de Proyecto de Titulación en Formato Digital

1. Identificación del Proyecto de Titulación

Nombre del Alumno: Ballesteros Correa Simón Cesar	
Dirección: Sauces 3 Mz. 174 V25	
Teléfono: 0996787858	**E-mail**: simon.ballesterosc@ug.edu.ec
Nombre del Alumno: Sarmiento Ronquillo Francisco Xavier	
Dirección: Cdla. Martha de Roldos Mz. 323 V10	
Teléfono: 0982267559	**E-mail**: frascisco.sarmientor@ug.edu.ec

Facultad: Ciencias Matemáticas y Físicas
Carrera: Ingeniería en Networking y Telecomunicaciones
Título al que opta: Ingeniero en Networking y Telecomunicaciones
Profesor guía: Ing. Eduardo Alvarado Unamuno.

Título del Proyecto de Titulación: ANÁLISIS DEL MÉTODO DE DUPLICACIÓN DE SESIÓN POR MEDIO DE COOKIES. CASO DE ESTUDIO: PLATAFORMAS DE AUDIO Y VIDEO BAJO DEMANDA POR STREAMING.

Tema del Proyecto de Titulación: ANÁLISIS DEL MÉTODO DE DUPLICACIÓN DE SESIÓN POR MEDIO DE COOKIES. CASO DE ESTUDIO: PLATAFORMAS DE AUDIO Y VIDEO BAJO DEMANDA POR STREAMING.

2. Autorización de Publicación de Versión Electrónica del Proyecto de Titulación

A través de este medio autorizo a la Biblioteca de la Universidad de Guayaquil y a la Facultad de Ciencias Matemáticas y Físicas a publicar la versión electrónica de este Proyecto de titulación.

Publicación electrónica:

Inmediata	**x**	Después de 1 año	

Firma Alumnos:

Simón Cesar Ballesteros Correa

Francisco Xavier Sarmiento Ronquillo

3. Forma de envío:

El texto del proyecto de titulación debe ser enviado en formato Word, como archivo .Doc. O .RTF y .Puf para PC. Las imágenes que la acompañen pueden ser: .gif, .jpg o .TIFF.

DVDROM [x] CDROM [ ]

INDICE GENERAL

ABREVIATURAS

RTP	Protocolo de transporte en tiempo real
UG	Universidad de Guayaquil
TCP	Protocolo de control de transmisión
UDP	Protocolo de datagrama de usuario
HTML	Lenguaje de Marca de salida de Hyper Texto
Http	Protocolo de transferencia de Hyper Texto
RTSP	Protocolo de transmisión Streaming en tiempo real
CC.MM.FF	Facultad de Ciencias Matemáticas y Físicas
ISP	Proveedor de Servicio de Internet
MITM.	Ataque hombre en el medio
MSc.	Master
URL	Localizador de Fuente Uniforme
www World Wide Web	(red mundial)

SIMBOLOGÍA

S	Desviación estándar
E	Error
E	Espacio muestral
E(*Y*)	Esperanza matemática de la v.a. y
s	Estimador de la desviación estándar
e	Exponencial

INDICE DE TABLAS

INDICE DE GRÁFICOS

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

ANÁLISIS DEL MÉTODO DE DUPLICACIÓN DE SESIÓN POR MEDIO DE COOKIES. CASO DE ESTUDIO: PLATAFORMAS DE AUDIO Y VIDEO BAJO DEMANDA POR STREAMING.

Autores: Ballesteros Correa Simón Cesar
Sarmiento Ronquillo Francisco Xavier
Tutor: Ing. Eduardo Alvarado, M. Sc.

RESUMEN

El presente proyecto de titulación orientado a tecnologías Streaming de audio y video bajo demanda, se determinó que los usuarios suscritos a plataformas de audio y video bajo demanda por Streaming no perciben cuando los piratas informáticos realizan ataques de duplicidad de sesión mediante cookies, en beneficio propio. Para el avance de la investigación se utiliza un marco teórico que permite comprender todas las funciones y conceptos de las tecnologías Streaming bajo demanda y los ataques informáticos que son utilizados por crackers para acceder al contenido multimedia. Para el desarrollo del proyecto se realizó una investigación de campo para la recopilación de información por medio de preguntas de encuesta. Se realizó el planteamiento de la propuesta con el fin de facilitar una guía de buenas prácticas que ayuden a los usuarios a evitar duplicidades de sesión por medio de cookies.

Palabras Claves: Streaming, Cookies, Duplicidad**,** Sesión, Crackers.

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

ANALYSIS OF THE SESSION DUPLICATION METHOD BY COOKIES. CASE STUDY: AUDIO AND VIDEO PLATFORMS UNDER DEMAND BY STREAMING.

Autores: Ballesteros Correa Simón Cesar
Sarmiento Ronquillo Francisco Xavier
Tutor: Ing. Eduardo Alvarado, M. Sc.

ABSTRACT

The present thesis project is oriented towards streaming audio and video on demand technologies. It was determined that the users subscribed to low demand audio and video platforms by Streaming do not perceive when the computer hackers perform cookies duplicity session with the purpose of establishing benefit for them.To advance the research, a theoretical framework is used to understand all the functions and concepts of Streaming technology on demand and the computer attacks that are used by crackers for illegal access to multimedia content. For the development of the project, a field investigation for the collection of information through survey questions was carried out. The proposal was presented in order to facilitate a guide to good practices that help users to avoid cookie duplication sessions.

Keywords: Streaming, Cookies, Duplicity, Session, Cookies.

INTRODUCCIÓN

Desde los inicios de la red de internet en todo el mundo, se han ido integrando diferentes tecnologías para establecer comunicaciones en la red y entretenimiento en ella tales como: mensajería instantánea, juegos en línea, redes sociales, videos conferencias y demás, una de las tecnologías que se ejecuta en el internet que ha tomado crecimiento a nivel mundial con el transcurso del tiempo son los sistemas de audio y video bajo demanda por Streaming, donde los usuarios se conectan a estos servicios para la descarga y visualización de contenido de películas, series de televisión y demás dejando atrás a la televisión tradicional en la cual los mismos acceden al material audiovisual sin importar la fecha u hora que se acceda al servicio.

Las empresas que se dedican a la prestación de servicios Streaming a entornos corporativos y residenciales han evolucionado constantemente por la mayor cantidad de clientes que se suscriben, logrando que las tiendas de video desaparezcan del mercado en donde las ventajas que proporcionan estos servicios Streaming bajo demanda es presentarle al usuario una lista de contenido para que él tome la elección de cual película o cortometraje desea visualizar con el fin de disminuir gastos de material de audio y video al usuario.

El avance de las plataformas Streaming en los distintos entornos ha llegado a que los usuarios puedan visualizar contenido altamente digital con una mejor calidad de imagen y de audio para una mejor escucha suministrando una efectividad en los servicios Streaming con la finalidad de que las compañías que toman a la tecnología Streaming como modelo de negocio puedan obtener mayor publicidad referente productos Streaming que ofrecen aumentado la productividad de la organización, además los servidores Streaming garantizan la disponibilidad de los usuarios para tener al acceso al contenido en cualquier momento.

Actualmente la gran necesidad de estar conectados a los servicios Streaming para efectuar tareas de aprendizaje y entretenimiento durante el transcurso del día se ha llegado a lograr un mayor despliegue en las redes de datos tomando en consideración

el ancho de banda disponible para cada servidor Streaming de audio y video bajo demanda evitando que no exista latencia en el servidor multimedia.

Con la aparición de nuevas redes en las últimas décadas tales como las redes inalámbricas con sus estándares IEEE 802.11a, b, g y n, las redes móviles con las respectivas arquitecturas 3G (UMTS), 4G (LTE) y 5G (LTE-A) los sistemas Streaming han convergido en todas estas redes de telecomunicaciones, dándole la oportunidad al usuario de estar conectados a los servicios Streaming de audio y video desde dispositivos móviles como Laptops, Tablets y Smartphone de una manera óptima y eficiente aumentado el nivel de entretenimiento de ellos.

A continuación se detallara los puntos a desarrollar en cada capítulo del proyecto de titulación referente al análisis del método de duplicidad de sesión en las plataformas Streaming de audio y video bajo demanda.

En la etapa del Capítulo I se indica el planteamiento del problema, las causas y consecuencias, el alcance del problema, los objetivos de la investigación y la justificación e importancia de la investigación para establecer una solución a la problemática presente.

En el Capítulo II se realiza el desarrollo del proyecto de investigación referente al análisis del método de duplicidad de sesión en las plataformas Streaming de audio y video, las funcionalidades de la plataforma de prueba a utilizar y las definiciones de cada término convergente a los sistemas Streaming de audio y video.

En el Capítulo III se define la metodología de análisis y gestión de riesgos MAGERIT, la población, la muestra y los instrumentos de recolección de datos que serán utilizados para la recopilación de la mayor cantidad de información referente a las plataformas Streaming bajo demanda.

En este último Capítulo IV se realizara un análisis de factibilidad que determine la viabilidad del proyecto, los entregables del proyecto, los criterios de validación de la propuesta y los criterios de aceptación del producto para identificar la aceptación de la

propuesta y que los usuarios la tomen como modelo para evitar duplicidades de sesión de usuarios con la finalidad de atentar a la confidencialidad de la información.

CAPÍTULO I

EL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

1.1.1 Ubicación del Problema en un Contexto

La revolución de las tecnologías de la información y comunicación han generado un verdadero cambio en el comportamiento de los usuarios, en la forma de llevar un nuevo estilo de vida en aprender, conocer, visualizar un contenido satisfactorio de acuerdo al entorno de trabajo cotidiano, utilizando tecnologías para accesar a un material audiovisual de bajo costo o gratuito. El buen uso de estas tecnologías puede ahorrarnos tiempo y dinero, acelerando las tareas y trabajos colaborativos en tiempo real. Un usuario residencial o corporativo puede ejecutar labores a través de un ordenador o dispositivo móviles inteligentes desde cualquier punto de la ciudad o país, sin la necesidad de trasladarse de un lugar a otro. Esta experiencia virtual se consigue gracias a las aplicaciones de sistemas avanzados de Streaming de audio y video que permiten ver y escuchar al interlocutor con una alta calidad del material audiovisual, simulando su presencia real y convirtiendo el ambiente en un entorno participativo. Los sistemas de “Live Streaming” y “Video bajo demanda” son aplicaciones avanzadas de difusión de contenido multimedia a través de un navegador web, ofreciendo facilidad de uso y acceso al servicio y contenido del mismo.[1]

Las Plataformas Streaming bajo demanda que son integradas en redes de internet, aplicaciones móviles, generan una gran demanda de clientes suscriptores, donde los mismos pueden tener acceso al contenido basado en largometrajes, cortometrajes, series de películas sin la necesidad de adquirir un plan de televisión pagada. Las transmisiones en tiempo real de contenido multimedia (Live Streaming) son uno de los servicios más solicitados por instituciones de carácter académico, financiero, socio-económico y habitantes de una comunidad, debido a que permiten la difusión de contenido bajo demanda sobre ambientes y entornos a través de la red de Internet.[1]

¿Pero serán seguras estas Plataformas de Streaming bajo demanda?

En la realidad estas plataformas no son seguras ya que atacantes maliciosos pueden duplicar sesiones de estas utilizando cookies en los navegadores de internet, facilitando este robo de ficheros de sesión mediante la realización de un ataque hombre en el medio ejecutando un proceso de captura de tráfico de red, utilizando herramientas adecuadas como por ejemplo el Ettercap. Debido a su naturaleza, estos servicios de audio y video Streaming dan lugar a nuevos desafíos de seguridad donde esta tecnología es susceptible a este tipo de ataque en el cual los crackers aprovechan estos fallos de seguridad presentes en los servidores para hacer daño a su objetivo, ocasionándole pérdidas económicas a las compañías que ofrecen este tipo de servicio, distribuyendo el contenido de manera ilegal con fines lucrativos.[2]

Con el análisis del método de duplicación de sesión por medios de cookies facilitado por un ataque hombre en el medio cuya funcionalidad es capturar el tráfico tanto para redes de área local y redes inalámbricas para tener acceso a todo el contenido almacenado en los servidores Streaming.[2]

En estos servicios también se derivan las expresiones de forma clausurada para la probabilidad de que el abonado de bajo pago y usuarios maliciosos intercepten los paquetes codificados donde estos sean capaces de experimentar la calidad de video más alta y su vez el acceso al servidor de manera ilegal.[3]

Este nuevo boom de televisión y audio por internet facilita a los usuarios poder estar conectado desde cualquier parte del mundo y disfrutar de la programación que tiene integrada las Plataformas Streaming en donde se autentica el usuario por medio de la red utilizando dispositivos móviles, computadora personal y demás equipos que nos ayuden a visualizar y escuchar este contenido. Las empresas que brindan el servicio de Streaming no poseen las medidas de seguridad por la cual los crackers pueden accesar a sus plataformas por medio de técnicas de navegación y causar perjuicios

económicos a las organizaciones y clientes suscriptores.

1.1.2 Situación Conflicto. Nudos Críticos

El uso de plataformas Streaming bajo demanda es cada vez más frecuente en el internet y su implementación han aportado nuevos retos a la comunidad científica, este servicio es provisto por un servidor el cual consiste en una aplicación que espera, procesa y sirve peticiones de uno, o varios clientes, esta solicitud contiene un comando donde el cliente solicita el contenido audiovisual que desea observar.[4]

Al no cumplirse con un control de sesión dinámico en los servidores de Streaming de audio y video bajo demanda (integrado con el protocolo RTSP y RTMP), que permite el ahorro al máximo del ancho de banda disponible por el cliente para descargar y visualizar el contenido, ocasiona un problema en el uso del ancho de banda necesario para ir reproduciendo el material en tiempo real.[5]

Muchas de estas organizaciones dedicadas a la prestación de servicios de audio video Streaming bajo demanda no tienen conocimiento las vulnerabilidades existentes en sus aplicaciones web enfocadas en contenido audiovisual de consumo para clientes suscriptores, debido a esto los ataques MITM tienen un gran crecimiento constante en el mundo, donde cuya finalidad, los atacantes que ejecutan este tipo de intrusión es degradar los niveles de fiabilidad de una empresa que presta este tipo de servicios. Los ataques MITM[1] consisten en capturar el tráfico de toda la red, en los servidores web generalmente escrito en JavaScript a través de las operaciones o parámetros descritos en el WSDL del objetivo, los cookies robados por los crackers se pueden utilizar para sustraer la información de carácter sensible, duplicar sesiones de usuario, y poner en peligro el servidor, atacando la integridad del sistema de video Streaming.[2]

Esta vulnerabilidad se produce cuando una aplicación web no emplea un túnel de cifrado para la encriptación del tráfico donde circula la información de los servidores de las compañías que proporcionan este servicio y páginas generadas dinámicamente.

---

[1] **MITM:** Man in the Middle

Varias empresas e instituciones que brindan servicios Streaming tienen la mayor parte de sus contenidos audiovisuales indexados por la cual estos aparecen entre los resultados de búsqueda en la red donde las personas que navegan en internet encuentran el acceso directo al contenido establecido y este a su vez no se mantiene anónimo y confiable.

1.1.4 Causas y Consecuencias del Problema

Tabla 1 Causas y Consecuencias

Causas	Consecuencias
Actualmente los servidores Streaming de audio y video bajo demanda manejan cookies de sesión el cual es enviado y alojado en los navegadores de internet.	**Crecimiento de los ataques MITM ejecutados por usuarios externos para la captura de cookies de sesión con esto realizar duplicaciones de las mismas a los clientes suscriptores de estas plataformas de servicio Streaming.**
La falta de un túnel de cifrado en la aplicación web enfocada en contenido audiovisual recibida por los usuarios suscriptores.	**Se producen vulnerabilidades de seguridad en las aplicaciones web.**
Poco control de sesiones dinámicas en las plataformas Streaming.	**Esto facilita al atacante realizar el ataque ya que no existe un doble procedimiento que valide al usuario legítimo en el sistema en mención.**
Distribución de cookies de sesión por parte del atacante de manera ilícita.	**Degradan el nivel económico y el grado de fiabilidad de las compañías dedicadas este servicio ya que su contenido es distribuido de manera ilegal.**

Fuente: Trabajo de investigación
Autores: Simón Ballesteros – Francisco Sarmiento

1.1.5 Delimitación del Problema

- **Campo:** Redes
- **Área:** Telecomunicaciones
- **Aspecto:** Seguridad informática en plataformas Streaming
- **Tema:** Análisis de duplicación de sesión por medio de cookies. Caso de estudio: Plataformas de audio y video bajo demanda por Streaming.

1.1.6 Formulación del Problema

La duplicación de sesión por medio de cookies de un cliente suscriptor de servicio Streaming de audio y video bajo demanda, ¿es una amenaza, para el usuario final?

1.1.7 Evaluación del Problema

En la evaluación del problema planteado sobre los ataques a las plataformas de Streaming bajo demanda se seleccionaron seis aspectos que se adaptan al proyecto de titulación a desarrollar.

Los aspectos generales de evaluación son:

Delimitado: Se podrá realizar una sustracción de credenciales de usuario, con el apoyo de la herramienta Evil Foca instalada en el sistema operativo Windows para llevar a cabo el respectivo ataque MITM obteniendo el tráfico de sesión y luego ser ejecutados en los navegadores de internet, logrando el acceso sin autenticación, una vez alcanzado dicho salto se podrá llevar a cabo el análisis del método de duplicación por medio de cookies y así dar a conocer al usuario sobre los riesgos presentes.

Concreto: Poseer la confiabilidad de los procesos de autenticación integrados en los sistemas Streaming y aplicar técnicas de protección para que los usuarios correspondientes solo tengan acceso al contenido audiovisual sin que terceros sepan del mismo material en mención.

Original: En la actualidad existen diversos métodos de duplicación de sesión tales como inyección de cookies en los navegadores y acceso por URL maliciosa permiten el salto de logueo. Sin embargo, esto no sería posible sin previa captura del tráfico mediante un ataque MITM ejecutado por el atacante.

Contextual: En la comunidad educativa y social la seguridad informática es cada vez deficiente por lo cual existen muchas falencias en las plataformas de servicios Streaming bajo demanda, debido a que atacantes externos pueden tener acceso ilegal al servicio de Streaming de contenido videotecario proporcionando el material de estudio a entidades educativas perjudicando a las empresas económicamente.

Factible: El proyecto de investigación se lo determinó factible por la cantidad de riesgos que pueden acarrearse al momento de que las empresas dedicadas a la prestación de servicios Streaming bajo demanda no poseen un sistema de detección referente a las duplicaciones de sesión de un usuario para la cual que utilizará diferentes herramientas que permitan analizar el método de duplicidad de sesiones que están integradas en sistemas operativos de código abierto, enfocados a la seguridad informática para implementar los ataques respectivos y así detectar fallos que estén afectando al positivo proceso de autenticación y a los activos económicos que poseen las organizaciones dedicadas a este tipo de servicios.

Identifica los productos esperados: Con los resultados que se obtendrán en el análisis del método de duplicación por medio de cookies se aplicaran técnicas de recomendación para efectuar los controles adecuados para que los sistemas Streaming bajo demanda estén protegidos.

1.1.8 Alcances del Problema

En el proyecto de investigación piloto se utilizara un ambiente de prueba basado en el análisis de duplicación de sesión por medio de cookies implementando una plataforma de audio y video bajo demanda por Streaming la cual es montada en un sistema operativo orientado a servidor, donde con esta se realizaran pruebas de ataque para la sustracción de cookies de sesión almacenadas en el navegador de un usuario.

Para realizar el ataque en el ambiente de prueba referente al análisis del método de duplicación de sesión por medio de cookies se utilizaran 3 herramientas de código abierto, que ayudaran a la obtención de la cookie de sesión, para la importación del fichero usaremos 2 navegadores de internet, estas herramientas facilitaran las máximas funcionalidades para la ejecución de este análisis de duplicidad y así verificar los fallos

que pueden estar expuestos en el servidor Streaming local de bajo demanda y poder dictaminar los controles adecuados para evitar que los atacantes maliciosos tengan acceso a los servicios Streaming de manera no autorizada.

Una vez obtenida la cookie de sesión se realizara la duplicación de sesión, detallando en un informe el resultado y el problema que ocasionara dicha duplicidad que pueden establecer los crackers para tener el acceso al contenido audiovisual de manera ilícita distribuyéndolo con un fin de lucrarse del servicio.

Así mismo se adjudicara una guía de buenas prácticas para el uso de mecanismos de protección para evitar la duplicidad de sesión.

1.2 OBJETIVOS DE LA INVESTIGACIÓN

1.2.1 Objetivo General

Realizar un análisis del método de duplicación de sesión, utilizando cookies en navegadores de internet para las Plataformas de audio y video bajo demanda por Streaming.

1.2.2 Objetivos específicos

1. Analizar las pruebas de duplicación de sesión en la plataforma de Streaming de audio y video bajo demanda de prueba.

2. Elaborar un informe sobre las pruebas de duplicación de sesión en la plataforma de audio y video Streaming bajo demanda de prueba.

3. Establecer planes de acción adecuados para llevar un control de acceso sobre estos servicios de Streaming bajo demanda de audio y video.

1.3 JUSTIFICACIÓN E IMPORTANCIA DE LA INVESTIGACIÓN

Con la ejecución del análisis de duplicación de sesión por medio de cookies utilizando las herramientas adecuadas, estas proporcionaran todas las funciones y características del buen uso y manejo de ellas, para verificar el estado de seguridad del servicio Streaming, así las compañías dedicadas a brindar dicho servicio aplicarían planes de capacitación para que el usuario se proteja de los robos de sesión y de contenido tomando los respectivos controles para restringir el mismo a usuarios que intenten hacer daño a la organización.

Como recomendación de seguridad se utilizaría un navegador de cifrado, para que las mismas tengan sus activos lógicos protegidos y los usuarios que estén suscritos a estas plataformas Streaming tengan acceso al contenido de manera encriptada, creando dificultades a los atacantes que intenten tener acceso al material audiovisual de manera ilegal, con la ejecución de un navegador de cifrado del lado del usuario luego de una campaña por parte de la empresa que brinda el servicio, estas plataformas en mención serán más seguras y confiables, obteniendo un adecuado control del mismo para evitar cualquier problemática que se genere con este tipo de casos de duplicación de sesión.

Muchas de los navegadores de internet que son utilizados para el acceso y ejecución de las plataformas Streaming no proporcionan la seguridad adecuada para mitigar o tener los riesgos presentes bajo control, donde los ataques de duplicación de sesión en mal uso pueden ocasionar un degrado económico en las organizaciones dedicadas a la prestación de estos servicios.

La mayor parte de los usuarios no poseen el conocimiento sobre las tecnologías Streaming de pago, mucho de ellos acceden al internet para navegar en redes sociales, efectuar transacciones en línea y demás, en muchas ciudades del mundo estas plataformas han generado los mayores éxitos debido al contenido que promocionan, las empresas dedicadas a estos servicios establecen convenios con compañías productoras para publicar las novelas, películas, series de televisión y demás hacia los usuarios suscritos y con esto poder generar ganancias económicas y popularidad. Pero en realidad deben protegerse estos servicios para disminuir los actos delictivos que

intenten piratear el material audiovisual de las organizaciones causando un declive financiero en ellas donde los atacantes buscan los mayores beneficios al distribuir estos contenidos.

Uno de los principales factores de un análisis del método de duplicación por medio de cookies es tener el acceso al contenido bajo demanda por parte del atacante informático hacia el usuario suscrito y verificar el mismo por categoría de uso alta, media y baja en beneficio propio. La investigación a desarrollar cuya finalidad es obtener resultados, en la captura de sesiones de usuarios, y activar los mecanismos de seguridad para salvaguardar los activos.

El análisis del método de duplicación de sesión en las Plataformas Streaming bajo demanda nos ayuda a definir los respectivos controles en la cual podemos implementar mecanismos de seguridad para evitar que los atacantes maliciosos inyecten cookies en los navegadores y tengan acceso de manera ilícita a las plataformas de contenido audiovisual de pago, configurando y actualizando las versiones de los navegadores en los distintos Sistema operativos, para reducir el nivel de amenaza expuesto en los sistemas de autenticación integrados en los servidores Web de contenido Audiovisual bajo demanda. Además este análisis nos permite como deshabilitar las opciones de introducir códigos maliciosos o cookies en los navegadores de internet para tener los servicios Web de manera segura.

Con la asistencia de un ataque informático daremos una perspectiva de todo el tráfico capturado, categorizando la información interceptada para aplicar las soluciones de seguridad adecuadas y que proporcionen al usuario un nivel de confiabilidad de acceso a las plataformas Streaming de audio y video desde cualquier punto de conexión a internet.

Transmitir los contenidos audiovisuales como películas, series de televisión, novelas y cortometrajes vía Streaming, podemos ver el incremento de usuarios de forma significativa, la presencia en línea de las organizaciones que transmiten el material por internet aplican la combinación entre un servicio profesional de Streaming como el realizado por las televisoras locales y privadas, asegurando que el contenido llegará a

la mayor cantidad de público objetivo, sumando a los que lo verán diferido bajo demanda, es decir que existe un aumento considerable de captación.

Los servicios Streaming son canales de gran importancia, efectivo y rentable, renunciando a los costos exorbitantes de las transmisiones televisivas tradicionales.

Actualmente algunas organizaciones dedicadas a la tecnología Streaming transmiten contenidos de audio y video bajo demanda demostrando que cuando la transmisión se realiza de una forma profesional, la credibilidad de las empresas aumenta, crecen las visitas en la web y definitivamente el aumento de clientes potenciales es significativa.

Hoy en día las herramientas digitales, como lo son las redes sociales y demás son utilizadas para efectuar transmisiones por Streaming, creando una conexión entre el público y la organización que está transfiriendo el material audiovisual, convirtiendo de esta forma la transferencia en una plataforma de comunicación interactiva y bidireccional.

Es importante recordar que las transmisiones vía Streaming son públicas y privadas, en caso de las plataformas de Streaming bajo demanda de pago el acceso es restringido por medio de filtros de paquetes, donde solamente el contenido es difundido a los usuarios suscriptores, asegurando que los paquetes de audio y video sean captados únicamente por el público deseado.

Durante las transmisiones de audio y video bajo demanda, dichas transmisiones son monitoreadas por un gran número de datos, que posteriormente son utilizados para mejorar la planificación de estrategias, para conocer la cantidad de usuarios que visualizan la transferencia y su localización.

En ambientes corporativos, las transmisiones vía Streaming facilitan el ahorro significativo enfocado en costos, es decir que las organizaciones adoptan por realizar anuncios sobre noticias a diferentes áreas, evitando desplazamientos innecesarios.

CAPÍTULO II

MARCO TEÓRICO

2.1 ANTECEDENTES DE ESTUDIO

Según Hugo Javier Ortega Bernal estudiante de la Universidad Católica del Perú detalla que el mundo posee un alto nivel competitivo en donde las empresas buscan constantemente medios tecnológicos que transmitan mensajes con contenido audiovisual a los clientes con mayor una eficiencia y efectividad, esta exigencia se manifiesta en el pedido en la información, no solamente se transmite local sino en toda la red de internet, para que los usuarios de diferentes naciones obtengan el acceso a la información en tiempo real y de una manera visualizada rápida y eficiente. Con el fin de satisfacer los requerimientos de la Internet, se presenta como un medio de comunicación alterna que busca cumplir con las necesidades, por lo que se han incrementado, estudios basados demuestran en poner todos los medios de comunicación sobre la Internet, como la televisión se alcanza a disminuir los costos de adquisición de canales por partes de las operadoras de cable. La constante evolución de las redes y telecomunicaciones ha desarrollado el Streaming como el instrumento para transmitir voz y video en tiempo real de una manera eficiente.[6]

Según estudios realizados por la Ingeniera en Telecomunicaciones Laura Pozueco Álvarez menciona que actualmente se han supuesto un gran cambio en cuanto a la forma de consumo de contenido audiovisual de una manera frecuente que el usuario elija al instante y el lugar para visualizar sus contenidos de películas, series y demás. Este fenómeno supone un desplazamiento de la televisión tradicional hacia el consumo multimedia en Internet.[7]

En los primeros años la transmisión de contenidos por Internet normalmente implicaba protocolos UDP[2] y RTP/RTSP, la aplicación era probablemente una sesión de video en

---

[2] **UDP:** Protocolo mínimo de nivel de transporte

tiempo real que, debido a la sensibilidad a la latencia de paquetes y la fluctuación de fase, esto no llego a ser muy notorio. Los materiales de audio y video bajo demanda basada en Internet comenzaron como descargas de archivos simples, esto aumento la popularidad de ver los videos a través de Internet con el transcurso del tiempo, los métodos de audio y video han evolucionado como la descarga progresiva, que permite que la reproducción de vídeo comience antes de que lleguen todos los datos y después fue reemplazada recientemente por técnicas de audio y video adaptativas dinámicas que permiten cambiar el contenido de vídeo de forma instantánea. Adobe, Apple, Microsoft, Netflix y las comunidades inalámbricas 3GPP han desarrollado métodos propietarios para la transmisión adaptativa basada en protocolo TCP. En el año 2009, la ISO solicitó propuestas para un marco basado en estándares para apoyar Dynamic Adaptive Streaming sobre HTTP (DASH). La norma fue ratificada en diciembre de 2011. La comunidad 3GPP finalizó recientemente su variante DASH que está optimizada para entornos inalámbricos.[8]

En la actualidad las plataformas de contenido audiovisual como Netflix, Viki, Hulu, Crackle entre otros son los principales proveedores de servicios de Streaming de vídeo basados en suscripción para películas, series, novelas y programas de televisión. En abril del 2014, estas organizaciones como Netflix han atraído al más de unos 35 millones de abonados en Estados Unidos y alrededor de 48 millones en todo el mundo. Los servicios Streaming de carácter privado son la mayor fuente de tráfico de Internet, consumiendo el 29,7% del tráfico en toda la red en el año 2011, la aplicación de Hulu posee 38 millones de espectadores casuales que acceden a su contenido al menos una vez al año y 3 millones de suscriptores de pago. Los proveedores Streaming ofrecen Audio y Video en múltiples niveles de calidad y estándares, capaces de adaptarse al ancho de banda disponible del usuario, estas plataformas de Audio y Video en mención son de gran escala y de rápido crecimiento con una alta disponibilidad y escalabilidad. Debido a su popularidad y tamaño, las decisiones de diseño y gestión de tráfico de estos servicios también tienen un profundo impacto en la infraestructura de Internet.[9]

Las aplicaciones multimedia de Streaming cambiaron su política de mercado por el incremento mayor de proveedores de contenidos bajo demanda que ofrecen este servicio a los usuarios por el uso de estos programas en mención. La necesidad de una entrega efectiva de material de Audio y Video reanimó el interés por el almacenamiento en caché: dado que la carga de trabajo similar a la Web de la década de los 90 ya no es apta para describir la nueva Web de vídeos actualmente, en este estudio se verifica la capacidad del conjunto de datos de los servidores implementados en las organizaciones dedicadas a publicar archivos multimedia en la red con disposición para el almacenamiento en caché donde este método reduce el tráfico y establece una mayor experiencia al usuario a través de un mayor rendimiento y menores retardos. El análisis enfocado a las plataformas de contenido audiovisual muestra que, a medida que el conjunto de datos evoluciona de forma continua, una descripción de estado estacionario no es estadísticamente significativa y a pesar de que la proporción de caché disminuye debido al crecimiento de películas activas en el catálogo, surge el creciente sesgo en la distribución de popularidad a lo largo del tiempo donde los usuarios acceden a estos servicios por medio del internet sin la necesidad de visitar una tienda que proporcione dicho producto como anteriormente lo hacían las compañías de venta de contenido audiovisual por ejemplo la distribuidora mundial en los Estados Unidos llamada BluckBuster donde esta acaparo mucha demanda de sus productos de alquiler de películas en la década de los 80, donde comenzó el uso de los reproductores de cinta de video.[10]

A medida que fue creciendo la tecnología multimedia de Audio y Video bajo demanda (YouTube, DailyMotion, Metacafé, etc.) o películas y programas de televisión (Netflix, Viki, Hulu, etc.) se hicieron conocer alrededor de todo el mundo. La red de internet se utiliza cada vez más como plataforma para la distribución y venta de contenido de una o más fuentes multimedia a una cantidad muy grande de usuarios. El contenido popular tiene que ser entregado varias veces y las solicitudes de los usuarios suelen ser asíncronas y no coordinadas. Además, el Audio y Video bajo demanda no es sólo un privilegio del Internet fijo, sino también de los entornos móviles, lo que ha sido posible

gracias al creciente desarrollo de las redes celulares 3G[3] y 4G[4] de alta velocidad, por una parte, y por la creciente integración de teléfonos inteligentes móviles y dispositivos de tabletas por otro lado. Por esta razón, el paradigma de multidifusión IP no es útil ya que el principio TCP/IP de extremo a extremo conduce a la pérdida de ancho de banda.[10]

En pleno siglo XXI proporcionar una autenticación segura en las plataformas Streaming de pago en la red de Internet es un verdadero desafío en esta nueva era de la ingeniería social enfocada en los ataques de suplantación, hombre en el medio y robo de sesiones mediante cookies donde cuyo objetivo de los crackers es tener el acceso ilícito a estas tecnologías ocasionando un declive económico en las organizaciones dedicadas a la prestación de estos servicios. Actualmente, la autenticación de usuarios en estos servicios de contenido audiovisual se ha vuelto de gran importancia ya que da el acceso a todo tipo de entretenimiento de películas, series, novelas y anime en estas páginas de Streaming como Netflix, Claro Video, HBO y muchos más, donde estos sistemas se ejecutan en el Internet. Investigadores detallan que la protección de las sesiones de los usuarios suscriptores a estos sistemas en mención es fundamentalmente relevante por la cual se logra identificar a los usuarios exactos que realmente han utilizado el sistema, independientemente de la dirección del dispositivo o la ubicación, desde donde el usuario tuvo el acceso a Internet.[11]

Hoy en día las plataformas Streaming como Netflix cuenta con más de 750 millones de usuarios activos en todo el mundo, un aspecto particular de Netflix ampliamente discutido en las noticias y fuertemente investigado en círculos académicos es el contenido de audio y video bajo demanda de carácter privado. Ingenieros del departamento de ciencias computacionales de la Universidad College del Londres descubrieron la vulnerabilidad de día cero al explotar este fallo se obtiene el acceso al material de Netflix. El ataque de día cero consiste en que el atacante suplanta la identidad de la víctima, teniendo el acceso indefinido al contenido de información privada

---

[3] **3G:** Tercera Generación

[4] **4G:** Cuarta Generación

aplicando técnicas de camuflaje, robo de cookies y demás. Los ataques de día cero causan el impacto a las victimas donde el cracker demuestra la facilidad de ganar confianza de los usuarios de Netflix para distribuir el contenido que proporciona estas plataformas Streaming de manera ilegal.[12]

En el año 2012 hasta la actualidad la suplantación de identidad se ha transformado en uno de los delitos cibernéticos con un crecimiento acelerado, la mayoría de los usuarios no poseen la consciencia sobre la cantidad de autenticaciones abiertas que dejan las víctimas cuando se loguean en servicios Streaming dejando una puerta abierta a los atacantes maliciosos para que tengan el acceso al contenido. El valor potencial de la información audiovisual es considerable para los delincuentes informáticos donde ellos poseen la capacidad de establecer un lucro económico degradando el sistema financiero de las organizaciones dedicadas a la suscripción de servicios Streaming bajo demanda. Este estudio trata sobre el robo de identidad y todas las cuestiones planteadas por este tipo de fraude informático, más precisamente, ilustra la variedad de información que los crackers pueden querer tamizar, los ataques que pueden realizar y los lugares donde pueden encontrar datos de carácter confidencial e íntegro.[13]

2.2 FUNDAMENTACION TEORICA

2.2.1 Streaming de información multimedia

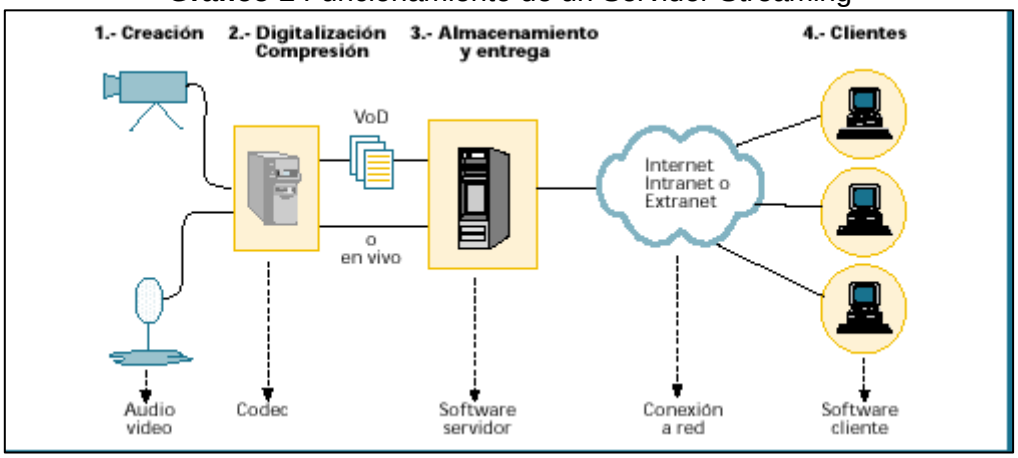
El proceso de Streaming consiste en la entrega de uno o varios medios multiplexados hacia un cliente en tiempo real, donde el usuario al que se le entrega el contenido audiovisual tiene que tener conexión a una red con un determinado ancho de banda. En el proceso de Streaming no contiene la capacidad de descarga de material de audio video bajo demanda en el ordenador del cliente, sino que el medio se reproduce conforme a la manera que se está recibiendo, y a su vez este se recibe a la velocidad adecuada para su reproducción. Esto contrasta con las descargas progresivas, en las que el fichero sí queda descargado en disco y además se recibe a la mayor velocidad posible, con el fin de terminar el proceso de descarga lo antes posible.[5]

El proceso de Streaming es un estándar de audio y vídeo sincronizado, donde las peticiones de servicio por parte de los clientes se pueden manejar utilizando el protocolo

RTSP (Real- Time Streaming Protocol). Este protocolo se encarga de controlar el stream de contenido multimedia en dos direcciones, de forma que los clientes pueden pedir al servidor hacer cosas como rebobinar la película, saltar al siguiente capítulo, etc. Esto se puede conseguir con Streaming ya que el medio no se descarga linealmente, sino que se reproduce conforme a lo que se obtiene, y se permiten saltos en la reproducción, consiguiendo un acceso aleatorio al contenido, incluso en saltos hacia delante.[5]

Los datos del medio (el stream que contiene típicamente audio y vídeo sincronizados) son transportados usando el protocolo estándar RTP (Real-Time Transport Protocol), que es un protocolo de transporte que permite la transmisión de información multimedia en tiempo real sobre cualquier tipo de red ya sea red de área local con acceso a internet o red inalámbrica (el protocolo RTP es una etiqueta que trabaja bajo el sistema UDP).[5]

Gráfico 1 Funcionamiento de un Servidor Streaming



Fuente: http://www.rediris.es/difusion/publicaciones/boletin/58-59/ponencia10.html
Autor: Josu Aramberri – Javier Lasa.

2.2.2 Tipos de Streaming

El proceso de Streaming se puede dividir en dos categorías, en función de cómo se obtiene la información a difundir: Streaming en directo o bajo demanda.

- **Streaming en Directo**: es aquel que transmite eventos que están sucediendo justo en el momento de la difusión. Por ejemplo, la transmisión de conciertos o de clases son eventos que típicamente se difunden usando este tipo de Streaming. La transmisión de radio y televisión por Internet también tiene estas

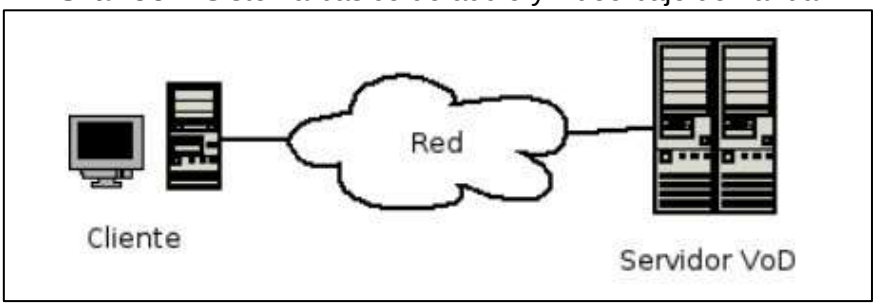
características, aunque en ocasiones parte de la información que se difunde no parte de un evento en directo (por ejemplo, un programa que ha sido grabado previamente, pero que se va a difundir en un momento determinado). En este tipo de transmisión se emplea el término difusión (broadcast) para efectuar las transmisiones en vivo hacia todos los clientes en ese momento. Así, independientemente de cuando se conecta un cliente al servidor, todos ven exactamente el mismo punto del stream en un instante determinado (excepto las lógicas variaciones de los retardos en la red que hacen que unos clientes reciban antes los datos que otros). Para poder ejecutar este tipo de transmisión, se dispone de un equipo que realice el proceso de captura y compresión en tiempo real (que a veces se conoce como difusor o broadcaster). Este equipo puede estar instalado en la misma máquina que el servidor de Streaming si el número potencial de clientes no es grande, pero para resultados profesionales, en un entorno con muchos clientes, es conveniente separar ambos programas en dos máquinas distintas. Además, para dar un servicio realmente eficiente de este tipo de Streaming es conveniente que la difusión se realice con técnicas de multicast.[5]

- **Streaming multimedia bajo demanda:** la transmisión del medio empieza desde el inicio del evento a ser reproducido para cada uno de los clientes. El medio a transmitir está preparado desde el comienzo del proceso en un fichero comprimido. En este caso no representa una ventaja adicional el disponer de posibilidad del realizar multicast en la red, ya que cada cliente recibe una parte distinta del stream y por lo tanto un paquete de datos diferente.[5]

2.2.3 Arquitectura de los servidores Streaming bajo demanda.

Arquitectura Elemental de un sistema Streaming Bajo Demanda.

Gráfico 2 Sistema básico de audio y video bajo demanda



Fuente: Trabajo de Investigación,
Autor: Oscar Daniel Torres.[14]

Las unidades son:

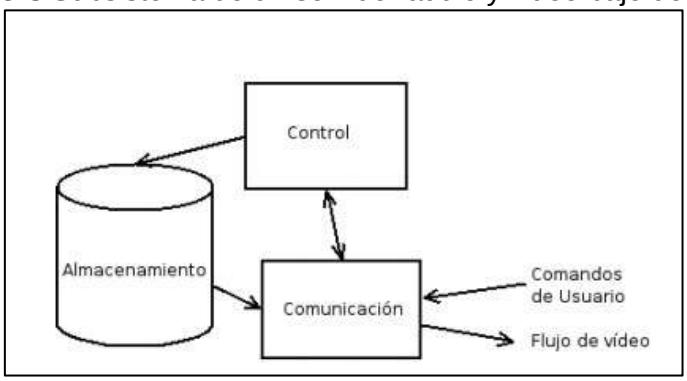
- El Servidor.
- La Red.
- Cliente.

El Servidor: Se compone de hardware y Software preciso para efectuar el deber principal de servir video y suministrar un flujo continuo de información con requerimientos de tiempo real, el servidor se compone de tres subsistemas: subsistema de control, almacenamiento y de comunicación.[14]

- **Subsistema de Control:** Toma y procesa las peticiones que necesita el cliente, cuando un cliente nuevo realiza una petición, el sistema establece si el servidor dispone de los recursos necesarios para poder entregar el video que se pide.[14]
- **Subsistema de Almacenamiento:** Es el encargado de todo el almacenamiento del contenido audiovisual, y disponer de ellos de una manera rápida para inmediatamente enviarlos al cliente.[14]

- **Subsistema de Comunicación:** Es el encargado de recibir los comandos para luego enviar el contenido a los clientes, más tarde ejecuta un conjunto de protocolos de comunicación trazados para esta labor como lo es el protocolo RTP.[14]

Gráfico 3 Subsistema de un servidor audio y video bajo demanda.



Fuente: Trabajo de Investigación,
Autor: Oscar Daniel Torres.[14]

La Red: Se encarga de conectar entre si los elementos que son parte del sistema Video bajo demanda, se debe garantizar una mínima latencia y efectuar los parámetros de velocidad y ancho de banda óptimos de transmisión .[14]

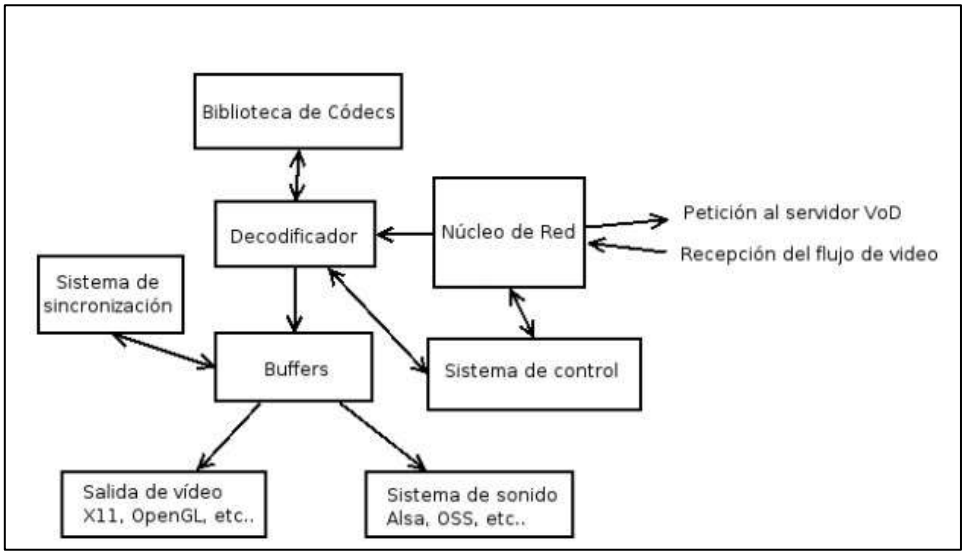
El Cliente: Más conocido como el reproductor es el que tiene la labor de de destinar los comandos coligados al control de reproducción, este a su vez reproduce el contenido que va recibiendo del servidor, el cliente consta de tres subsistemas: núcleo de red, sistema de control y decodificador, Buffers y sistemas de sincronización.[14]

- **Núcleo de Red**: ejecuta el mismo conjunto de protocolos utilizados por el servidor, para implantar comunicación con este, el núcleo se encarga de dar los comandos ingresados por del usuario y recoger los flujos de video del servidor.[14]
- **Sistema de control:** traduce las instrucciones ingresadas por el cliente :

Reproducir, pausar, adelantar, etc., todo esto es recogido para ser enviadas al servidor.[14]

- **Decodificador**: Es el encargado de decodificar la información recibida para poder ser ejecutada por el equipo de video o sonido con la ayuda de la librería de códecs coligados que se encuentran en la biblioteca de códecs disponibles.[14]
- **Buffers**: es necesario retener unos segundos del video y el audio antes de ser reproducidos ya que por excelente que este la red, jamás se recibirá los datos a igual velocidad, es decir que la variación de la latencia como hecho inevitable provocaría cortes en la reproducción.[14]
- **Sistema de sincronización:** tanto el video y el audio se codifican por separado, cada quien en un bloque independiente del otro, para todo el proceso se necesita un sistema que certifique la sincronización de los dos flujos.[14]

Gráfico 4 Subsistemas de un Cliente.



Fuente: Trabajo de Investigación,
Autor: Oscar Daniel Torres.[14]

2.2.4 Otras Arquitecturas Presentes en los Sistemas de Streaming de audio y video bajo demanda.

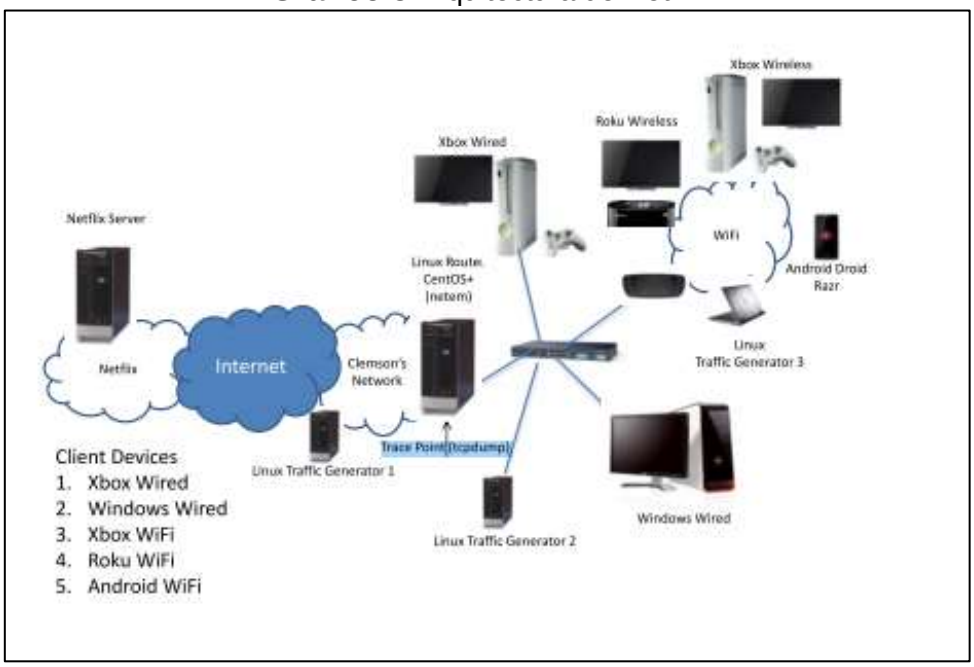
- **Arquitectura Centralizada:** Radica en un servidor centralizados en el cual todos los usuarios del sistema están conectados mediante una red de comunicación.[14]
- **Servidores Independientes:** Es una red partida y segmentada en diferentes redes las cuales están acopladas a servidores independientes o servidores proxy.[14]
- **Distribuidas:** Es cuando un cliente propio actúa de servidor para otros clientes .pudiendo así encadenar varios. [14]

Arquitectura del servidor de Netflix.

La arquitectura de los servidores Streaming está compuesta por una red inalámbrica privada con el estándar de red 802.11n donde esta tiene conectado cuatro dispositivos cliente diferente tales como: un Xbox, un Roku, una computadora portátil con sistema operativo Windows y un Smartphone Android para la visualización del material audiovisual como se ve en el grafico 1. Los dispositivos siguientes se conectan a una red de área local a través de una interface Gigabit Ethernet privada para la transmisión de contenido audiovisual hacia el cliente. En el lado del usuario final todos audios y videos bajo demanda se aprecian en un monitor de alta definición (con capacidad para el formato 1080p) conectado al puerto HDMI de Xbox y Roku, con esto se supervisa el tráfico de Netflix mediante la obtención de trazas de red utilizando el analizador de tráfico tcpdump en un enrutador de Linux. El enrutador conecta el banco de pruebas de medición con la red que proporciona una conexión de 10 Gbps al Internet (público). En esta infraestructura se utiliza la característica netem Linux para aplicar un nivel deseado de pérdida de paquetes no correlacionados en paquetes entrantes (es decir, paquetes desde el servidor Netflix al cliente) asociados con la sesión Netflix bajo observación, los cuadros de Linux adicionales instalados en el banco de pruebas sirven como generadores de tráfico de fondo para proporcionar datos de métricas de rendimiento

adicionales. Los generadores de tráfico 1 y 2 de Linux son PCs de escritorio con Linux. Traffic Generator 3 era un ordenador portátil que ejecuta Linux.[8]

Gráfico 5 Arquitectura de Netflix



Fuente: 2013 IEEE 10th Consumer Communications and Networking Conference, CCNC 2013

Autor: Martin, Jim Fu, Yunhui Wourms, Nicholas Shaw, Terry.[8]

2.2.5 Difusión de Streaming a varios clientes usando multicast

Los servicios Streaming orientados a redes multicast, son aquellos que comparten contenido entre diferentes clientes, de forma que el servidor envía la información una vez al lugar de destino de todos los clientes conectado al servicio, esta técnica es ideal para la difusión de medios en vivo (por ejemplo, radio en Internet) ya que todos los clientes están dispuestos a recibir el mismo flujo de datos (por ejemplo, el audio que corresponde al programa de radio que una emisora está difundiendo en un momento determinado).[5]

La técnica de difusión multicast tiene la funcionalidad de disminuir el tráfico en la red, y evita posible congestión en los dispositivos que proporcional el servicio en el internet. Sin embargo, para llevarla a cabo este método de aplicación es necesario tener acceso a un enlace troncal con soporte multicast (por ejemplo, Mbone en Internet), o que el servidor y los clientes estén conectados a una red o redes IP bajo un mismo dominio de administración en las que el multicast esté habilitado y existan routers dispuestos a encaminar información multicast (router multicast).[5]

En otro caso la transmisión Unicast es aquella que inicia su propio stream en cada cliente, independientemente de que todos los usuarios estén conectados al mismo contenido transmitido ya sea difusión bajo demanda o en vivo, de forma que se inician muchas conexiones uno-a-uno (una entre el servidor y el cliente por cada uno de los clientes). Esta técnica requiere que el servidor solicite un ancho de banda que excede a los 20Mbps aproximadamente aumentando el tráfico en la red. Sin embargo, este método es el único cuya disponibilidad está garantizada en Internet actualmente, ya que no necesita de acceso a Mbone (cuya disponibilidad no está garantizada por todos los ISP) ni capacidad multicast entre los clientes y el servidor.[5]

2.2.6 Protocolos para los servicios Streaming

DASH Protocol

DASH es un protocolo que se enfoca en los sistemas de distribución de vídeo. El contenido multimedia se codifica en una o más representaciones en diferentes velocidades de bits, permitiendo al cliente solicitar cualquier parte de una representación en unidades de bloques de datos de tamaño variable. El contenido de la información se encuentra disponible en los dispositivos del cliente tales como Smartphone, computadoras personales, ordenadores y tabletas mediante un estándar de solicitud HTTP. El servidor DASH tiene las similitudes de un servidor web HTTP estándar donde las representaciones utilizables se mantienen en un archivo de resumen denominado MPD (Media Presentation Description). MPD describe varios tipos de medios que son los siguientes:[8]

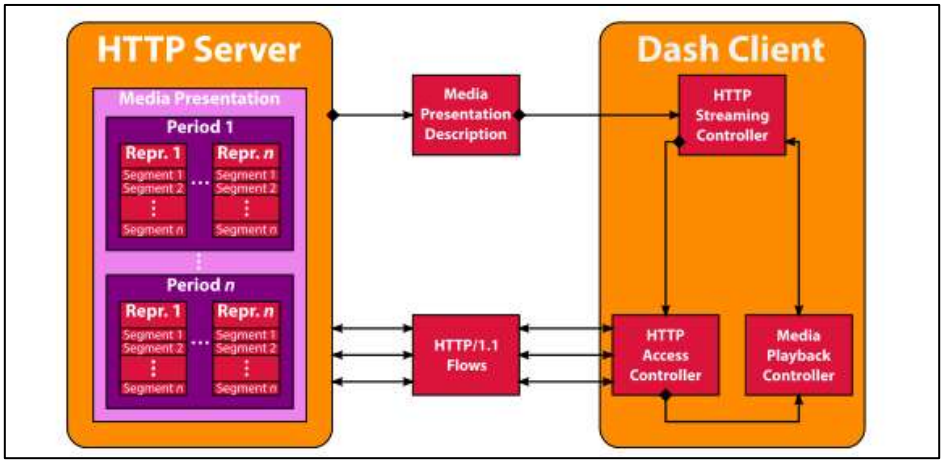
- Resoluciones del contenido audiovisual
- flujo alternativo requerido
- URLs de acceso
- Anchos de banda mínimos y máximos y
- Información de gestión de derechos digitales (DRM) requerida.

Los clientes que se asocian al servicio DASH utilizan las tres funcionalidades principales del protocolo en mención que son las siguientes:

- El acceso HTTP.
- El motor multimedia que decodifica y procesa el flujo de video
- El motor de control.

Este último componente supervisa el flujo de vídeo que llega y determina cuándo se debe solicitar un flujo de calidad inferior o superior. El cliente mantendrá un búfer de reproducción que sirve para suavizar las tasas de llegada de contenido variable para soportar la reproducción de vídeo. El cliente solicita un nuevo segmento (marcado con la velocidad de bits deseada) una vez que el búfer de reproducción se encuentre debajo de cierto umbral el usuario acude al almacenamiento del búfer para el acceso al contenido audiovisual.[8]

Gráfico 6 Servidor DASH



Fuente: 2013 IEEE 10th Consumer Communications and Networking Conference, CCNC 2013

Autor: Martin, Jim Fu, Yunhui Wourms, Nicholas Shaw, Terry.[8]

Protocolo RTP

El protocolo de transporte en tiempo real (RTP) es aquel que procesa corrientes de señales multimedia en Internet que son utilizadas para realizar transmisiones de señales en tiempo real en unicast o entorno de red de multidifusión. RTP normalmente utiliza UDP para la transferencia de contenido audiovisual, mientras que TCP, ATM u otros protocolos están disponibles en momentos determinados para efectuar la misma transmisión. RTP es un protocolo que está diseñado para suministrar información timestamp y la señal de sincronización de flujo en tiempo real para la visualización de material de audio y video. El protocolo RTP proporciona el campo de número de serie para hacer que el destinatario detecte el número de secuencia de paquete recibido para averiguar si hay pérdida de paquetes y luego restaurar el orden de secuencia de paquete de envío.[15]

Cuando el usuario inicia una sesión RTP por medio de una aplicación Streaming, el protocolo utiliza dos puertos: uno para RTP y otro para RTCP. Durante la sesión RTP, cada participante transmite periódicamente paquetes RTCP. Los paquetes RTCP contienen la información tal como los números de paquetes de datos enviados y paquetes perdidos y otras estadísticas, de modo que el servidor puede usar esta

información para cambiar dinámicamente la velocidad de transmisión e incluso cambiar el tipo de carga útil. Con el uso de RTP y RTCP[5], se consigue una retroalimentación efectiva y una sobrecarga mínima para optimizar la eficiencia de transmisión, lo cual es particularmente adecuado para la transmisión de datos de señal en tiempo real en red.[15]

Una vez que los servidores Streaming recepten los paquetes IP, el extremo receptor analiza la cabecera RTP para determinar la validez de la información del usuario verificando el tipo de carga. Estos receptores Streaming, actualizan la información RTP, es decir, el número de bytes recibidos, tramas de video, paquetes y número de serie, en el búfer, la sincronización de origen proporciona un acuerdo con el timestamp RTP, facilitando el número de serie del paquete y con esto establecer la orden del paquete RTP[6] y reconstruir el marco de audio y vídeo. Los datos se decodifican basándose en la identificación del tipo de carga y luego se ponen en el búfer, que se abastece al decodificador para la salida del contenido, al mismo tiempo el receptor, devuelve periódicamente paquetes RTCP que contienen información de control de realimentación QoS[7] al emisor para detectar la consistencia de datos entre el remitente y el receptor.[15]

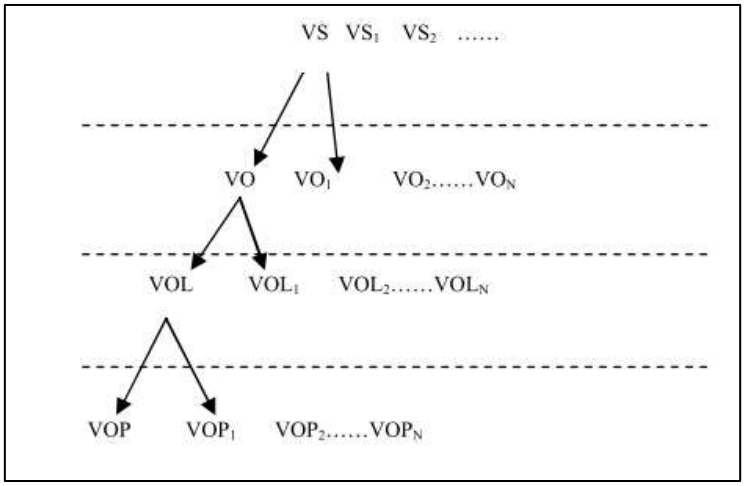
---

[5] **RTCP:** Protocolo de información de control y flujo de datos para aplicaciones multimedia

[6] **RTP:** Protocolo en tiempo real

[7] **QoS:** Calidad de servicio

Gráfico 7 Sesiones RTP



Fuente: http://0-ieeexplore.ieee.org.almirez.ual.es/document/7490965/
Autor: Zhen-ping, Fan Kang, Bai Standard, A Mpeg- Compression

2.2.7 Streaming Media Server

DARWIN Streaming Media Server es un software de sistema de servicio de medios de Streaming de código abierto proporcionado por Apple donde los usuarios utilizan esta aplicación para modificar y ampliar el rendimiento del servidor en una forma simplificada del Servidor de transmisión de QuickTime, su principal función es el QuickTime[8] Streaming Server.[15]

El servidor Streaming en mención recibe la petición RTSP[9] enviada por el usuario y luego de esto genera un objeto de petición RTSP y este es llamado módulos de función específico, en el cual los clientes solicitan el contenido del audio y video al servidor a través del protocolo RTSP para el servicio de unidifusión, este servidor detalla el contenido de la solicitud con forma de sesión de transmisión por medio de la información de respuesta del protocolo incluyendo el número de flujos de datos, el tipo de medio y el códec. Una sesión de transmisión está compuesta por uno o más flujos de datos, como el Streaming de vídeo y el Streaming de audio. El flujo de datos real se transmite

[8] **QUICTIME:** Aplicación de reproducción de contenido multimedia

[9] **RTSP:** Real Time Streaming Protocol

al cliente a través del protocolo RTP, donde el sistema proporciona una interfaz de desarrollo de aplicaciones basadas en Java para la visualización del video, este servicio utiliza los métodos de desarrollo que permiten crear un reproductor de cliente sin utilizar el QuickTime Player suministrado por el sistema.[15]

La carga y consulta sobre la información de Streaming de los medios de comunicación utilizan la estructura de base de datos del sistema cliente / servidor de SQL, los datos de los medios de comunicación son almacenados en el servidor para cuando el cliente los requiera el servicio pueda facilitarlos.[15]

2.2.8 Ancho de banda Requerido para las Plataformas de Streaming

El extendido despliegue de asignación de ancho de banda de transmisión está haciendo que el video por Internet sea más rápido sin la necesidad de que existan retardos durante la reproducción del contenido audiovisual por Internet, el Streaming de audio y video ha sido ampliamente desplegado y estudiado durante décadas, el flujo basado en DASH es muy diferente ya que implica la adaptación tanto por el servidor que se ejecuta bajo el protocolo TCP, donde la dinámica y las implicaciones de los múltiples niveles de control de congestión de extremo a extremo son enfocados en disminuir los retardos del material de audio y video bajo demanda. La contribución de este estudio detalla lo siguiente: se caracteriza el consumo de ancho de banda de una aplicación DASH[10] ampliamente implementada en el sistema Streaming; se indica información sobre cómo diferentes implementaciones y diferentes redes de acceso pueden afectar el consumo de ancho de banda. Los resultados sugieren que la adaptación de estos servidores por defecto a los mecanismos subyacentes del protocolo TCP sea durante los períodos de pesada de la congestión de red sostenida. Sin embargo, el algoritmo de aplicación está claramente entrelazado con los mecanismos TCP[11] subyacentes durante períodos de condiciones de red volátiles. En un escenario de red, observamos que un flujo TCP con backlogged alcanzó un rendimiento de 6 Mbps mientras que una sesión de una

---

[10] **DASH:** estándar para Streaming adaptativo sobre HTTP.

[11] **TCP:** Protocolo de control de transmisión.

plataforma en mención (bajo condiciones de ruta similares) consumía menos de 3 Mbps de ancho de banda.[8]

2.2.9 Códecs De Video

El contenido de vídeo está constituido por una gran parte del tráfico de datos en Internet debido a los protocolos que manejan, la transmisión de video es permitida por la difusión capilar de las tecnologías de los códecs de vídeo: actualmente, cada ordenador, tableta y teléfono inteligente está equipado con codificación de vídeo y tecnologías de decodificación para la reproducción del mismo. Los contenidos de vídeo a menudo existen en diferentes formatos donde se verifica que hay incompatibilidad hoy en día con distintas plataformas que tienen una significativa redundancia mutua. La incompatibilidad impide una explotación eficiente de la escalabilidad, que por otra parte es una característica de gran importancia cuando se trata de un uso eficiente de la red. Una alternativa sugestiva al vídeo escalable clásico es utilizar la codificación video distribuida (DVC) para las capas de la mejora. En los escenarios, los clientes tienen diferentes decodificadores para la capa base, adaptados a las características de su dispositivo. Sin embargo, pueden compartir la misma capa de mejora, ya que DVC permite codificar marcos independientemente de la referencia que se empleará en el decodificador. Este enfoque ha sido considerado en el pasado con el fin de mejorar la escalabilidad temporal y espacial. El códec DVC posee la capacidad, de mejora en la reproducción del contenido audiovisual utilizando las técnicas del mismo actualizadas.[16]

El internet es una recopilación híbrida de redes, donde los usuarios pueden tener acceso a los diferentes recursos en términos de memoria y arquitectura computacional. Actualmente, la mayor parte del tráfico de Internet se relaciona con las aplicaciones de vídeo como la videoconferencia, el Streaming de audio y vídeo, la descarga y el uso compartido de archivos multimedia. Una manera trivial de tener en cuenta las diferentes peticiones de los usuarios es codificar las versiones compatibles de un video en diferentes calidades y almacenar todas las versiones en un servidor de contenido audiovisual. Visiblemente, entre las distintas versiones de video existe una gran redundancia sobre la codificación de vídeo escalable (SVC) desarrollado como una

extensión de H.264 / AVC para codificar las diferentes versiones del video, eliminando tanto como sea posible las redundancias.[16]

SVC es aquel que permite codificar el vídeo para que este sea apreciado mediante el estándar de calidad de imagen configurado, una vez aplicado los procedimientos SVC[12] proporciona a los usuarios una opción de elegir los parámetros del vídeo seleccionando un subconjunto de secuencia de bits utilizada por SVC para codificar el vídeo es decir que la corriente de bits se divide en una capa de base que consiste en la capa de calidad más baja con varias mejoras.[16]

En los entornos de audio y video Streaming existen 3 tipos principales de escalabilidad que son las siguientes:

- **Temporal:** La escalabilidad temporal permite al usuario decodificar el vídeo a la velocidad de fotogramas más baja y luego aumentar paulatinamente la velocidad de fotogramas. Esto es posible utilizando marcos jerárquicos como en H.264 - AVC.[16]
- **Espacial:** La escalabilidad espacial consiste en descifrar el vídeo en diferentes resoluciones espaciales que sean apreciados por el usuario.[16]
- **Calidad:** La escalabilidad de calidad es aquella que para cada capa de mejora que se envía, a la PSNR de la imagen decodificada w.r.t. sobre la capa base se incrementa. Sin embargo, además de estas formas "clásicas" de escalabilidad, aparecen nuevas capas, asociadas a los formatos emergentes, como el video de más profundidad (MVD): podemos tener escalabilidad de vista cuando un subconjunto de las ventanas totales es decodable sin tener que decodificar todas las ventanas, y la escalabilidad de componentes cuando el acceso a un componente no se basa en la decodificación del otro.[16]

[12] **SVC:** Sistemas de video de comunicación

Códec DVC

La codificación de video distribuida DVC es aquella que se basa en un código fuente distribuido para la codificación de las fuentes dependientes de manera independientemente conjuntamente mediante algunos parámetros sobre las características estadísticas de las fuentes, la pérdida en términos de rendimiento de distorsión de la tasa es despreciable. En cuanto a la escalabilidad de esta codificación, DVC posee la capacidad de codificar las diferentes capas independientemente donde la decodificación es emancipada de la información disponible en el lado del decodificador. De esta manera, se puede tener diferentes capas de base compartiendo la misma capa de mejora codificada en DVC. Esto puede permitir ahorros de ancho de banda notables, sobre todo cuando se consideran muchos códecs diferentes. Debido a las diferentes técnicas de codificación de vídeo que se presentan actualmente en una red, (por ejemplo H.264 / AVC con sus diferentes perfiles, HEVC, MPEG-2, MPEG-4), sería necesario codificar la capa de mejora del video en Todos estos formatos, si la capa base está en la misma conformación. Por el contrario, si DVC se utiliza, sólo en una versión de la capa de mejora es suficiente para todos los usuarios independientemente de la técnica utilizada para la capa base.[16]

Este códec, el flujo de vídeo se divide en marcos clave (KF) y marcos Wyner-Ziv (WZF), tomando en consideración la terminología del contexto predictivo de codificación de vídeo, un KF y todos los siguientes WZF antes del siguiente KF forman un grupo de imágenes (GOP), por lo tanto, la distancia entre dos KFs sucesivos se denomina tamaño GOP. Los KF están codificados por INTRA (es decir, sin estimación de movimiento y compensación). Los marcos Wyner-Ziv se introducen en un codificador de canal sistemático donde la parte sistemática se descarta y los bits de paridad se envían al decodificador, en el lado del decodificador, se aplica una estimación del Frame Wyner-Ziv para obtener por interpolación las tramas ya descodificadas. Esta estimación se denomina información lateral (SI) y puede considerarse como una versión ruidosa de la verdadera WZF. El decodificador de canal debe corregir estos errores de estimación utilizando los bits de paridad.[16]

La codificación de los WZFs es completamente independiente debido a la arquitectura de Stanford donde en esta se ejecutan las herramientas de codificación de los KF y los WZF, esta codificación se ha convertido en la técnica de referencia para el vídeo monovisual y multiview distribuida. En la codificación DISCOVER el SI se genera mediante un algoritmo de interpolación de movimiento lineal de los fotogramas más cercanos disponibles en el lado del decodificador, el algoritmo de interpolación de movimiento de alto orden (HOMI) posee una base de 4 imágenes para la mejora del rendimiento de RD de las técnicas clásicas de interposición.[16]

DVC Escalable

La escalabilidad en DVC, proporciona las diferentes capas de video codificadas y decodificadas independientemente es decir que la capa base puede codificarse con cualquier técnica sin afectar la decodificación de los WZF, en particular, la escalabilidad temporal es intrínseca en DVC, aplica el procedimiento de codificación y decodificación para tamaños GOP mayores que dos similar a la estructura de los marcos B jerárquicos de H.264 / AVC[13]. Consideremos un tamaño GOP igual a 4. Entonces, sea Ik-2 e Ik + 2 dos KFs consecutivos. Estas tramas se utilizan para la estimación del WZF en el instante k. Una vez que este cuadro ha sido decodificado, el cuadro Ik está disponible en el lado del decodificador puede utilizarse junto con los KF para obtener la estimación de los WZF en los instantes k - 1 y k + 1. Tagliasacchi ingeniero en computación propuso un DVC escalable temporal para el códec PRISM enfocado al esquema de la capa base obtenida mediante el códec H.263 + / INTRA. La capa de mejora fue adquirida mediante el uso de algoritmos de interpolación linearmotion para la realización de una comparación de DVC escalable temporal w.r.t H.264 / AVC. Además, para la codificación DVC maneja un módulo de generación de información lateral basada en

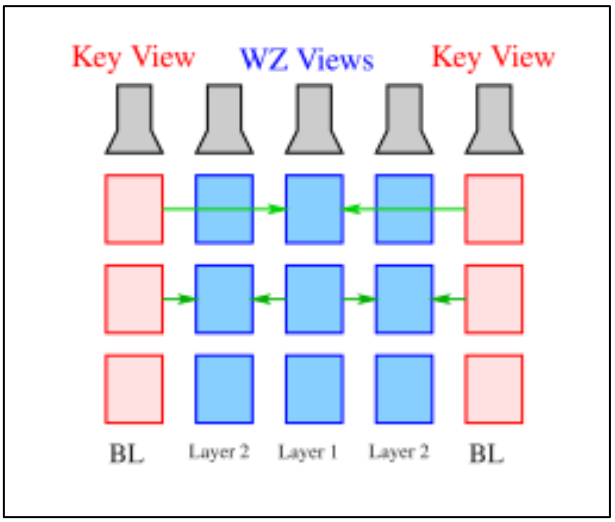
[13] **H.264/AVC:** Códec de video que proporciona una buena calidad de imagen con tasas binarias notablemente inferiores a los estándares previos (MPEG-2, H.263 o MPEG-4

compensación de movimiento de bloques superpuesto y un módulo de modelo de ruido de canal virtual adaptativo.[16]

2.2.10 Análisis De Performance Del Sistema Streaming

Las capas de mejora DVC son codificadas con un códec Wyner-Ziv, para que la transmisión del flujo de bits sea suficiente para todos los usuarios consumidores de los servicios Streaming. La codificación de vídeo escalable es temporal a lo largo del eje de vista en vídeo multiview. Una cámara fuera de V es una cámara Key donde las otras son cámaras Wyner-Ziv. La capa base consiste en enviar sólo las vistas Clave y las demás vistas están codificadas jerárquicamente, como en el dominio estacional, como se muestra en el grafico 5, cada cuatro cámaras es una cámara Key donde la numeración 0 y 4 equivalen a dos de estas cámaras. Entonces, en la primera capa de realce, se envía el número de vista 2 y para la segunda capa se envían las cámaras 1 y 3.[16]

Gráfico 8 Flujo de Cámaras



Fuente: Trabajo de investigación
Autores: Mines-t, Institut.

CUADRO DE RENDIMIENTO RD POR BJONTEGAARD METRIC W.R.T. H.264 + HEVC + H.264 (BAJA COMPLEJIDAD)

Gráfico 9 Tabla DVC

method	Δ_R [%]	Δ_{PSNR} [dB]
BQSquare - layer 1		
DVC (KF coded with H.264/AVC)	-4.70	0.86
DVC (KF coded with HEVC)	-23.58	0.40
DVC (KF coded with H.264/AVC l.c.)	-4.73	0.20
BQSquare - layer 2		
DVC (KF coded with H.264/AVC)	19.17	3.54
DVC (KF coded with HEVC)	4.24	0.83
DVC (KF coded with H.264/AVC l.c.)	20.20	0.84
Party Scene - layer 1		
DVC (KF coded with H.264/AVC)	-12.79	0.80
DVC (KF coded with HEVC)	-16.36	1.07
DVC (KF coded with H.264/AVC l.c.)	-11.56	0.78
Party Scene - layer 2		
DVC (KF coded with H.264/AVC)	-13.71	1.06
DVC (KF coded with HEVC)	-18.22	1.08
DVC (KF coded with H.264/AVC l.c.)	-12.89	1.02

Fuente: Trabajo de investigación
Autores: Mines-t, Institut

2.2.11 Códecs de audio

La cantidad de servicios multimedia son proporcionados a través de la red de internet tales como: la radio, la televisión, contenido audiovisual educativo, Streaming multimedia, juegos, etc. Según Mueller ingeniero alemán detalla que hay una gran cantidad de plataformas multimedia y protocolos utilizados en diferentes desde el entretenimiento hasta la formación ambiente de negocios. Actualmente las redes de datos ya cumplen con los requisitos de tolerancia a fallos, escalabilidad, calidad de servicio y seguridad, para la transmisión de medios de transmisión de audio y video y el control multimedia.[17]

Para realizar las transmisiones de audio por internet o redes de área amplia, se reduce la cantidad de información entregada que ayudan a mantener el buen nivel de calidad de audio (percibido por el usuario final). La transmisión de audio en redes de área local inalámbricas (WLAN), dispone de la cantidad de ancho de banda proporcionada por varios puntos de acceso, para que los usuarios puedan emplear todo el ancho de banda disponible. Igualmente los clientes logran disponer del ancho de banda en otro tipo de redes inalámbricas, como Long Term Evolution (LTE).[17]

Los códecs utilizados en los servicios Streaming son los siguientes:

- **WMA pro V10. Windows Media Audio 10 Professional (WMA Pro 10):** Es el códec de audio más flexible de Windows Media. Proporciona perfiles que incluyen audios de 24 bits / 96 kHz de resolución total en estéreo, sonido envolvente de 5.1 canales o incluso 7.1 canales, hasta capacidades móviles altamente eficientes de 24 Kbps a 96 Kbps para estéreo y de 128 Kbps a 256 Kbps para sonido de 5.1 canales.[17]

- **Lame Mp3:** LAME es un codificador MPEG Audio Layer III (MP3) de alta calidad con licencia de la GNU Lesser General Public License. Hoy en día, LAME es considerado como el mejor codificador de MP3 a velocidades de bits de media-alta y VBR (Variable Bit Rate), gracias al laborioso trabajo de sus desarrolladores y al modelo de licencia de código abierto que permite aprovechar los recursos

de ingeniería de todo el mundo. Ambas mejoras de calidad y velocidad siguen ocurriendo, lo que probablemente convierte a LAME en el único codificador de MP3 que aún se está desarrollando activamente.[17]

- **OGG Vorbis:** Ogg Vorbis es un formato de compresión de audio Desarrollado por la fundación Xiph.Org. Es Diferente de otros formatos de compresión, ya que es completamente gratuito, abierto y no patentado. Vorbis está destinado a las tasas de muestreo de telefonía de 8 kHz a 192 kHz maestros digitales. Permite una amplia gama de representaciones de canales (monaural, polifónico, estéreo, cuadrafónico, 5.1, ambisonic o hasta 255 canales discretos).[17]

- **Nero AAC:** Advanced Audio Coding (AAC) es un esquema de codificación estandarizado de compresión con pérdida. AAC admite la inclusión de 48 canales de audio de ancho de banda completo (hasta 96 kHz) en una sola fuente más 16 canales de efectos de baja frecuencia, hasta 16, canales de diálogo hasta 16 flujos de datos.[17]

Gráfico 10 Códecs de Audio

Bitrate (kbps)	Audio Codec			
	Nero AAC	*Lame MP3*	*WMA pro 10*	*OGG Vobis*
32	97.61%	97.67%	97.67%	97.70%
40	97.05%	97.15%		97.13%
48	96.49%	96.56%	96.53%	96.55%
56	95.93%	96.01%		95.98%
64	95.36%	95.45%	95.39%	95.40%
80	94.24%	94.43%	94.26%	94.27%
96	93.11%	93.33%	93.12%	93.11%
112	91.99%	92.26%		91.97%
128	90.86%	91.20%	90.85%	90.82%
160	88.59%	89.07%	88.58%	88.56%
192	86.31%	86.82%	86.31%	86.27%
224	84.06%	84.64%		83.98%
256	81.86%	82.39%	81.76%	81.70%
320	77.55%	78.73%		77.13%

Fuente: 2014 IEEE Globecom Workshops, GC Wkshps 2014
Autores: Tortosa, Ruben Jimenez, José M. Díaz, Juan R. Lloret, Jaime

2.2.12 Definición de EMBY.

EMBY: Es una aplicación Streaming de audio y video bajo demanda con la finalidad de convertir el ordenador en un centro multimedia para el acceso al contenido de audiovisual referente a películas, series de televisión, novelas y demás. Además EMBY puede ser instalado en Linux, Windows y MAC.[18]

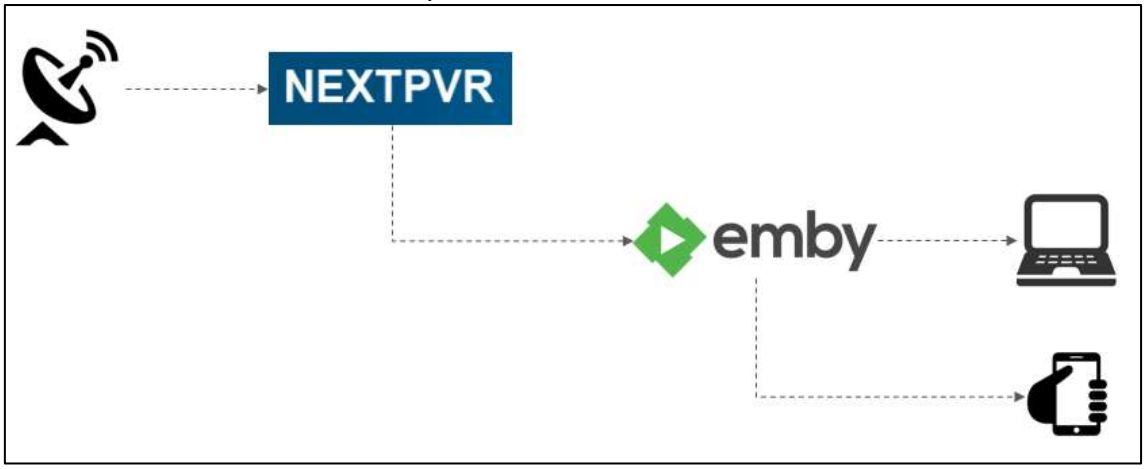
MULTISERVICIOS: EMBY es una de las aplicaciones Streaming que tiene varias bibliotecas con servicios de música, películas y galería de fotos, con la finalidad de acceder al contenido multimedia para mostrarlo por pantalla, dejando unos pasos atrás a sus competidores directos como PLEX y KODI.[18]

INTERFACE: EMBY posee una interface Web para el control de la aplicación de manera remota y una interfaz gráfica para el usuario que pueda tener el acceso al contenido

audiovisual mediante un televisor SMARTH TV, dispositivo móvil con sistema operativo Android y computadoras en general.[18]

EMBY: Es una aplicación que converge en redes inalámbricas, redes móviles, redes cableadas y demás con la finalidad de proporcionarle al usuario EMBY una conexión eficiente y efectiva.[18]

Gráfico 11 Arquitectura de EMBY-MEDIA-SERVER.



Fuente: http://www.gearnut.com.au/htpc/emby-next-pvr-kodi/
Autor: EMBY.

2.2.13 Características de Emby media server

Tabla 2 CARACTERISTICAS DE EMBY MEDIA SERVER

CARACTERISTICAS DE EMBY MEDIA SERVER	
1	Fácil acceso al servicio de distintos sistemas operativos
2	Opciones de TV en vivo
4	Administración de Emby desde dispositivos móviles
5	Ejecutable en distintas redes fijas y móviles
6	Control parental
7	Integración con servicios IPTV, radio online y bibliotecas multimedia.
8	Configuración de bibliotecas multimedia muy sencilla
9	Códecs de audio y video incorporados para la ejecución de contenido de alta resolución
10	Soporta tarjetas sintonizadora de TV
11	Posee robustez y un rápido acceso al contenido audiovisual
12	Máxima calidad de imagen en momento de reproducir contenido multimedia
13	Fácil uso para usuarios finales

14	80% de código Abierto.
15	Integración con más aplicaciones Streaming de audio y video bajo demanda

Fuente: Trabajo de investigación.
Autores: Simón Ballesteros-Francisco Sarmiento.

2.2.14 Metodología de Gestión de análisis de riesgos

MAGERIT es una metodología de análisis y gestión de riesgos enfocada en los sistemas de información y comunicación, a la vez es un método valido fundamental para realizar una investigación profunda sobre los riesgos soportados por las tecnologías Streaming de audio y video bajo demanda, con esto se plantearan alternativas de solución acopladas a la mitigación de los riesgos detectados. Cuando hablamos de MAGERIT es la metodología de análisis de las tecnologías de información de las administraciones públicas, que fue creado por el Consejo Superior de Administración Electrónica (CSAE), el uso de la metodología en mención es de carácter privado y público en general, en la cual pertenece al Ministerio de Administraciones Públicas (MAP) de España.[19]

La metodología MAGERIT en si se creó para que los medios informáticos, electrónicos y telemáticos puedan ser analizados y aplicar el respectivo tratamiento para los riesgos. La utilización de esta es encaminada a ejecutar auditorias de seguridad de la información para el hallazgo de fallas en los sistemas informáticos y como protegerlos reduciendo el nivel de ataques en las organizaciones. Conocer los riesgos al que están expuesta las tecnologías Streaming de audio y video, es fácilmente despectivo para gestionarlos, con MAGERIT se procura establece una metódica que no deje lugar a la descuido de las empresas dedicadas a la prestación de servicios de contenido audiovisual.[19]

2.2.15 Objetivos de Magerit

Los objetivos de la metodología MAGERIT se clasifican en directos e indirectos:

Directos

1. Alcanzar que los responsables de las organizaciones y empresas tomen la respectiva conciencia sobre los riesgos existentes y tomarlos en consideración para prevenir incidentes de seguridad a futuros.
2. Proponer de manera metodológica y sistemática una ayuda para el análisis que se emplean en la tecnología de la información y comunicaciones. (TIC)
3. Colaborar con el descubrimiento y la correcta planificación de medidas de salvaguardia para el control de los diferentes riesgos.

Indirectos

1. Disponer a las organizaciones dedicadas a la prestación de servicios Streaming bajo demanda a los diferentes procesos de evaluaciones, auditorías, certificaciones o acreditaciones.
2. Tomar en cuenta los proyectos de seguridad informática con su respectivo modelado de concepto donde los mismos permiten recoger descubrimientos y las respectivas conclusiones mediante las tareas del análisis y gestión de riesgos.

Entre los conceptos que debemos agregar tenemos los más relevantes tenemos:

2.2.16 Modelo de valor

En los modelos de valores se identifican los valores que representaran a los activos de carácter físico y lógico de las organizaciones y asignado las dependencias de cada una de ellas.[19]

2.2.17 Mapa de riesgos

En los mapas de riesgos se procede a identificar las diferentes amenazas tanto internas y externas para cada uno de los activos expuestos a ellas.[19]

2.2.18 Declaración de aplicabilidad

Se agrupan las medidas de salvaguardas aplicables a los sistemas de información y comunicación implementados en las organizaciones.[19]

2.2.19 Evaluación de salvaguardas.

Las salvaguardas son evaluadas por los profesionales de seguridad informática que aplican la metodología MAGERIT para fijar su eficacia con relación a los riesgos que tienen en frente.[19]

2.2.20 Estado de riesgo

En los estados de los riesgos presentes se procede a la identificación de los activos clasificándolos por el riesgo residual, los procesos considerados incluyendo las medidas de salvaguardas.[19]

2.2.21 Informe de insuficiencias.

En los informes de insuficiencias se detallan todas las debilidades y carencias en relación a los mecanismos de protección que se destinan para reducir el riesgo presente en el sistema.[19]

2.2.22 Plan de Seguridad

Los planes de seguridad son planificados mediantes proyectos que garanticen la madurez de las decisiones referente a los tratamientos de los riesgos.[19]

2.2.23 Seguridad de la Información

Seguridad es la suficiencia de las redes y de los sistemas de información para aplicar los mecanismos de protección con un determinado nivel de confiabilidad evitando los incidentes o accesos ilícitos a los servicios de una organización, los ataques o acciones e interferencias ilegales o malintencionadas son aquellas que comprometen la disponibilidad, autenticidad, integridad y confidencialidad de la información almacenada

en los servicios que se ejecutan en la red y sistemas ofrecen o hacen accesibles a los usuarios con un cierto nivel de privilegio.[19]

Disponibilidad.- Consiste en que un servicio telemático o de telecomunicaciones esté disponible hacia los usuarios las 24 horas del día. La falta de disponibilidad de los sistemas informáticos admite la perturbación total del servicio. La no existencia de la disponibilidad afecta directamente la productividad de las organizaciones de índole corporativo.[19]

Confidencialidad.- Consiste en que usuarios legítimos tengan acceso a la información de carácter privilegiada almacenada en ordenadores, servidores y bases de datos, entendiéndose que solamente personas de alto nivel de confiabilidad eviten que se divulgue la misma a usuarios malintencionados cuyo objetivo es apoderarse de los datos de carácter sensible para beneficio propio.[19]

Integridad.- La integridad de la información consiste en que los datos de carácter confidencial no hayan sido manipulados con anterioridad antes de ser transmitidos por la red corporativa de la organización y almacenados en los servicios de tecnología de las empresas, es decir que no deberá presentarse alteraciones sin que se produzcan operaciones maliciosas por personas o sistemas no autorizados.[19]

Autenticidad.- Es la legitimidad de la información es aquella que proviene por medio de servicios auténticos es decir que los datos sensibles descienden de una fuente que está autorizada por entes regulares para la transmisión de los mismos a los usuarios finales. Contra la autenticidad de los activos lógicos podemos tener la alteración del origen o el contenido de los datos. Contra la autenticidad de los usuarios corporativos de los servicios de acceso empresariales, podemos tener la suplantación de identidad.[19]

2.2.24 Visión de Conjunto sobre los riesgos detectados mediante una auditoria de seguridad informática

Para ejecutar una detección de amenazas realizamos lo siguiente:

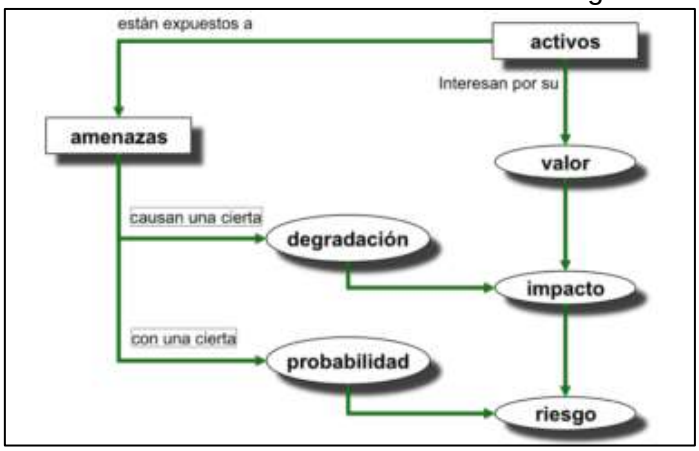
- Análisis de Riesgos
- Gestión de Riesgos

Análisis de Riesgo

El análisis de riesgo es uno de los puntos de gran importancia para la gestión de la seguridad informática en las organizaciones dedicadas a la prestación de servicios Streaming de audio y video bajo demanda, el análisis en mención es la parte fundamental del proceso de seguridad informática donde los administradores de tecnología deberán mantener actualizado los esquemas principales para la gestión de riesgos, este procedimiento servirá para determinar el riesgo existente en el sistema, a través del siguiente diagrama que se detalla gráficamente.[19]

Elementos de los análisis de riesgo potenciales

Gráfico 12 Gestión de Análisis de Riesgos

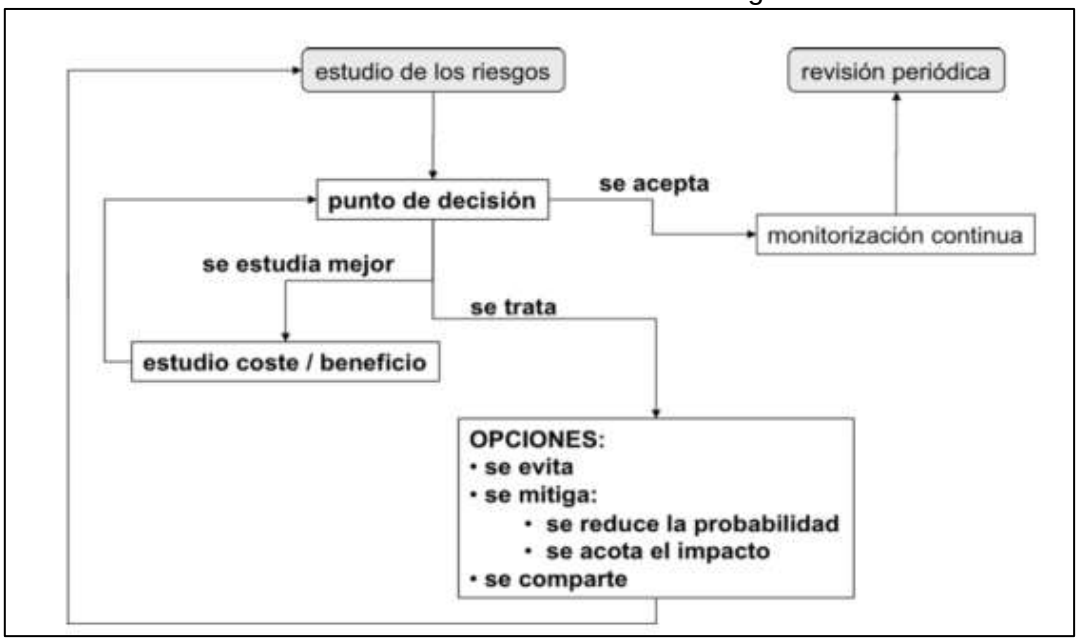


Fuente: Trabajo de Investigación
Autores: Amutio Gómez, Miguel Ángel.

Tratamiento de los riesgos

Actividades encaminadas a modificar la situación de riesgo, que permite organizar la defensa concienzuda y prudente, Es así que mediante la Reevaluación del riesgo y la evaluación de riesgo se ha determinado nuevas salvaguardas que ayuden a disminuir la materialización de amenaza frente a un activo, para seguir operando en las mejores condiciones.

Gráfico 13 Tratamiento de los riesgos



Fuente: Trabajo de Investigación
Autores: Amutio Gómez, Miguel Ángel.[19]

2.2.25 Determinación de activos

Los activos son los elementos que constituyen un valor lógico o un beneficio para cualquier organización de índole público y privado. Los activos de una empresa son aquellos que requieren un nivel de seguridad y protección elevado para evitar que usuarios no autorizados accedan a ellos y para la operatividad de la organización enfocada en el negocio.

Los activos de las organizaciones se clasifican de la siguiente manera:

Activos de Información: Base de datos de servidores Streaming bajo demanda, documentación del sistema, manuales técnicos, materiales de entrenamiento, procedimientos operativos y planes de continuidad de negocio.

Activos de software: Software de aplicaciones Streaming, sistemas operativos modo servidor de contenido audiovisual y herramientas de desarrollo.

Activos físicos: Estaciones de trabajo, servidores de comunicación audiovisual, dispositivos de red inalámbrica y alámbrica

Personas: Administradores de seguridades de redes, clientes de servicios Streaming bajo demanda y proveedores de Internet.

Imagen y prestigio de las compañías dedicadas a la prestación de servicios Streaming de audio y video bajo demanda.

Servicios: Servicios Streaming bajo demanda.

2.2.26 Amenazas

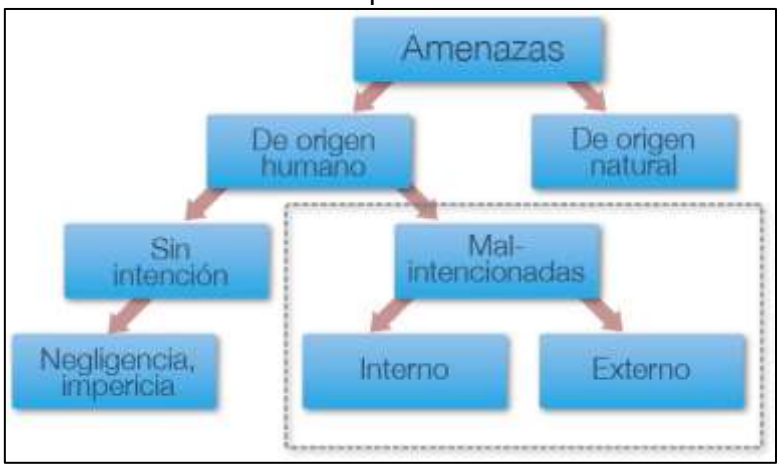
Las amenazas son aquellas que producen un incidente de seguridad en las organizaciones, produciendo daños o pérdidas de los activos de la información de gran importancia. Una amenaza es un evento potencial que trae consecuencias cuando se modifica el estado actual de la seguridad.[19]

2.2.27 Tipos de Amenazas

Los tipos de amenazas son aquellos que se clasifican por su naturaleza:

- No humanas.
- Humanas involuntarias.
- Humanas intencionales (proceden de un origen remoto).

Gráfico 14 Tipos de Amenazas



Fuente: http://www.magazcitum.com.mx/?p=2193#.WY43r1EjHIU

Autores: **Patricia Prandini (CISA y CRISC) y Marcela Pallero**

Amenazas en los sistemas Streaming de audio y video

La seguridad informática enfocada a los servidores Streaming de audio y video bajo demanda es de gran importancia como la seguridad en la red corporativa debido a que los servidores usualmente contienen una gran cantidad de información vital de la organización dedicada a la prestación de contenido audiovisual. Si un servidor está comprometido, todos sus implícitos pueden estar disponibles para que un pirata informático tenga la capacidad de manipular u obtenga el acceso al material de video bajo demanda.

2.2.28 Herramienta Pilar

Pilar es una herramienta desarrollada en lenguaje de programación java, específicamente para él análisis y procesos de gestión de riesgos ya que proporciona la información requerida en las actividades para el tratamiento de los diferentes riesgos identificados mediante el análisis en mención. Las actividades realizan labores de agregar activos físicos y lógicos, valorización e identificación de amenazas, detección de vulnerabilidades y las salvaguardas que ayudaran a proteger los servicios Streaming bajo demanda.[19]

Pilar está compuesto por un grupo de aplicaciones concretas para realizar el análisis de riesgos en diferentes superficies de la seguridad informática gestionando atender los requerimientos de los sistemas de tecnología de la información y comunicación como es la confidencialidad, autenticidad, disponibilidad e integridad, disminuyendo los tiempos en la cual se interrumpe el servicio frente a un ataque cibernético o una amenaza. El análisis que se ejecuta puede ser cualitativo o cuantitativo, se basa en la metodología de Magerit para realizar los diferentes cálculos.[19]

2.2.29 Caracterización de Activos

La caracterización de activos se detalla en tres sub-tareas:

- Identificación de los activos
- Dependencia entre los activos
- Valoración de activos

2.2.30 Identificación de los Activos

La inicialización de un análisis de riesgos es mediante el proceso de identificación y selección de todos los activos implicados en los sistemas de la información de contenido audiovisual es decir los elementos comprendidos en gestionar la comunicación vía Streaming hacia los clientes suscriptores en la cual se detallan en esta labor para ir descubriendo la fortaleza y el nivel de seguridad que poseen luego de su implementación.

Debemos ser muy minuciosos al momento de identificar los activos puesto que esto nos lleva a revelar la dependencia y luego darle su valoración con referencia a los activos.

También me ayuda a identificar y valorar las amenazas existentes y poder definir qué salvaguarda debo escoger para garantizar la protección del sistema.

2.2.31 Servicios internos

Las organizaciones y empresas dedicadas a la prestación de servicios Streaming bajo demanda integran los siguientes servicios:

- Internet
- Tecnología Streaming

2.2.32 Aplicaciones software de Streaming bajo demanda:

- Gestor de Base de datos de usuarios suscriptores
- Métodos de autenticación.
- Sistemas de encriptación.
- Aplicaciones móviles Streaming bajo demanda

2.2.33 Equipos Streaming:

- Servidores Streaming bajo demanda montados en el internet.
- Televisores Smart TV.
- Servidores de Base de Datos.
- Sistemas IPTV.
- Estaciones de trabajo.

2.2.34 Comunicaciones y redes:

- Redes de área local.
- Redes de Fibra Óptica.
- Redes Satelitales.
- Redes Inalámbricas.
- Redes Móviles 3G y 4G.

2.2.35 Instalaciones

- Centros de Cómputo.
- Conjuntos residenciales.
- Dispositivos móviles.
- Ordenadores.
- Hoteles
- Estaciones de metro
- Buses de metro
- Centro comerciales.
- Hospitales.
- Instituciones Públicas y Privadas.

2.2.36 Equipamiento auxiliar:

- Cableado.
- Alimentación eléctrica.
- Antenas.

2.2.37 Personal que componen un sistema Streaming:

- Usuario suscriptor.
- Administrador de Base de Datos.
- Administrador del Servidor Streaming.
- Mantenimiento y soporte de red de audio y video.

En la herramienta pilar integramos todos los activos físicos y lógicos, referente al proyecto de titulación en fase de desarrollo para iniciar el proceso de análisis una vez que se ha detectado todos los activos.

Se debe ir ingresando cada activo según la clasificación establecida por la herramienta Pilar.

Gráfico 15 Identificación de Activos

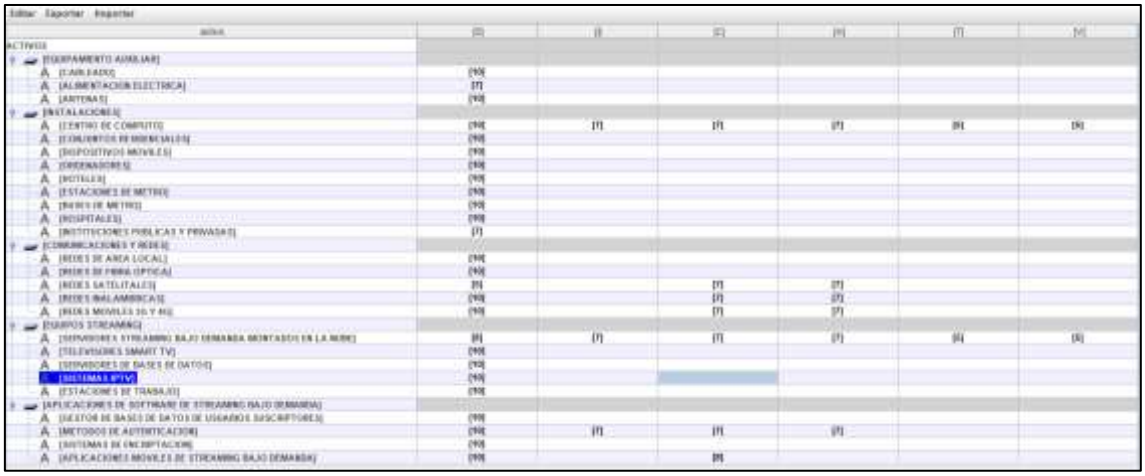
Fuente: Trabajo de Investigación
Autor: Simón Ballesteros – Francisco Sarmiento

2.2.38 Valoración de los activos

Para la valoración de los activos de la organización debemos considerar la siguiente información:

- Activos relevantes dentro del sistema a analizar
- Valoración de las dimensiones de seguridad son importantes

Gráfico 16 Valoración de Activos

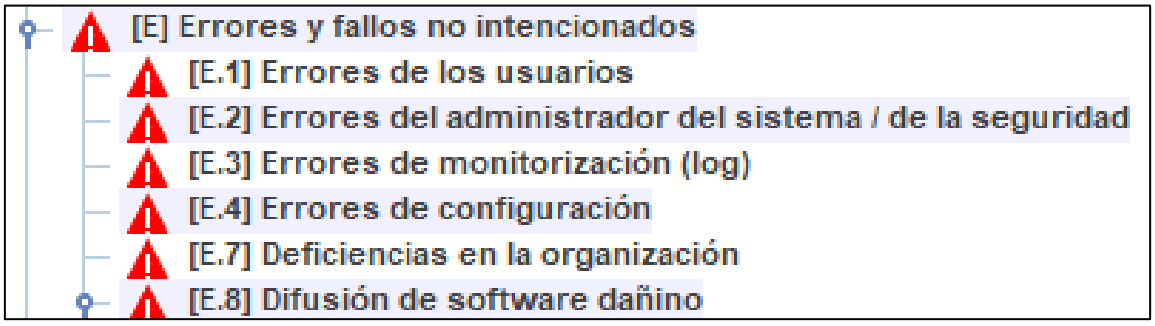


Fuente: Trabajo de Investigación
Autor: Simón Ballesteros – Francisco Sarmiento

2.2.39 Identificación de las amenazas

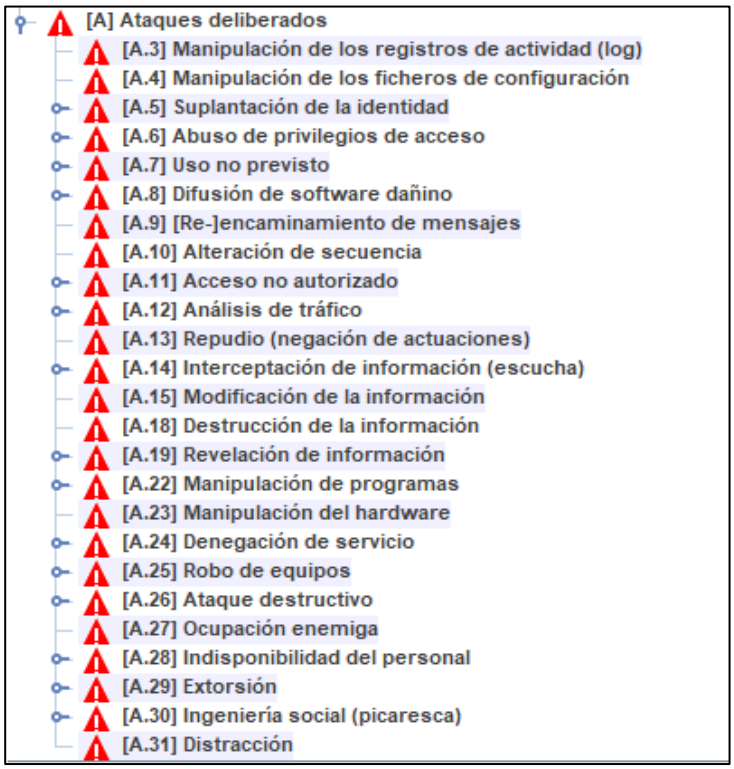
El objetivo de la tarea es fijar el ambiente al que está expuesta la tecnología Streaming de audio video bajo demanda estudiada, y que consecuencias se derivarían de ellas y cuál es la probabilidad de que ocurra, es decir conocida como conoce a tu adversario.

Gráfico 17 Identificación de Amenazas



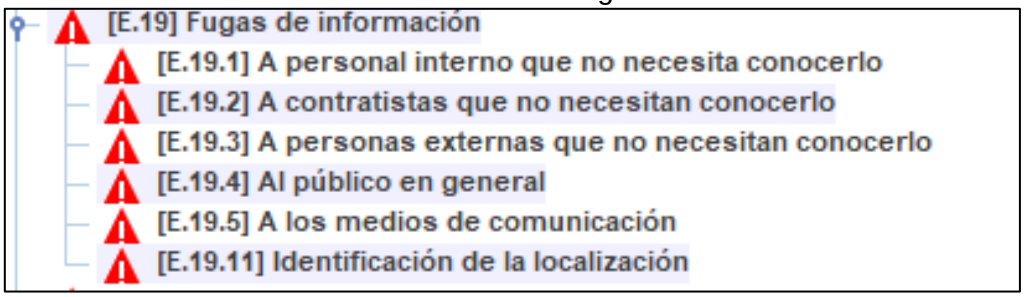
Fuente: Trabajo de Investigación
Autor: Simón Ballesteros – Francisco Sarmiento

Gráfico 18 Identificación de Amenazas



Fuente: Trabajo de Investigación
Autor: Simón Ballesteros – Francisco Sarmiento

Gráfico 19 Identificación de Fugas de información



Fuente: Trabajo de Investigación
Autor: Simón Ballesteros – Francisco Sarmiento

Gráfico 20 VALORACION DE AMENAZAS

Fuente: Trabajo de Investigación
Autor: Simón Ballesteros – Francisco Sarmiento

2.2.40 Caracterización de las salvaguardas

Esta actividad consiste en identificar las salvaguardas convenientes o aquellas medidas de protección que ayuden a resguardar el contenido audiovisual almacenado en los servidores de audio y video Streaming aplicando procedimientos o componentes tecnológicos que disminuya el riesgo o tenerlos bajo control, existen amenazas que son organizadas apropiadamente para comprometer los sistemas de información y comunicación, algunas de ellas demandan de ayuda técnica mediante programas o equipos que proporcionen soluciones para reducir los niveles de amenaza, en algunos casos comprometer la seguridad física del entorno en las instalaciones informáticas y en cierto modo las políticas de seguridad que no han sido correctamente definidas.

El objetivo final de esta actividad es doble: saber que se requiere salvaguardar el sistema informático por su eficacia y si es lo suficiente para mitigar el riesgo presente en toda la red corporativa protegiendo así la información de carácter confidencial, en la metodología de estudio detallaremos varias fases que abarcar, pero para el caso de estudio del proyecto consideraremos tres fases:

- Primera etapa llamada potencial.
- Segunda etapa llamada situación actual.
- Tercera etapa llamada objetivo.

Esta etapa consta de dos sub tareas:

- Identificación de las salvaguardas pertinentes
- Valoración de las salvaguardas

Gráfico 21 IDENTIFICACION DE SALVAGUARDAS

Fuente: Trabajo de Investigación
Autor: Simón Ballesteros – Francisco Sarmiento

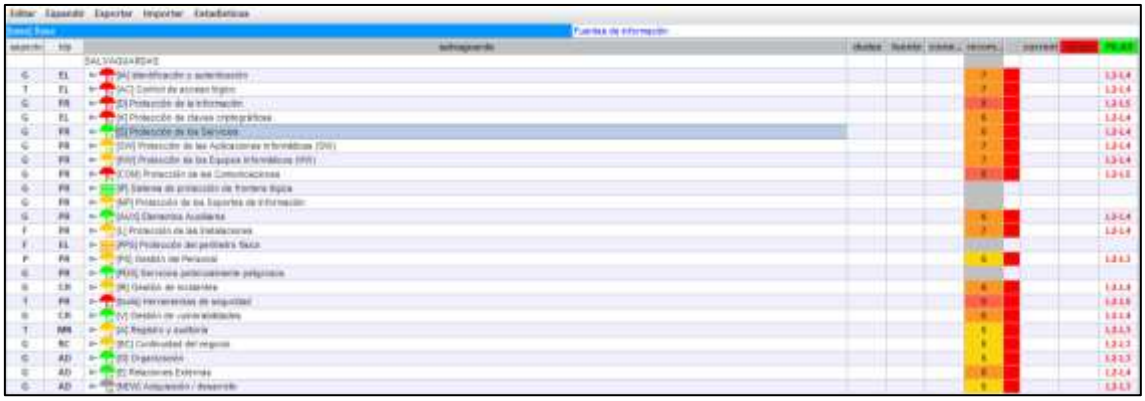
2.2.41 Valoración de las Salvaguardas

El objetivo principal de la metodología MAGERIT es el siguiente:

Identificar las salvaguardas que favorablemente satisfagan la mitigación máxima del riesgo identificado en la red de la organización.

Para este objetivo hemos aplicado la herramienta PILAR en su versión más reciente la cual ayudara a establecer las salvaguardas beneficiosas para la organización dedicadas a la prestación de servicios de audio y video Streaming.

Gráfico 22 VALORACION DE SALVAGUARDAS



Fuente: Trabajo de Investigación
Autor: Simón Ballesteros – Francisco Sarmiento

2.2.42 SEGURIDADES EN LOS SERVIDORES STREAMING DE AUDIO Y VIDEO BAJO DEMANDA

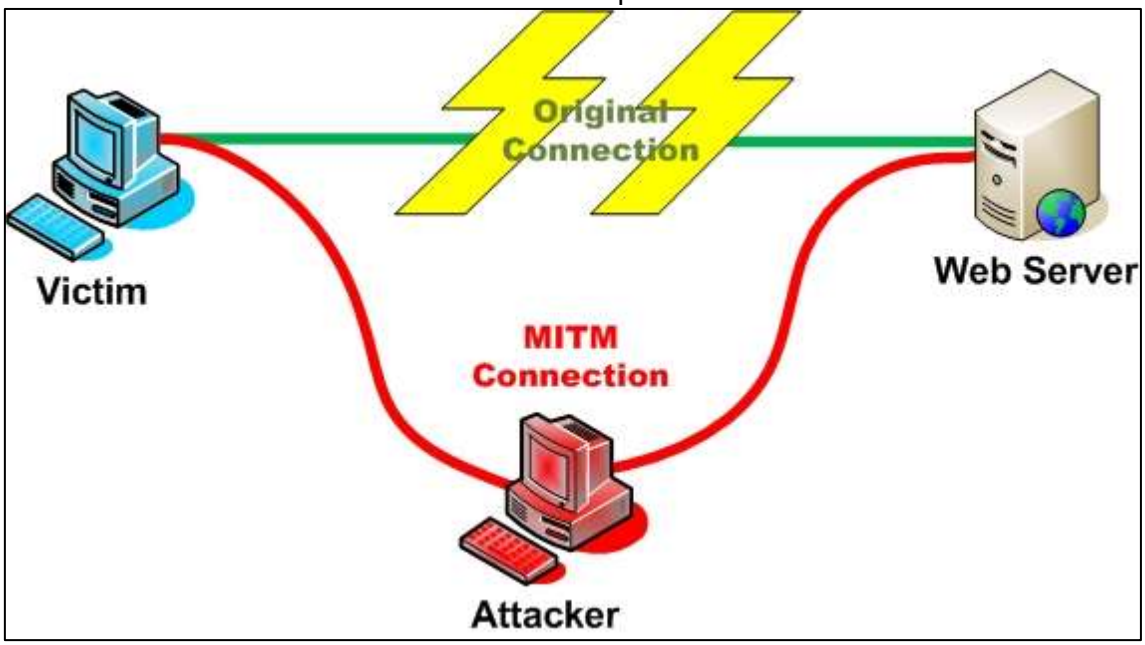
Tipos De Ataques A Los Servicios Streaming

Ataque hombre en el medio: El ataque hombre en el medio, es un ataque pasivo, que se lleva a cabo en redes LAN como WLAN la finalidad del ataque en mención es interceptar todo el tráfico de un usuario que está conectado a una red.[2]

Un ejemplo de este ataque se detalla a continuación:

En la red inalámbrica de la empresa Géminis se tienen 4 hosts conectados a la red uno de los host es el del atacante, el host A es una computadora de escritorio, el host B es un dispositivo móvil Android, el host C es una laptop y el host D es un servidor de aplicaciones de Streaming de audio y video bajo demanda. El host A quiere intercambiar información con el host D (éste host puede o no estar en la misma red), para ello, los paquetes deben enviarse a través del router o equipo de capa 3 que dirige el tráfico hacia el lugar de destino. Ahora, si el host C tiene intención de 'escuchar' el mensaje que A envía a D, sólo tiene que establecer un puente en la red entre A y el router inalámbrico.[2]

Gráfico 23 Ataque MITM



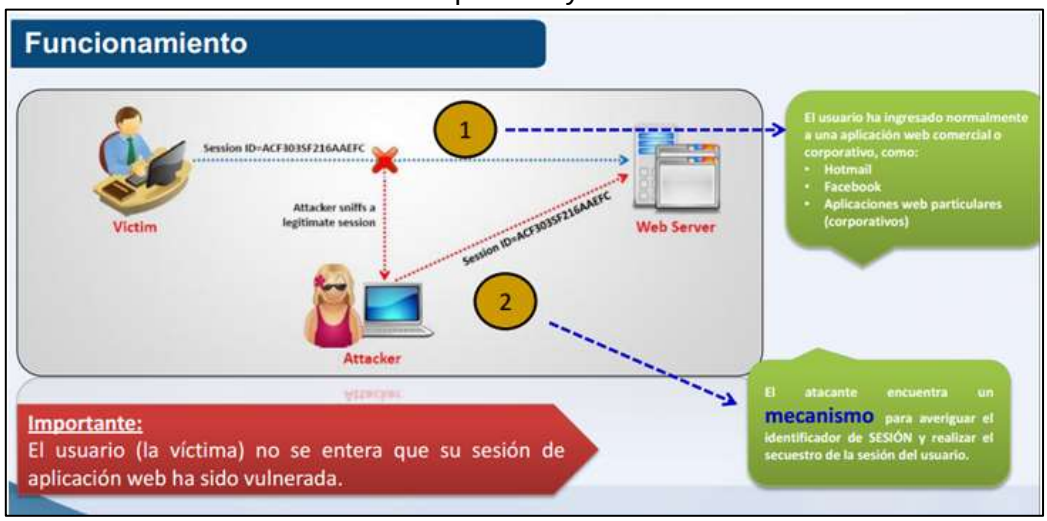
Fuente: http://highsec.es/2013/07/man-in-the-middle-mitm-suplantacion-de-dns-dns-spoofing-y-set/
Autor: Trabajo de investigación.

Inyección de Cookies en los navegadores de internet

El crecimiento de las aplicaciones web de servicios Streaming de audio y video en la actualidad han surgido un seguimiento de los usuarios que usan estas plataformas de entretenimiento, donde las mismas proporcionan una experiencia al usuario extremadamente personalizada a través de la búsqueda de contenido audiovisual. Normalmente, estos servicios se basan en material de audio y video. La amplia inclusión e incorporación de contenido en las páginas web de Streaming plantean muchas preocupaciones de privacidad en las organizaciones que brindan este servicio a los clientes e incluso si esos servicios no se utilizan directamente para el pasatiempo de los usuarios y servicios como de optimización de tiempo de carga del contenido, alojamiento del mismo, mejor experiencia de usuario con sugerencias personalizadas. Por lo tanto, los atacantes son vistos como peligros de privacidad recolectando información sobre sitios web visitados, preferencias del usuario o como instrumentos de vigilancia masiva.[20]

Los archivos de cookies tienen varios usos prácticos: las cookies se utilizan para el mantenimiento de la sesión, la persistencia de las tarjetas comerciales, las preferencias del usuario, para el rastreo de anuncios mostrados al usuario, la detección de los usuarios con fines analíticos, etc. Los archivos de cookies pueden almacenar información confidencial: detalles de autorización, identificador de sesión, información personal que los convierte en blanco popular de ataques y parte de vulnerabilidades exploradas como sesión Hijacking y MITM.[20]

Gráfico 24 Ataque de inyección de cookies



Fuente: https://losindestructibles.wordpress.com/2012/09/24/robo-de-sesiones-por-medio-de-cookies/

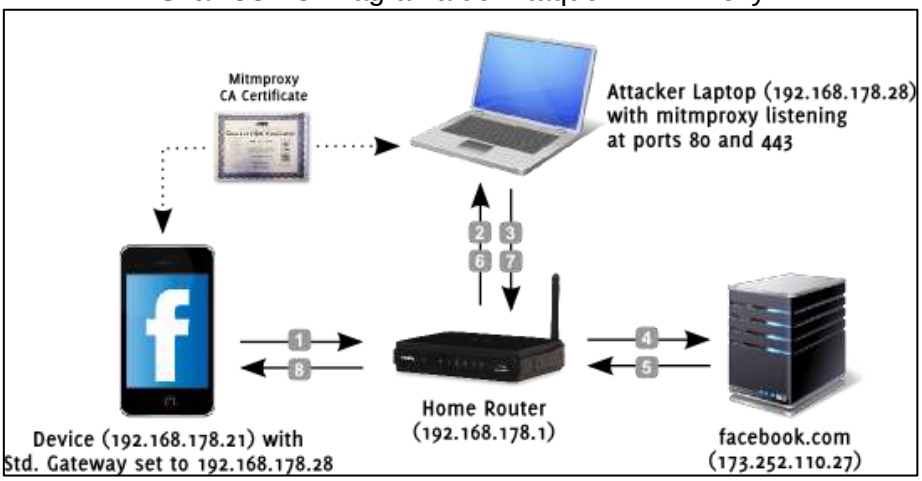
Autor: Trabajo de investigación.

2.2.43 Herramientas para realizar Ataques hombre en el medio

Ferret: Es un sniffer cuya funcionalidad es capturar cookies almacenándolas en un archivo de texto o fichero PCAP, este software se complementa con una aplicación llamada Hámster, la cual se encarga de abrir en el navegador Firefox el archivo con el contenido de la cookie y con esto los atacantes maliciosos acceden a los sitios con las cookies obtenidas para la ejecución de la herramienta Ferret el primer paso que se efectúa es un ataque ARP Spoofing que permite al cracker procesar el tráfico de la víctima, y poder acceder a los cookies de sesión de una aplicación web.

MITMPROXY: Es un proxy que permite interceptar y modificar tráfico HTTP mediante un ataque hombre en el medio, además permite almacenar el mismo e interceptar los certificados SSL generados.

Gráfico 25 Diagrama del Ataque MITM Proxy

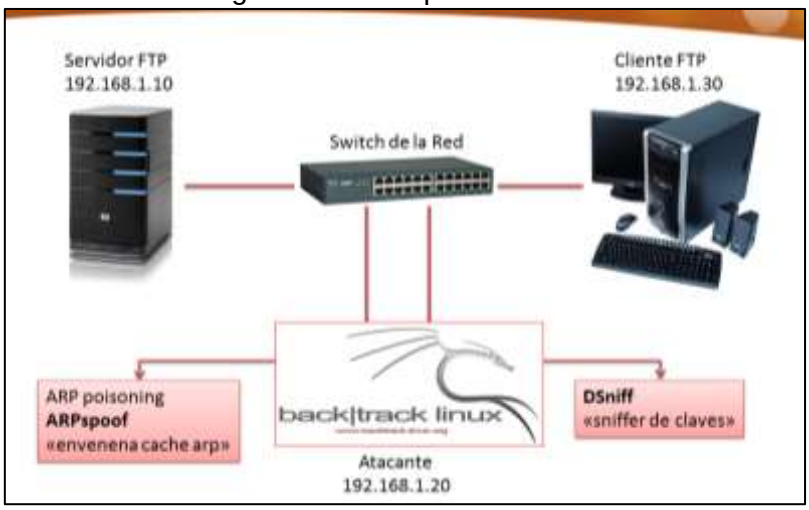


Fuente: https://blog.heckel.xyz/2013/07/01/how-to-use-mitmproxy-to-read-and-modify-https-traffic-of-your-phone/
Autor: Philipp C. Heckel

URLSnarf: Es una herramienta que filtra las peticiones de tráfico HTTP y los muestra por pantalla, esta aplicación permite realizar un seguimiento de la navegación de la víctima y las peticiones que esta solicita. Este software es muy utilizado si se necesita realizar alguna acción sobre el tráfico interceptado del involucrado y visualizar rápidamente los resultados adquiridos.

DSniff: Esta herramienta permite escuchar el tráfico y filtrar credenciales de protocolo inseguros, DSniff es el nombre de la suite que dispone de diferentes aplicaciones para el filtrado en distintas funciones como por ejemplo obtener cookies, filtrado de peticiones, correos electrónicos e imágenes.

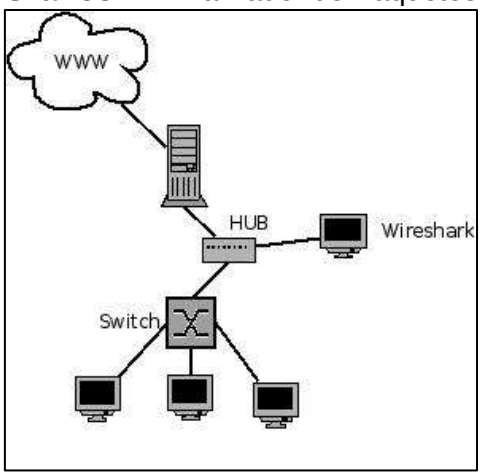
Gráfico 26 Diagrama del Ataque MITM mediante DSNIFF



Fuente: https://losindestructibles.wordpress.com/tag/dsniff/
Autor: Trabajo de Investigación

Wireshark: Es un analizador de tráfico muy esencial que permite analizar verificar todas la tramas que son capturadas en un adaptador de red, esta aplicación posee la funcionalidad de realizar grandes ataques en la red.

Gráfico 27 Analizador de Paquetes



Fuente: https://www.mentebinaria.com.br/artigos/0x05/0x05-wireshark.html
Autor: Trabajo de Investigación

2.7.2 Ficheros De Almacenamiento De Información De La Sesión De Usuario.

Cookies

Las cookies son ficheros de datos pequeños que prácticamente se alojan en su terminal cuando navega en internet y utiliza sitios web y otros servicios en línea. Estos archivos se emplean ampliamente para que marchen bien los sitios web, o para que sean más eficaz, así como para abastecer información de noticia y ayudar con el servicio o la caracterización de la publicidad. Las cookies no es la única tecnología que facilita el trabajo; también se emplean otras tecnologías equivalentes.[21]

Tipos de cookies que utiliza una plataforma Streaming.

- **Cookies esenciales:** Estas cookies son ajustadamente indispensables para el sitio web o servicio en línea que se esté utilizando. Por ejemplo, el usuario y sus Proveedores de servicio pueden usar estos ficheros para autenticar e identificar a sus miembros cuando utilizan sus sitios web y aplicaciones, de modo que puedan proveerles sus servicios. Además, los ayudan a aplicar sus Requisitos de uso para evitar fraudes y mantener la seguridad del servicio.[21]
- **Cookies de rendimiento y funcionamiento:** Estos Ficheros no son esenciales, pero nos socorren a personificar y optimar la práctica en línea con el servicio de Streaming bajo demanda. Por ejemplo, ayudan a recordar su contenido de preferencias para que no tenga que volver a escribir la información ya provista (por ejemplo, durante el inicio de sesión). También utilizamos estas cookies para recoger información (por ejemplo, páginas populares, tarifas de cambio, modelos de vista, proporción de clics y otra información) sobre el uso que hacen los visitantes del servicio de Streaming, de carácter que podamos optimizarlo y personalizarlo, así como nuestro sitio web, y ejecutar una investigación de mercado. Si se borran estos ficheros de cookies, el funcionamiento del servicio se verá limitado.[21]

- **Cookies de publicidad:** Estos ficheros traen información de la visita de los usuarios al sitio web, el uso que hace del servicio o su respuesta a los anuncios comerciales y los correos electrónicos, para presentar noticias más relevantes para el usuario suscrito. Este tipo de informes comerciales se llama "publicidad basada en el interés del usuario". Muchas de las cookies de anunciante asociadas al servicio de Streaming pertenecen a los propios Proveedores de servicio de la organización.[21]
- **Cookies de sesión:** son cookies temporales que permanecen alojadas en el navegador hasta que el usuario abandone la página web, por lo cual ninguna queda registrada en el disco duro del usuario. La información obtenida por medio de estos ficheros, sirven para analizar pautas de tráfico en la web. Prolongadamente, esto nos permite facilitar una mejor experiencia para optimizar el contenido y facilitando su uso.[22]
- **Cookies permanentes:** son acumuladas en el disco duro y nuestra web las lee cada vez que un usuario realiza una nueva inspección. Una web permanente posee una fecha el cual la cookie dejará de funcionar después de esa fecha. Las utilizamos, generalmente, para facilitar los servicios de contratación y registro.[22]

2.3. FUNDAMENTACIÓN SOCIAL

El proyecto de investigación de Análisis de duplicación de sesión por medio de cookies. Caso de estudio: Plataformas de audio y video bajo demanda por Streaming, cumple con los precisiones para que a futuro las organizaciones dedicadas a los servicios Streaming aseguren los sistemas de contenido audiovisual aplicando técnicas de protección que ayuden a salvaguardar el contenido logrando que solamente el usuario suscriptor tenga acceso al mismo.

¿Qué impacto social tendrá la ejecución del análisis de duplicación de sesión de usuario en las plataformas Streaming?

El impacto que tendrá el proyecto del análisis de duplicación de sesión por medio de cookies en las plataformas Streaming es que las organizaciones podrán conocer las debilidades del sistema de contenido audiovisual y con esto poder implementar métodos que proporcionen el aseguramiento del material de audio y video y que los usuarios suscriptores a los servicios Streaming tengan el acceso al mismo de manera privada.

¿De qué manera va a intervenir o a resolver la problemática existente la ejecución de los análisis de duplicación de sesión por medio de cookies?

Asegurando la confidencialidad, integridad y disponibilidad de los sistemas Streaming de audio y video bajo demanda donde los usuarios puedan autenticarse a las plataformas Streaming en mención de manera segura.

¿Qué impacto tendrá en la comunidad el proyecto en mención?

Que los usuarios puedan tener acceso a los servicios Streaming de manera segura y a su vez evitando la distribución ilegal del contenido audiovisual donde los atacantes no puedan lucrarse de los materiales de audio y video ilícitamente.

2.4 FUNDAMENTACIÓN LEGAL

2.4.1 Código Orgánico Integral Penal

Artículo 230.- Interceptación ilegal de datos.- Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.
3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

2.4.2 Ley de Comercio Electrónico

Art. 5.- Confidencialidad y reserva.- Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia.

Art. 9.- Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes

de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

Art. 32.- Protección de datos por parte de las entidades de certificación de información acreditadas.- Las entidades de certificación de información garantizarán la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de esta ley.

Art. 50.- Información al consumidor.- En la prestación de servicios electrónicos en el Ecuador, el consumidor deberá estar suficientemente informado de sus derechos y obligaciones, de conformidad con lo previsto en la Ley Orgánica de Defensa del Consumidor y su Reglamento.

Cuando se tratare de bienes o servicios a ser adquiridos, usados o empleados por medios electrónicos, el oferente deberá informar sobre todos los requisitos, condiciones y restricciones para que el consumidor pueda adquirir y hacer uso de los bienes o servicios promocionados.

La publicidad, promoción e información de servicios electrónicos, por redes electrónicas de información, incluida la internet, se realizará de conformidad con la ley, y su incumplimiento será sancionado de acuerdo al ordenamiento jurídico vigente en el Ecuador.

En la publicidad y promoción por redes electrónicas de información, incluida la Internet, se asegurará que el consumidor pueda acceder a toda la información disponible sobre un bien o servicio sin restricciones, en las mismas condiciones y con las facilidades disponibles para la promoción del bien o Servicio de que se trate.

En el envío periódico de mensajes de datos con información de cualquier tipo, en forma individual o a través de listas de correo, directamente o mediante cadenas de mensajes, el emisor de los mismos deberá proporcionar medios expeditos para que el destinatario, en cualquier tiempo, pueda confirmar su suscripción o solicitar su exclusión de las listas, cadenas de mensajes o bases de datos, en las cuales se halle inscrito y que ocasionen el envío de los mensajes de datos referidos.

La solicitud de exclusión es vinculante para el emisor desde el momento de la recepción de la misma. La persistencia en el envío de mensajes periódicos no deseados de cualquier tipo, se sancionará de acuerdo a lo dispuesto en la presente ley.

El usuario de redes electrónicas, podrá optar o no por la recepción de mensajes de datos que, en forma periódica, sean enviados con la finalidad de informar sobre productos o servicios de cualquier tipo.

2.5 HIPÓTESIS

¿Si en el ambiente de prueba se comprueba que se puede duplicar una sesión de usuario por medio de cookie, es necesario crear una guía de buenas prácticas para los usuarios finales y así evitar este tipo de inconvenientes?

¿Si más del 70% de los usuarios indican que las redes inalámbricas son vulnerables, se podría presentar métodos alternativos referentes a la navegación anónima?

¿Con navegadores que proporcionen una navegación anónima se disminuirá el nivel de intercepción de tráfico de internet que genera el usuario suscriptor del servicio Streaming bajo demanda?

2.6 VARIABLES DE INVESTIGACIÓN

Variable dependiente: Plataformas de audio y video bajo demanda por Streaming.

Variable independiente: Duplicación de sesión por cookies.

2.7 DEFINICIONES CONCEPTUALES

Servidor Streaming: Servidor de contenido multimedia donde los usuarios pueden tener el acceso a películas, series de televisión, novelas y demás para el aumento del entretenimiento.

Duplicidad de sesión: Abrir sesiones de usuarios en diferentes ordenadores conectados a una red sin la necesidad de saber el usuario y la contraseña.

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1 DISEÑO DE LA INVESTIGACIÓN

Los anteriores capítulos desarrollados han otorgado un enfoque de como comprender las tecnologías Streaming de audio y video bajo demanda, los tipos de amenazas y vulnerabilidades que acarrean en si estas plataformas de contenido audiovisual los ataques cibernéticos que pueden ser ejecutados por los crackers por medio de los fallos de seguridad identificados por los mismos hacen que las empresas dedicadas a la prestación de servicios audiovisuales, basado en estos puntos críticos se aplica la metodología de investigación de campo que es aquella que permite utilizar técnicas de recolección de datos para la recopilación de la información referente a los sistemas de Streaming de audio y video bajo demanda, para la ejecución del proceso de recabación de información se utilizara métodos de encuesta que serán dirigidas a los estudiantes de la unidad de titulación 2017 ciclo I de la Universidad de Guayaquil.[19]

Métodos de La Investigación

En esta sesión del proyecto referente al análisis del método de duplicación se considera el método de investigación analítico que permiten alcanzar u obtener un fin propuesto.

Método Analítico

El método analítico comprende todo lo que corresponda al análisis, enfocado en la distribución de porciones o elementos constitutivos conformados en el proceso de investigación. Con el uso de este método se sostendrá afirmaciones o conocimientos sobre los casos de investigación es indispensable detallar cada una de sus partes en lo más mínimo.

3.3.1 Tipo de investigación.

El tipo de investigación exploratorio está fundamentado principalmente en un análisis y del método de duplicación de sesiones por medio de Cookies en las tecnologías Streaming bajo demanda que ayudará a explorar los riesgos presentes y que tipo de daños se pueden surgir por medio de estos peligros en la duplicidad de sesiones, para aplicar medidas de protección que ayuden a evitar el acceso ilícito a los contenidos audiovisuales, tomando en consideración también que llegar a un mecanismo de protección no es válido y que el máximo grado de seguridad tampoco es el adecuado para salvaguardar la información de carácter confidencial, esta investigación proporcionara recomendaciones y las medidas apropiadas que se debe recoger para mitigar estos riesgos. Para efectuar la investigación aplicaremos una investigación de campo con el fin de explorar todos los efectos que causa en el momento que atacantes malicioso duplican sesiones de sistemas Streaming de audio y video bajo demanda en beneficio propio.[19]

La Investigación de campo consiste en la recolección de la información por medio de cuestionario de encuesta y entrevista que son directamente enfocadas a usuarios para tratar de un tema específico, las preguntas de encuestas elaboradas fueron dirigidas a los estudiantes de la Universidad de Guayaquil en la unidad de titulación 2017 ciclo I con el fin de recabar datos importantes referentes a las plataformas Streaming bajo demanda.

En la investigación referente al análisis de duplicidad de sesión se basó en la investigación de campo, por lo imprescindible conocer el entorno, observar los riesgos y amenazas sobre las duplicaciones de sesiones de usuarios y encuestar a estudiantes del curso de titulación 2017 ciclo I de sexo masculino y femenino entre edades de 24 a 42 años pertenecientes a la Universidad de Guayaquil.

3.2 POBLACIÓN Y MUESTRA

Población

Para esta investigación referente al análisis del método de duplicación de sesión por medio de cookies la población fue dirigida a los usuarios de la unidad de titulación de la carrera de Ingeniería en Networking y Telecomunicaciones:

Curso G1, Curso G2 y Curso G3 correspondiente a la unidad de titulación 2017 ciclo I.

Muestra

La muestra es un subconjunto representativo de la población que ayudan al investigador a seguir con el transcurso de la investigación. Existen diferentes tipos de muestreo. El tipo de muestra seleccionada dependerá de la calidad y cuán representativo se quiera sea el estudio de la población.

El muestreo es un elemento de gran importancia en donde el investigador puede verificar la factibilidad del proyecto, por la cual es imposible encuestar a todos los miembros de la población debido a los problemas de tiempo y recursos. Al seleccionar una muestra los investigadores estudian una parte o un subconjunto de la población, pero que la misma es lo suficientemente representativa para la ejecución de pruebas experimentales.

3.2.1 Planteamiento de La Muestra

Para realizar el cálculo de la muestra se define lo siguiente:

m= Tamaño de la población (100)

e= Error de estimación (0.06)

n= Total de la muestra

$$\mathrm{n} = \frac{m}{e^2(m-1)+1}$$

$$n = \frac{100}{(0.06)^2(100-1)+1}$$

$$n = \frac{100}{(0.06)^2(99)+1}$$

$$n = \frac{100}{(0.0036)(99)+1}$$

$$n = \frac{100}{0.3564+1}$$

$$n = \frac{100}{1.3564}$$

$$n = 73.72$$

$$n = 74\ personas\ a\ encuestar$$

Tabla 3 Muestra estratificada no proporcional

INVOLUCRADOS	POBLACION	MUESTRA	PORCENTAJE
Usuarios de la Unidad de Titulación de la Universidad de Guayaquil.	100	74	100%
TOTAL:	**100**	**74**	**100%**

Fuente: Trabajo de Investigación
Elaboración: Simón Ballesteros - Francisco Sarmiento

3.3 INSTRUMENTOS DE RECOLECCIÓN DE DATOS

3.3.1 Encuesta

La encuesta es un estudio en el cual el investigador obtiene los datos a partir de plantear un conjunto de preguntas normalizadas dirigidas a una muestra representativa o al conjunto total de la población estadística en estudio, formada a menudo por personas, empresas o entes institucionales, con el fin de conocer estados de opinión, características o hechos específicos o un tema a tratar.

3.3.2 Tipos de encuestas

Existen varios tipos de encuestas que se detallan a continuación:

- **Encuestas cara a cara:** Consisten en realizar entrevistas directas y personales con cada encuestado.
- **Encuestas telefónicas:** Este tipo de encuesta consiste en una entrevista vía telefónica con cada encuestado.
- **Encuestas por correo:** Consiste en el envío de un cuestionario a los potenciales encuestados, pedirles que lo rellenen y hacer que lo devuelvan completo.
- **Encuestas por Internet, encuestas online:** Este tipo de encuesta consiste en colocar un cuestionario en una página web o crear una encuesta online y enviarla a los correos electrónicos de cada usuario a encuestar.

3.3.3 Procesamiento y Análisis

El proceso y análisis surge a partir de la finalización de las encuestas a la muestra y se comienza a interpretar cada ítem, para realizar esta interpretación se utiliza la herramienta Microsoft Excel, la cual permite desarrollar gráficos de pastel para la tabulación de datos por medio de la utilización de complementos como crear tablas y generar gráficos estadísticos, en este caso el diagrama de barra fue el seleccionado para la representación de salida.

Esto permite manejar una excelente distribución de la información para un adecuado análisis y compresión de la operación llevando así, a lograr la interpretación de datos concretos e ir obtenido los porcentajes generales para sustentar los argumentos y propuestas validos puntualizados en el presente documento.

Todo el proceso requiere seguir una serie de pasos sencillos para elaboración de cada opción mencionada en el texto:

- Se plantearán un total de 10 preguntas.
- El objetivo por el cual se formuló las preguntas, consultar las opiniones.
- Elaborar un gráfico de pastel por cada pregunta de la encuesta y porcentaje de los resultados obtenidos.
- Representar gráficamente los porcentajes resultantes de la encuesta.
- Análisis e interpretación de la información por cada pregunta.
- Una resumen de los resultados obtenidos.
- Se presentan la validación de la hipótesis.

3.3.4 Análisis e Interpretación de Resultados

A continuación, se visualizarán los datos de la encuesta, entre esto es el origen del análisis e interpretación de resultados en base a la aplicación previa de los instrumentos y herramientas de recolección para la información obtenida.

En el proceso cada pregunta fue enfocada a los estudiantes mediante la selección de repuesta de forma opcional con los valores de si o no, es obligatorio marcar una de estas 2 opciones.

El formulario está conformado por 10 ítems. La finalidad de la operación se basó en recopilación de datos para validar, respaldar y mantener resultados claros, precisos y evidenciables. La distribución de información que se reflejará está sustentada por su respectiva conclusión y la resolución de los casos manejados en la investigación.

3.3.5 Encuestas Realizada

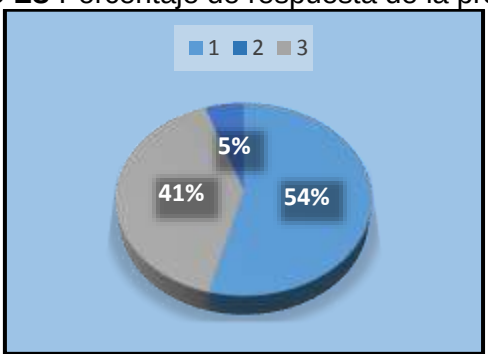
1. ¿Qué entiende usted por servidor Streaming de audio y video bajo demanda?

Tabla 4 Resultados pregunta 1

ALTERNATIVAS	CANTIDAD	PORCENTAJES
Servidor Que Proporciona Contenido de audio y video bajo demanda.	40	54%
Servidor que facilita contenido por Streaming en vivo.	30	41%
Ninguna de las Anteriores.	4	5%
Total	74	100%

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros –Francisco Sarmiento

Gráfico 28 Porcentaje de respuesta de la pregunta 1



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros –Francisco Sarmiento

Análisis e interpretación

Mediante la encuesta realizada a los estudiantes de la unidad de titulación 2017 ciclo I, surgió que el 54% de los encuestados dan su afirmación sobre el concepto de Streaming de audio y video bajo demanda. Por lo contrario el 41% dice que los Streaming son en vivo y el 5% no conoce sobre el termino Streaming.

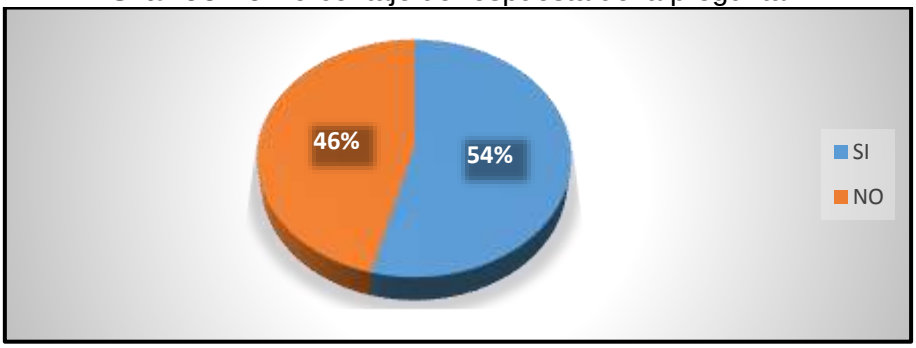
2. ¿Utiliza algún tipo de plataforma de servicio Streaming de audio y video bajo demanda?

Tabla 5 Resultados pregunta 2

ALTERNATIVAS	CANTIDAD	PORCENTAJES
SI	40	54%
NO	34	46%
Total	74	100%

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros –Francisco Sarmiento

Gráfico 29 Porcentaje de respuesta de la pregunta 2



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros –Francisco Sarmiento

Análisis e interpretación

Mediante la encuesta realizada a los estudiantes de la unidad de titulación 2017 ciclo I, surgió que el 54% de los encuestados utilizan las plataformas Streaming de pago para la visualización de contenido de series, películas y novelas. Por lo contrario el 46% no utilizan los servicios Streaming.

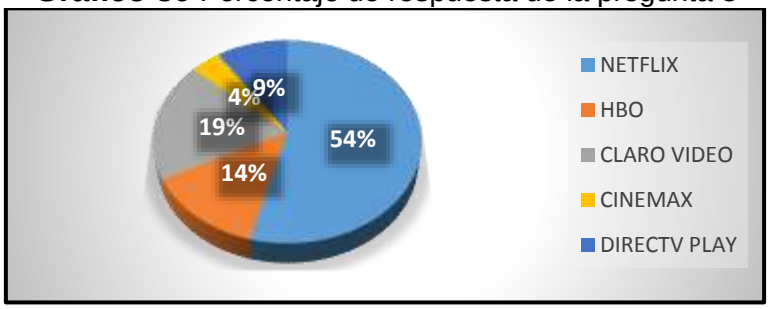
3. ¿Dentro del Ecuador, ¿cuál es servidor Streaming de pago más conocido?

Tabla 6 Resultados pregunta 3

ALTERNATIVAS	CANTIDAD	PORCENTAJES
NETFLIX	40	54%
HBO	10	14%
CLARO VIDEO	14	19%
CINEMAX	3	4%
DIRECTV PLAY	7	9%
Total	74	100%

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros –Francisco Sarmiento

Gráfico 30 Porcentaje de respuesta de la pregunta 3



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros –Francisco Sarmiento

Análisis e interpretación

Mediante la encuesta realizada a los estudiantes de la unidad de titulación 2017 ciclo I, surgió que el 54% de los encuestados dan su afirmación que Netflix es el servidor Streaming de audio y video bajo demanda más conocido en el Ecuador. Por lo contrario el 19% comenta que Claro Video es el más conocido.

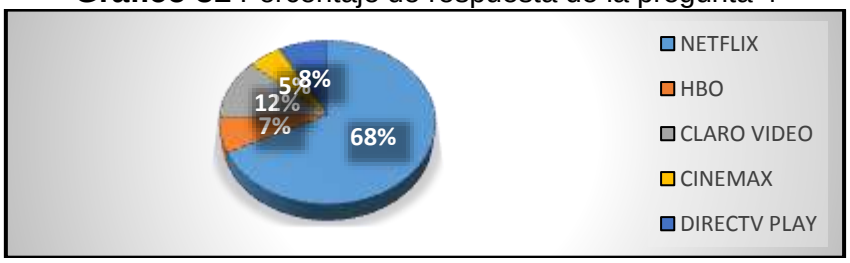
4. ¿Cuáles son las empresas dedicadas a los servicios Streaming bajo demanda que ganaron popularidad en el mercado ecuatoriano?

Tabla 7 Pregunta 4

ALTERNATIVAS	CANTIDAD	PORCENTAJES
NETFLIX	50	68%
HBO	5	7%
CLARO VIDEO	9	12%
CINEMAX	4	5%
DIRECTV PLAY	6	8%
Total	74	100%

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros –Francisco Sarmiento

Gráfico 31 Porcentaje de respuesta de la pregunta 4



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros –Francisco Sarmiento

Análisis e interpretación

Mediante la encuesta realizada a los estudiantes de la unidad de titulación 2017 ciclo I, surgió que el 68% de los encuestados afirmaron que la plataforma Netflix gano popularidad en el mercado ecuatoriano con más de 6000 usuarios. Por lo contrario el 12% de los encuestados mencionan a Claro Video como la plataforma con más popularidad en el mercado.

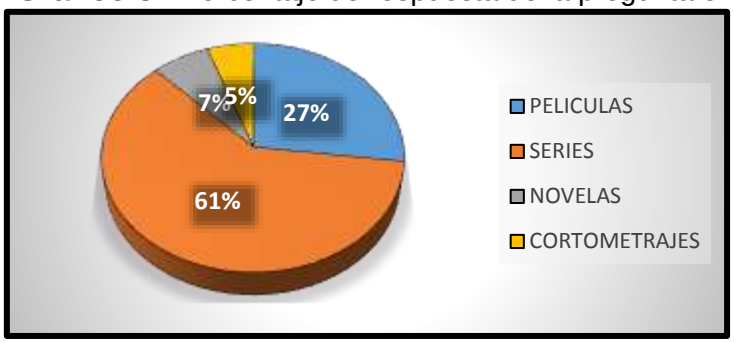
5. ¿Cuál es el contenido de audio y video más visualizado en las plataformas Streaming mencionadas anteriormente por los usuarios?

Tabla 8 Resultados pregunta 5

ALTERNATIVAS	CANTIDAD	PORCENTAJES
PELICULAS	20	27%
SERIES	45	61%
NOVELAS	5	7%
CORTOMETRAJES	4	5%
Total	74	100%

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros –Francisco Sarmiento

Gráfico 32 Porcentaje de respuesta de la pregunta 5



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros –Francisco Sarmiento

Análisis e interpretación

Mediante la encuesta realizada a los estudiantes de la unidad de titulación 2017 ciclo I, surgió que el 61% de los encuestados comentan que el contenido más visualizado en las plataformas Streaming de audio y video bajo demanda son las series de películas. Mientras que el 27% dice que el contenido audiovisual más visto por el Publico mundial son las películas y por último el 7% y el 5% mencionan que las novelas y los cortometrajes son los más vistos.

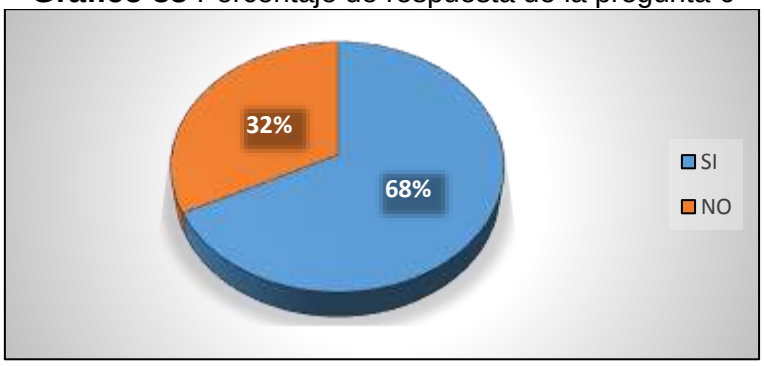
6. ¿Cree usted que la tecnología Streaming de audio y video bajo demanda reemplazara a la televisión de pago tradicional?

Tabla 9 Resultados pregunta 6

ALTERNATIVAS	CANTIDAD	PORCENTAJES
SI	50	68%
NO	24	32%
Total	74	100%

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros –Francisco Sarmiento

Gráfico 33 Porcentaje de respuesta de la pregunta 6



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros –Francisco Sarmiento

Análisis e interpretación

Mediante la encuesta realizada a los estudiantes de la unidad de titulación 2017 ciclo I, surgió que el 68% de los encuestados afirman que la tecnología de audio y video Streaming bajo demanda reemplazara a la televisión de pago tradicional. Por lo contrario el 32% dice que la tecnología Streaming no reemplazara a la televisión privada.

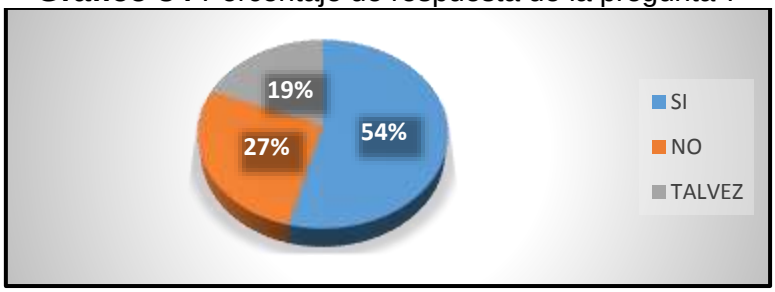
7. ¿La distribución de contenido audiovisual de manera ilegal, en las tiendas de video, ¿proviene del acceso ilícito a las plataformas Streaming de pago?

Tabla 10 Resultados pregunta 7

ALTERNATIVAS	CANTIDAD	PORCENTAJES
SI	40	54%
NO	20	27%
TALVEZ	14	19%
Total	74	100%

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros –Francisco Sarmiento

Gráfico 34 Porcentaje de respuesta de la pregunta 7



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros –Francisco Sarmiento

Análisis e interpretación

Mediante la encuesta realizada al a los estudiantes de la unidad de titulación 2017 ciclo I, surgió que el 54% de los encuestados mencionan que la distribución de contenido audiovisual en las tiendas de video proviene del acceso ilícito a las plataformas Streaming de pago. Por lo contrario el 27% dice que el contenido distribuido en las tiendas es de manera legal y el 19% comenta que talvez puede ser ilícito en el contenido audiovisual.

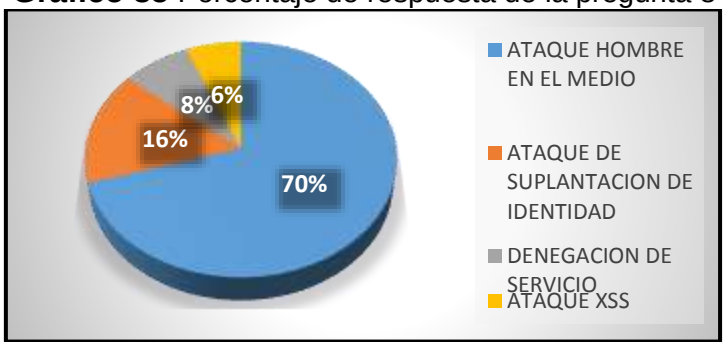
8. Conoce usted, ¿cuál es el tipo de ataque realizado en las plataformas Streaming de audio y video bajo demanda?

Tabla 11 Resultados pregunta 8

ALTERNATIVAS	CANTIDAD	PORCENTAJES
ATAQUE HOMBRE EN EL MEDIO	45	70%
ATAQUE DE SUPLANTACION DE IDENTIDAD	10	16%
DENEGACION DE SERVICIO	5	8%
ATAQUE XSS	4	6%
Total	74	100%

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros –Francisco Sarmiento

Gráfico 35 Porcentaje de respuesta de la pregunta 8



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros –Francisco Sarmiento

Análisis e interpretación

Mediante la encuesta realizada al a los estudiantes de la unidad de titulación 2017 ciclo I, surgió que el 70% de los encuestados afirmaron que los ataques informáticos realizados a las plataformas Streaming son los ataques hombre en el medio. Por lo contrario el 16% dice que los ataques realizados a los servidores Streaming son los ataques de suplantación de identidad.

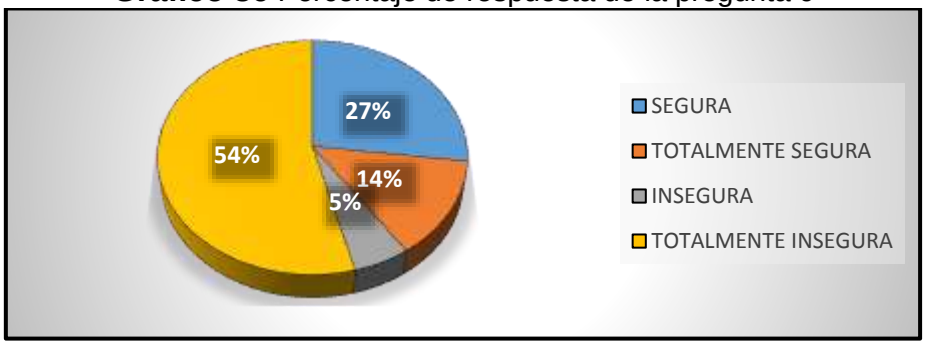
9. ¿Qué opina usted sobre la seguridad de su red inalámbrica cuando accede a una de las plataformas Streaming de audio y video?

Tabla 12 Resultados pregunta 9

ALTERNATIVAS	CANTIDAD	PORCENTAJES
SEGURA	20	27%
TOTALMENTE SEGURA	10	14%
INSEGURA	4	5%
TOTALMENTE INSEGURA	40	54%
Total	74	100%

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros –Francisco Sarmiento

Gráfico 36 Porcentaje de respuesta de la pregunta 9



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros –Francisco Sarmiento

Análisis e interpretación

Mediante la encuesta realizada al a los estudiantes de la unidad de titulación 2017 ciclo I, surgió que el 54% de los encuestados dan su afirmación que la red inalámbrica instalada en sus residencias es totalmente insegura. Por lo contrario el 27% afirma que su red es segura por los mecanismos de protección que implementa el proveedor de servicios de internet en la red de los clientes.

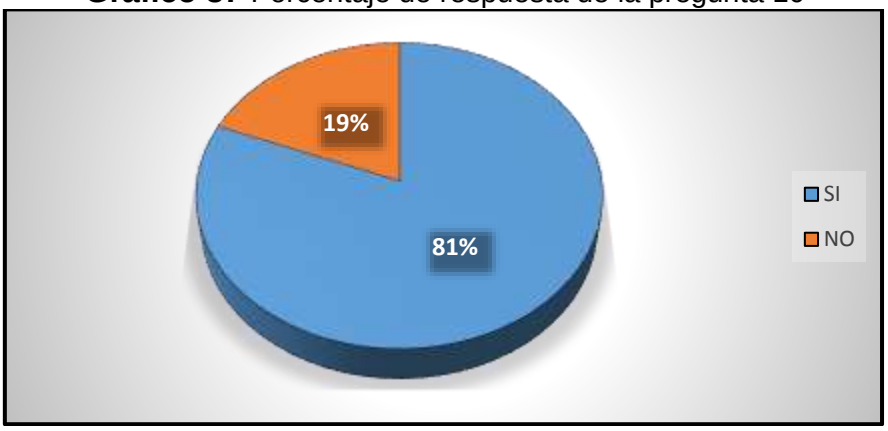
10. ¿Conoce usted el término de cookies?

Tabla 13 Resultados pregunta 10

ALTERNATIVAS	CANTIDAD	PORCENTAJES
SI	60	81%
NO	14	19%
Total	74	100%

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros –Francisco Sarmiento

Gráfico 37 Porcentaje de respuesta de la pregunta 10



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros –Francisco Sarmiento

Análisis e interpretación

Mediante la encuesta realizada al a los estudiantes de la unidad de titulación 2017 ciclo I, surgió que el 81% de los encuestados afirman que conocen el término de cookies. Por lo contrario el 19% dicen que no conocen el término de cookies.

3.3.6 Validación de la Hipótesis

¿Si en el ambiente de prueba se comprueba que se puede duplicar una sesión de usuario por medio de cookie, es necesario crear una guía de buenas prácticas para los usuarios finales y así evitar este tipo de inconvenientes?

Esta hipótesis se valida porque en el test penetración realizado que se encuentra en el anexo 2 se comprueba que es posible ejecutar el método de duplicación de sesión por medio de cookies ocasionado daños al usuario final, siendo necesario el desarrollo de una guía de buenas prácticas.

¿Si más del 70% de los usuarios indican que las redes inalámbricas son vulnerables, se podría presentar métodos alternativos referentes a la navegación anónima?

Esta hipótesis se valida en la pregunta número 8 de la encuesta planteada en el capítulo tres, donde se pudo verificar que más del 70% de los usuarios afirmaron que las redes inalámbricas son vulnerables a los ataques informáticos, dando inicio a utilizar métodos alternativos referentes a la navegación anónima.

¿Con navegadores que proporcionen una navegación anónima se disminuirá el nivel de intercepción de tráfico de internet que genera el usuario suscriptor del servicio Streaming bajo demanda?

Tomando en consideración los resultados del test de penetración se guiara al usuario final a poner en práctica el uso de navegadores que faciliten la navegación anónima para disminuir el nivel de intercepción de tráfico de internet en las plataformas de audio y video bajo demanda por Streaming.

CAPÍTULO IV

4.1 PROPUESTA TECNOLÓGICA

4.1.1 Análisis de Factibilidad

Luego de identificar la problemática actual, presente en la plataforma Streaming de audio y video bajo demanda de prueba, referente a la duplicidad de sesión de un usuario, los atacantes pueden vender la sesión capturada, ocasionándole a las organizaciones dedicadas a la prestación de servicios Streaming un grave problema de fiabilidad, logrando que ellas pierdan nuevos usuarios por suscribirse, debido a que estos usuarios prefieren comprar la cookie de sesión por un valor mínimo, favoreciendo a los piratas informáticos que se benefician de estas falencias que poseen las empresas que prestan este tipo de servicio a los clientes suscriptores. Con la implementación de un servidor de audio y video Streaming de manera local llamado EMBY MEDIA SERVER se realizaran pruebas de duplicidad de sesión por medio de cookies para demostrar los riesgos que se pueden acarrear al no protegerse de este tipo de método, que utilizan los crackers para tener el acceso al contenido de audio y video en beneficio propio, además se tomó en consideración cuatro áreas específicas que son enfocadas al proyecto de análisis del método de duplicación de sesión por medio de cookies en las plataformas Streaming de audio y video bajo demanda tales como:

- Factibilidad Operacional.
- Factibilidad Técnica.
- Factibilidad Económica.
- Factibilidad Legal.

4.1.2 Factibilidad Operacional

Tomando en consideración el ambiente de prueba implementado y realizando el respectivo pentest, indicamos que el análisis del método de duplicación de sesión por medio de cookies es factible operacionalmente ya que se puede recomendar el uso de una guía de buenas prácticas para el usuario final, con la finalidad de proteger la sesión

del mismo, pero con un buen conocimiento aprenderá todo lo que se necesita para tener seguridad de navegación Web, De igual forma se hará hincapié sobre el uso de navegadores que proporcionen navegación anónima de tipo web VPN.

4.1.3 Factibilidad Técnica

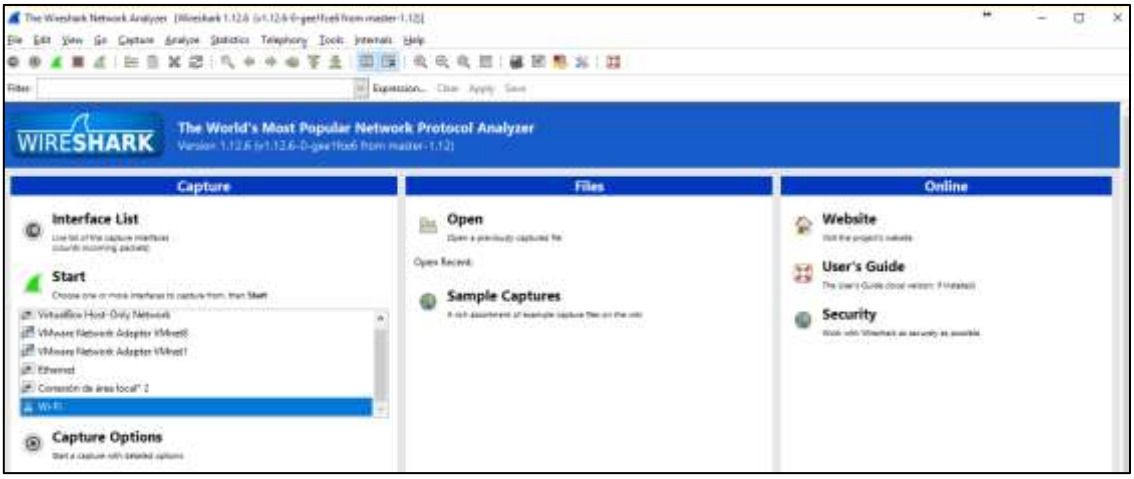
En esta etapa de la factibilidad técnica se identificaran las herramientas necesarias para ejecutar las pruebas de duplicación de sesión y además para la realización del proyecto de investigación se utilizó el sistema operativo libre Ubuntu fácil de encontrar en los repositorios Web para el montaje de un servidor Streaming bajo demanda de prueba, instalando la aplicación de código abierto Emby la cual se manejara como entorno de experimento para la realización de un análisis del método de duplicación de sesión por medio de cookies utilizando el aplicativo de Evil Foca encontrado en las fuentes de seguridad informática y de fácil descarga.

A continuación se detallaran las herramientas y complementos a utilizar en el proyecto de “Análisis de métodos de duplicación por medio de cookies” en las cuales son las siguientes:

Listado de herramientas que se utilizaran en el proyecto

WIRESHARK: Esta herramienta posee la funcionalidad de realizar captura de trafico de una red de área local o una WLAN, detectado las direcciones IPs disponibles en cada equipo conectado a la red, con la finalidad de interceptar el tráfico y por medio del mismo se captura el tráfico de toda la red proporcionado por los clientes para verificar si existe una captura de sesión por parte de uno de ellos.

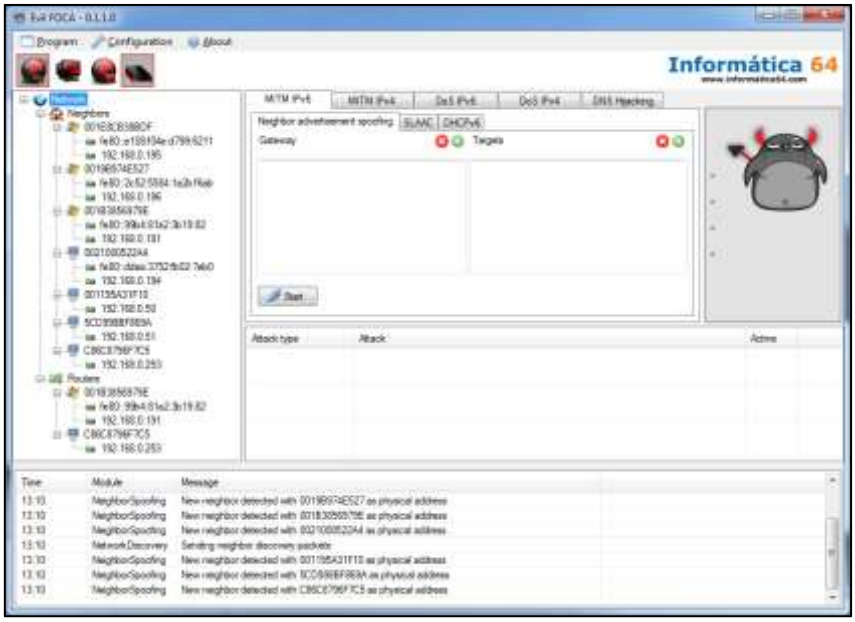
Gráfico 38 Herramienta Wireshark



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

EVIL-FOCA: Es una herramienta similar a ETTERCAP, el funcionamiento de esta aplicación es seleccionar la tarjeta de red en la que se está utilizando como medio de conexión a la red de internet y esta escanea automáticamente los host que están conectados a la red, con esto ya se puede realizar un ataque hombre en el medio para poder capturar todo el tráfico que circula en el internet.

Gráfico 39 Herramienta EVIL-FOCA

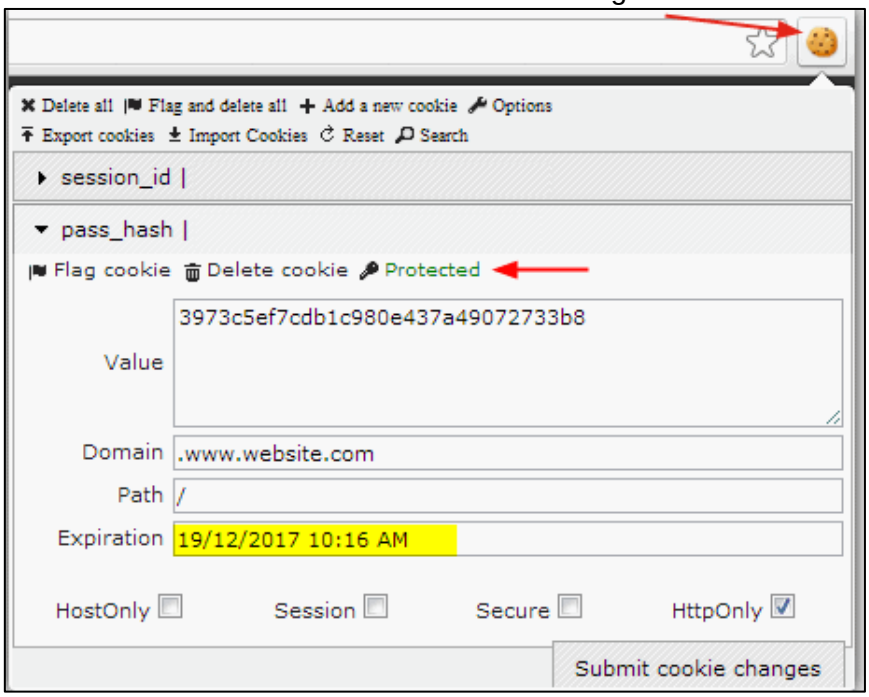


Fuente: https://www.redeszone.net/2015/09/26/la-herramienta-evil-foca-se-vuelve-opensource/

Autor: Rubén Velasco

EDIT THIS COOKIE: El editor de cookie consiste en importar la cookie de sesión de un usuario obtenida por el pirata informático por medio de un ataque hombre en el medio y luego de este proceso se comienza a duplicar la sesión del usuario para tener el acceso a al contenido. Esta herramienta funciona en los navegadores de Google Chrome y Firefox.

Gráfico 40 Editor de Cookies de Google Chrome



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Edit Cookies Firefox: Este complemento pertenece al Navegador Mozilla Firefox, cumple las mismas funciones de importación de cookies.

Gráfico 41 Edit Cookies Firefox

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

De acuerdo a la disponibilidad de estas herramientas indicamos que el proyecto de investigación de muestra la viabilidad técnica para poder ser implementado.

4.1.4 Factibilidad Económica

La facilidad económica dependerá del monto a invertir en el proyecto de investigación, en la cual no se requiere hacer gastos referentes al plan piloto planteado debido a que se utilizaran herramientas de código abierto por lo que estas son de libre acceso sin ningún costo de licencia. El proyecto posee una planificación con un margen de la cantidad que se debe regir. Dentro de la propuesta se consideran 6 herramientas open source para la realización de las pruebas y disponibilidad para su respectiva ejecución por la cual se determina que el proyecto es factible económicamente.

Además en esta etapa se detalla los costos de desarrollo de la propuesta mediante la siguiente tabla:

Tabla 14 Costo de desarrollo del proyecto

Costo de desarrollo del proyecto	
Descripción	**Costo Total**
Servicio de Internet	$ 25
Recursos Varios	$ 100
Laptop HP con procesador Core I3 para la implementación del servidor	$ 400
Laptop HP con procesador Core I3	$ 400
TOTAL	**$ 925.00**

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Mediante la tabla de costos se determina la viabilidad económica del plan piloto es decir que para el desarrollo del proyecto en la cual no se requirieron hacer gastos de licencia de la herramienta Emby ya que es una aplicación Streaming Gratuita.

4.1.5 Factibilidad Legal

La factibilidad legal en el presente proyecto permite especificar que no va a existir vulneración y violación de las leyes vigentes de la República del Ecuador, debido a que solamente se realiza un análisis del método de duplicación de sesión por medio de cookies de un usuario suscriptor para poder establecer los controles que ayuden a disminuir el riesgo de duplicidad de sesión en las plataformas de audio y video bajo demanda por Streaming.

Si se empleara en otras plataformas Streaming bajo demanda se llegaría a un acuerdo de confiabilidad por parte del auditor de seguridad informática y la empresa que presta servicios Streaming. Se entiende que estas compañías tienen conocimiento de todo los temas de seguridad.

4.1.6 Etapas de metodología del proyecto

Para el desarrollo de este proyecto de investigación se aplicara la metodología MAGERIT con sus respectivas etapas.

Siguiendo la terminología de la metodología MAGERIT describimos las siguientes fases dentro de un marco de trabajo suministrado por la misma, para que la toma de decisiones durante el desarrollo del proyecto se tome en consideración sobre los riesgos derivados del uso de tecnologías de la información y comunicación.

A continuación se detallan las siguientes etapas de la metodología MAGERIT en la cual fue aplicada en el capítulo III.

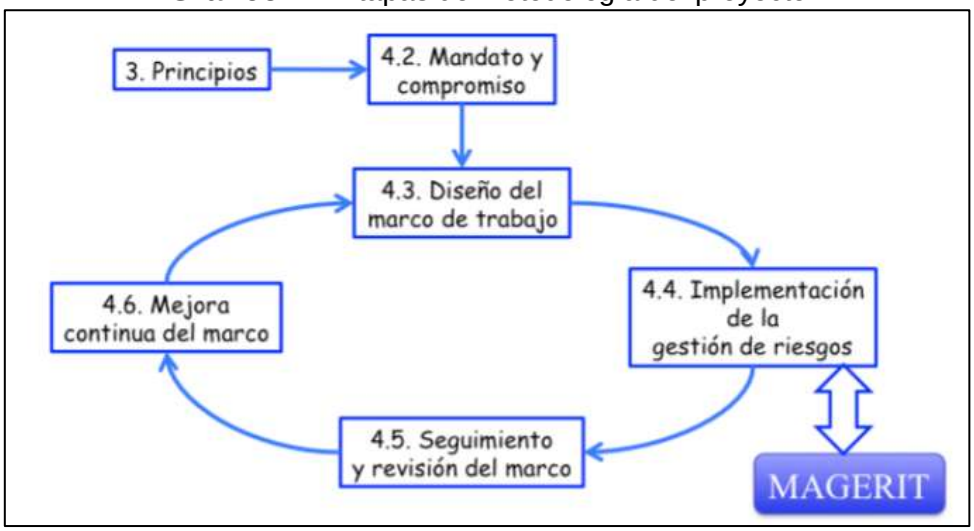
Diseño del marco de trabajo: En esta fase se planifica un proceso de análisis del método de duplicación de sesión por medio de cookies orientado a las plataformas Streaming de audio y video bajo demanda, demostrando en los alcances del proyecto pruebas de duplicidad que determinan la cantidad de amenazas en la cual son asociadas al método a utilizar estableciendo este tipo de duplicidad.

Implementación de la Gestión de Riesgos: Después de establecer el diseño del marco de trabajo en la etapa anterior, se dará el inicio de las pruebas de duplicidad de sesión identificando los riesgos que pueden dar en el momento de la ejecución de las pruebas y se realizara un análisis de los riesgos en la cual pueden ocasionar daños a la información.

Seguimiento y revisión del marco: Una vez realizadas las pruebas de duplicidad de sesión se hará un seguimiento por medio de una guía de buenas prácticas en la cual se dictamina el uso de técnicas que proporcionen niveles de seguridad que ayuden a proteger la confidencialidad de la información en el lado del usuario.

Mejora continua del marco: Con la mejora continua del marco de trabajo propuesto en el inicio de las etapas de metodología del proyecto mencionando en párrafos anteriores se realizara nuevas pruebas de duplicidad de sesión verificando que el uso de la guía de buenas prácticas haya proporcionado los mejores niveles de seguridad para evitar que los atacantes maliciosos logran alterar la confidencialidad de la información.

Gráfico 42 Etapas de metodología del proyecto



Fuente: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WcNKt7Lyh0w

Autores: Consejo de Administración Electrónica de España

4.1.7 Entregables del proyecto

Al finalizar la propuesta orientada al análisis del método de duplicación de sesión se entregara los siguientes documentos:

- Manual de implementación del servidor Streaming de prueba de manera local.
- Reporte de test de penetración referente al análisis del método de duplicidad de sesión por medio de cookies en la plataforma Streaming de prueba.
- Guía de buenas prácticas orientadas al usuario para la protección de su información y evitar ataques de duplicación de sesión por cookies.

4.1.8 Criterios de Validación de la propuesta

En la siguiente tabla se hace el análisis de validación de la propuesta dando valor a las escalas de muy adecuada, adecuada, medianamente adecuada, poco adecuada, nada adecuada.

Tabla 15 Validación del Proyecto

Escalas					
Aspectos a considerar	**Muy Adecuada**	**Adecuada**	**Medianamente Adecuada**	**Poco Adecuada**	**Nada Adecuada**
1. La propuesta es una alternativa para mejorar la seguridad de la información del usuario.	**X**				

2. Fortalecerá la confidencialidad de la información del usuario a través de ejecución de procedimientos**.**	**X**				
3. Dar a conocer los mecanismos de protección que sean de gran ayuda para el usuario.	**X**				

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

4.1.9 Criterios de aceptación del producto

Tabla 16 Criterio de aceptación 1

CRITERIO **ALCANCE**	**Positiva**	**Indiferente**	**Negativa**
Asesorar a los usuarios sobre el buen uso de técnicas que proporcionen navegación anónima logrando evitar que los atacantes procedan a duplicar sesiones protegiendo la información del usuario a través de herramientas tecnológicas.	X		
El resultado de este análisis del método de duplicación de sesión por medio de cookies			

será transmitido a los usuarios de como se les puede duplicar la sesión donde por medio de una guía de buenas prácticas ellos puedan protegerse de este tipo de duplicidad.	X		
Se realizará un estudio completo sobre el análisis en mención detallando las falencias detectadas durante la ejecución de las pruebas de duplicidad de sesión de usuario que son clientes en las plataformas Streaming de audio y video bajo demanda.	X		

Fuente: Datos de la investigación.
Autores: Simón Ballesteros – Francisco Sarmiento

Tabla 17 Criterio de aceptación 2

CRITERIO ALCANCE	Positiva	Indiferente	Negativa
Al final del estudio se entregará un informe referente al análisis realizado en la plataforma Streaming de prueba, siendo posible su demostración en la cual se planteara un ambiente virtual para la realización de las pruebas referente a la duplicidad de sesión.	**X**		
Es necesario citar que para la demostración del estudio realizado donde se utilizara un entorno virtual de acuerdo a las funcionalidades del servidor Streaming audio y video bajo demanda, en esta simulación se podrá observar como realizan la duplicidad de sesión y de qué manera podrían llegar afectar la confidencialidad de la información.	**X**		

Fuente: Datos de la investigación.
Autores: Simón Ballesteros – Francisco Sarmiento

4.2 CONCLUSIONES Y RECOMENDACIONES

4.2.1 Conclusiones

- Como conclusión de este proyecto se llega a culminar que la plataforma Streaming de audio y video bajo demanda de prueba permite realizar una duplicación de sesión de usuario.

- Se demostró en el anexo dos, el acceso ilícito a una sesión de un usuario suscrito, ejecutando un ataque hombre el medio para la sustracción de credenciales de logueo para luego dar uso de ellas y establecer el método de duplicación de sesión por medio de cookies en la plataforma Streaming de prueba.

- En conclusión se dio la necesidad de dar a conocer una guía de buenas prácticas indicándole al usuario que mecanismo de protección él debe utilizar para evitar la duplicidad de sesión del mismo por parte de los atacantes informáticos.

4.2.2 Recomendaciones

- Se recomienda al usuario el uso de navegación anónima en navegadores de internet tales como el Google Chrome que proporciona el modo incognito donde le permite al usuario no almacenar registros de navegación de páginas web.

- Se recomienda la guía de buenas prácticas para el uso de mecanismos de protección para evitar la duplicidad de sesión.

- En una segunda fase de este proyecto de titulación, la implementación de navegadores proporcionara al usuario una conexión segura por medio de una Web VPN que encripta la información generada por el mismo evitando la captura del tráfico por parte de los atacantes.

BIBLIOGRAFIA

[1] J. Luis, B. Larrea, G. R. Kruger, and M. Teórico, “Live Streaming y Video On Demand de contenido académico producido en la PUCP,” 2014.

[2] “Ataques MITM,” 2012.

[3] M. S. Karim, M. Esmaeilzadeh, and P. Sadeghi, “On Reducing Intercept Probability for Unsubscribed Video Layers Using Network Coding,” vol. 21, no. 6, pp. 1385–1388, 2017.

[4] R. G. y D. M. Wilmar Y. Campo(1), Jose L. Arciniegas*(1), “Análisis de Tráfico para un Servicio de Vídeo bajo Demanda sobre Recles HFC usando el Protocolo RTMP,” 2012. [Online]. Available: http://www.scielo.cl/scielo.php?pid=S0718-07642010000600006&script=sci_arttext&tlng=pt.

[5] C. Tx, D. Multimedia, and P. La, “Transmisión En Internet : Streaming De Audio Y Vídeo,” pp. 1–8, 2015.

[6] H. J. Ortega Bernal, “Analisis e implementacion de un sistema video streaming en redes dual stack IPV4/IPV6,” p. 123, 2010.

[7] L. P. ÁLVAREZ, “PhD.Tesis. DISEÑO Y EVALUACIÓN DE SISTEMAS DE ESTIMACIÓN DE ANCHO DE BANDA DISPONIBLE PARA SERVICIOS ADAPTATIVOS DE VÍDEO STREAMING,” 2014.

[8] J. Martin, Y. Fu, N. Wourms, and T. Shaw, “Characterizing Netflix bandwidth consumption,” *2013 IEEE 10th Consum. Commun. Netw. Conf. CCNC 2013*, pp. 230–235, 2013.

[9] V. K. Adhikari, Y. Guo, F. Hao, V. Hilt, and Z. L. Zhang, “A tale of three CDNs: An active measurement study of Hulu and its CDNs,” *Proc. - IEEE INFOCOM*, vol. 23, no. 6, pp. 7–12, 2012.

[10] W. Bellante, R. Vilardi, and D. Rossi, “On Netflix catalog dynamics and caching performance,” *2013 IEEE 18th Int. Work. Comput. Aided Model. Des. Commun. Links Networks, CAMAD 2013*, pp. 89–93, 2013.

[11] N. K. Nandhakumar, A. Binu, and V. Paul, “Non repudiation for internet access by using browser based user authentication mechanism,” *Proc. - 2013 3rd Int.*

Conf. Adv. Comput. Commun. ICACC 2013, pp. 296–299, 2013.

[12] S. Mahmood and Y. Desmedt, “Your Facebook deactivated friend or a cloaked spy,” *2012 IEEE Int. Conf. Pervasive Comput. Commun. Work. PERCOM Work. 2012*, no. March, pp. 367–373, 2012.

[13] E. Aïmeur and D. Schonfeld, “The ultimate invasion of privacy: Identity theft,” *2011 9th Annu. Int. Conf. Privacy, Secur. Trust. PST 2011*, pp. 24–31, 2012.

[14] O. D. Torres, “EVOLUCION Y TENDENCIA DE LA TECNOLOGIA STREAMING EN INTERNET,” 2012.

[15] F. Zhen-ping, B. Kang, and A. M.-C. Standard, “Analysis and Implementation of Streaming Media System Based on RTP and MPEG-4,” no. Iccsnt, pp. 1286–1289, 2015.

[16] I. Mines-t, “Versatile Multiview Layered Video Based on Distributed Source Coding.”

[17] R. Tortosa, J. M. Jimenez, J. R. Diaz, and J. Lloret, “Optimal codec selection algorithm for audio streaming,” *2014 IEEE Globecom Work. GC Wkshps 2014*, pp. 237–242, 2014.

[18] KODI, “KODI,” 2016. [Online]. Available: https://www.xataka.com/basics/kodi-que-es-y-como-funciona.

[19] M. A. Amutio Gómez, “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información,” p. 127, 2012.

[20] L. Polytechnic, “Detecting Third-Party User Trackers with Cookie Files,” pp. 78–80, 2016.

[21] Netflix, “Declaracion de Privacidad,” *01/01/2017*, 2017. [Online]. Available: https://help.netflix.com/legal/privacy.

[22] “Uso de Cookies,” pp. 788–789.

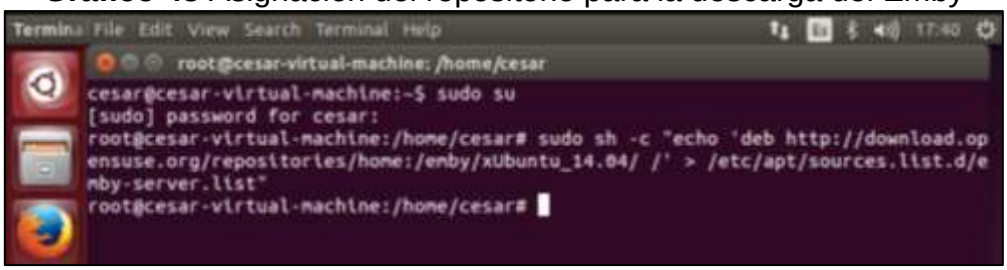
[23] A todo curso, “Las cookies, ventajas y desventajas.” [Online]. Available: https://www.atodocurso.com/noticias/las-cookies-ventajas-y-desventajas.

ANEXOS

ANEXO 1: MANUAL DE IMPLEMENTACIÓN DEL EMBY

Para iniciar la instalación de Emby-Media-Server se utilizó el sistema operativo Ubuntu con su versión 14.04, en donde se aplicó el comando sudo sh –c para agregar el link del repositorio del paquete Emby al sistema operativo como se muestra en el Gráfico 43.

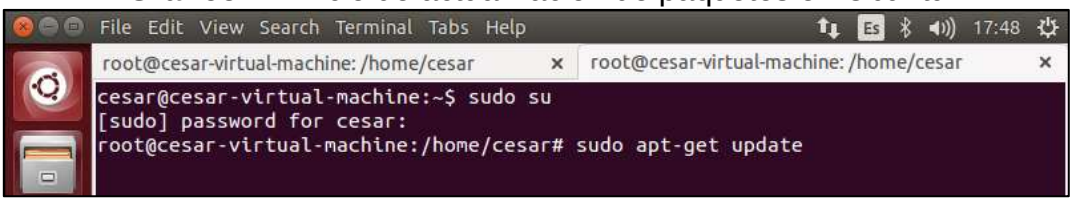
Gráfico 43 Asignación del repositorio para la descarga del Emby



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

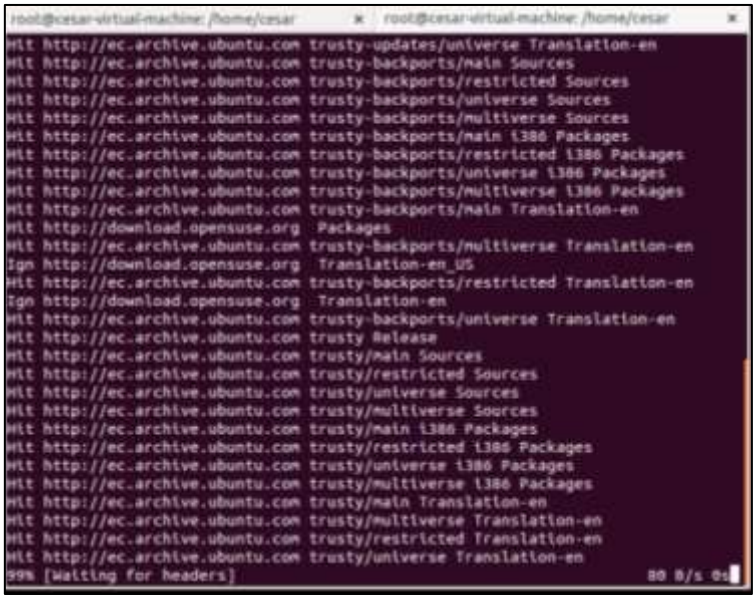
Una vez realizado el primero paso de la instalación de Emby-Media-Server se procede a actualizar los paquetes del sistema operativo Ubuntu como se muestra en el Gráfico 44 y 45.

Gráfico 44 Inicio de actualización de paquetes en Ubuntu



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

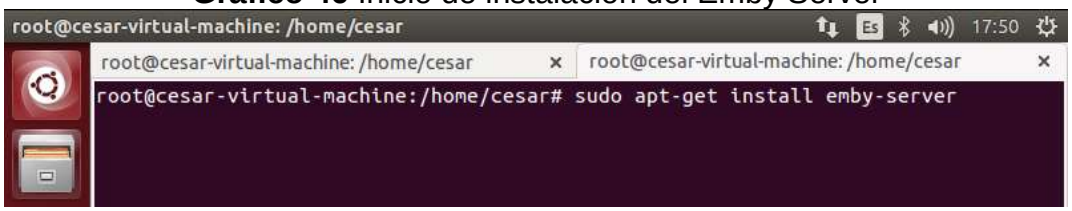
Gráfico 45 Finalización de actualización



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

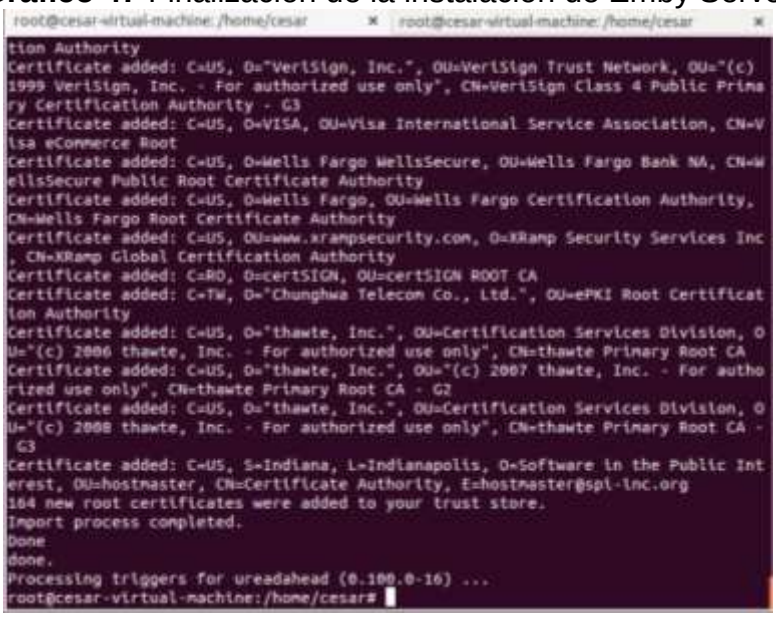
Después de haber realizado el proceso de actualización de paquetes en Ubuntu se inicia la instalación del servidor Emby como se indica en el Gráfico 46 y 47.

Gráfico 46 Inicio de instalación del Emby Server



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 47 Finalización de la instalación de Emby Server



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Una vez terminado el proceso de instalación de Emby-Media-Server, se comienza a instalar el servidor SSH en modo cliente como se muestra en el Gráfico 48 en la cual lo utilizaremos para la transferencia de archivo multimedia por medio de la herramienta WinSCP.

Gráfico 48 Instalación del servicio SSH en modo cliente

```
root@cesar-virtual-machine: /home/cesar    root@cesar-virtual-machine: /home/cesar
root@cesar-virtual-machine:/home/cesar# sudo apt-get install openssh-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  libpam-ssh keychain monkeysphere
The following packages will be upgraded:
  openssh-client
1 upgraded, 0 newly installed, 0 to remove and 655 not upgraded.
Need to get 576 kB of archives.
After this operation, 1.024 B of additional disk space will be used.
Get:1 http://ec.archive.ubuntu.com/ubuntu/ trusty-updates/main openssh-client i3
86 1:6.6p1-2ubuntu2.8 [576 kB]
Fetched 576 kB in 2s (218 kB/s)
(Reading database ... 167483 files and directories currently installed.)
Preparing to unpack .../openssh-client_1%3a6.6p1-2ubuntu2.8_i386.deb ...
Unpacking openssh-client (1:6.6p1-2ubuntu2.8) over (1:6.6p1-2ubuntu2) ...
Processing triggers for man-db (2.6.7.1-1) ...
Setting up openssh-client (1:6.6p1-2ubuntu2.8) ...
root@cesar-virtual-machine:/home/cesar#
```

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

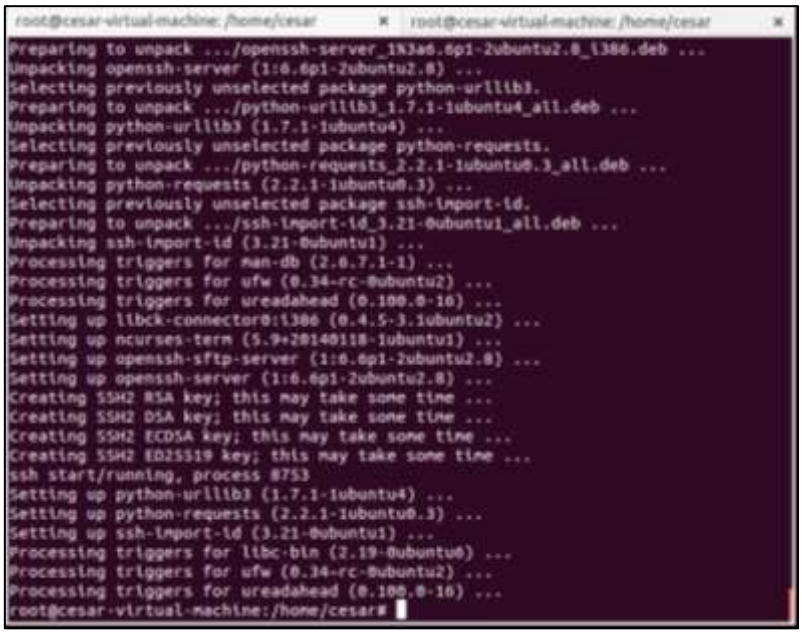
Después de instalar el servicio SSH en modo cliente, se comienza a instalar el servidor SSH Servidor como se muestra en el Gráfico 49 y 50 para el acceso desde una herramienta externa.

Gráfico 49 Instalación del servicio SSH en modo server

```
root@cesar-virtual-machine: /home/cesar    root@cesar-virtual-machine: /home/cesar
root@cesar-virtual-machine:/home/cesar# sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libck-connector0 ncurses-term openssh-sftp-server python-requests
  python-urllib3 ssh-import-id
Suggested packages:
  rssh molly-guard monkeysphere
The following NEW packages will be installed:
  libck-connector0 ncurses-term openssh-server openssh-sftp-server
  python-requests python-urllib3 ssh-import-id
0 upgraded, 7 newly installed, 0 to remove and 655 not upgraded.
Need to get 706 kB of archives.
After this operation, 3.902 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 50 Proceso de instalación del servicio SSH



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

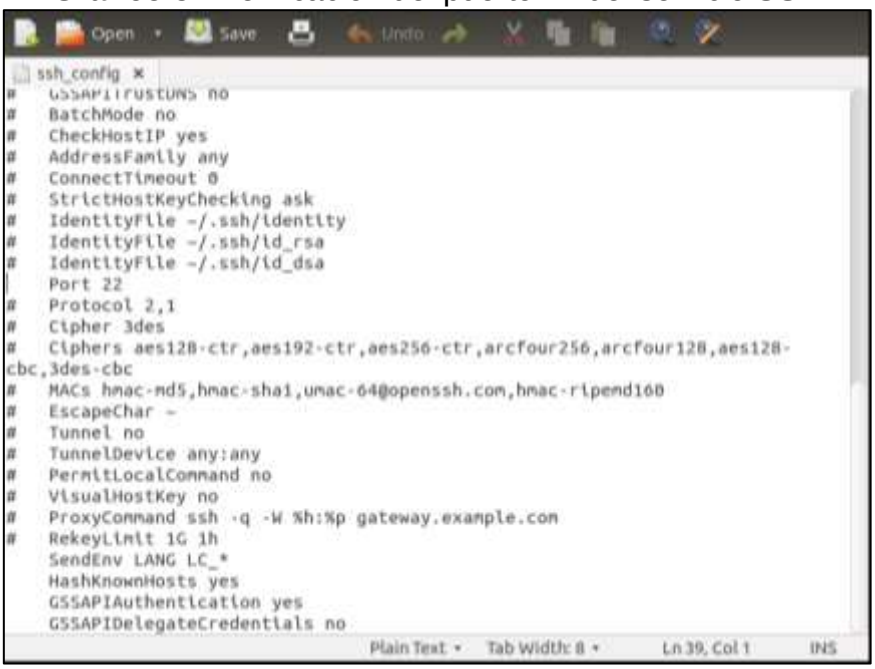
Una vez instalado el servicio SSH se procede a la configuración del archivo ssh_config por medio del comando Gedit que se encuentra ubicado en la ruta /etc/ssh.

Gráfico 51 Acceso al archivo ssh_config

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Una vez abierto el archivo ssh_config se ubica en la línea 39, se quita el numeral de dicha línea, habilitando el puerto 22 como se muestra en el Gráfico 52.

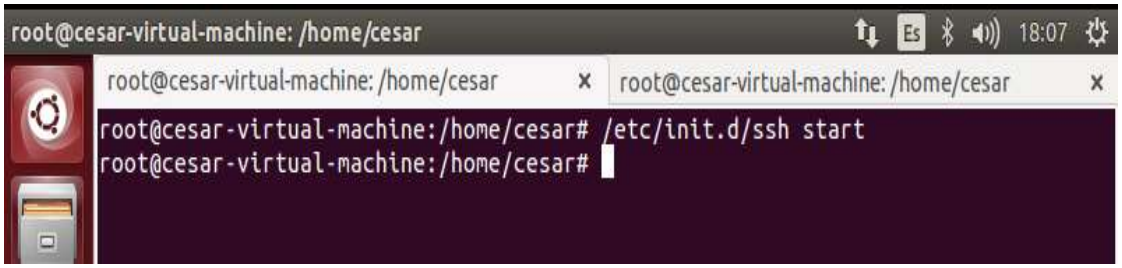
Gráfico 52 Verificación del puerto 22 del servicio SSH



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Una vez configurado el archivo ssh_config se procede a levantar el servicio de ssh como se indica el Gráfico 53.

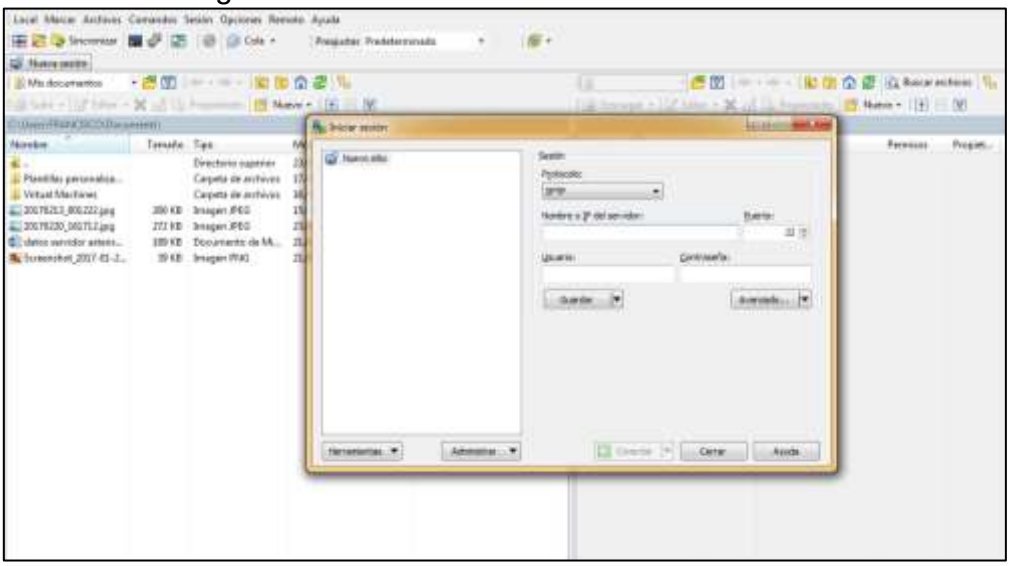
Gráfico 53 Levantamiento del servicio SSH



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Una vez levantado el servicio SSH se procede a loguear con las credenciales de Ubuntu en la herramienta WinSCP para la transferencia de contenido multimedia como se indica en el Gráfico 54.

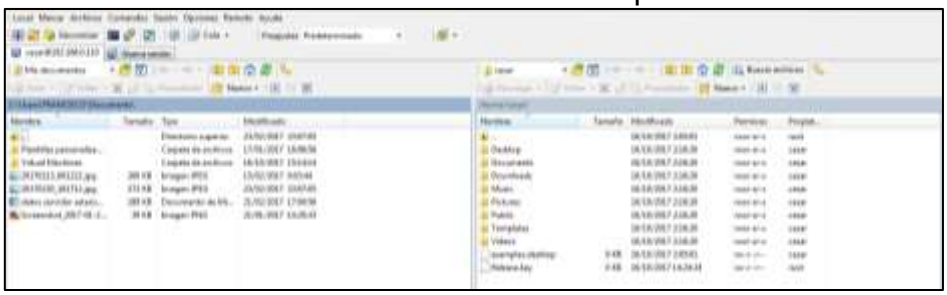
Gráfico 54 Logueo de las credenciales de Ubuntu mediante WinSCP



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Una vez establecido él logueo con las credenciales de Ubuntu con la herramienta WinSCP se procede a transferir el contenido multimedia desde el cliente al servidor.

Gráfico 55 Acceso al servidor de Ubuntu por medio WinSCP



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

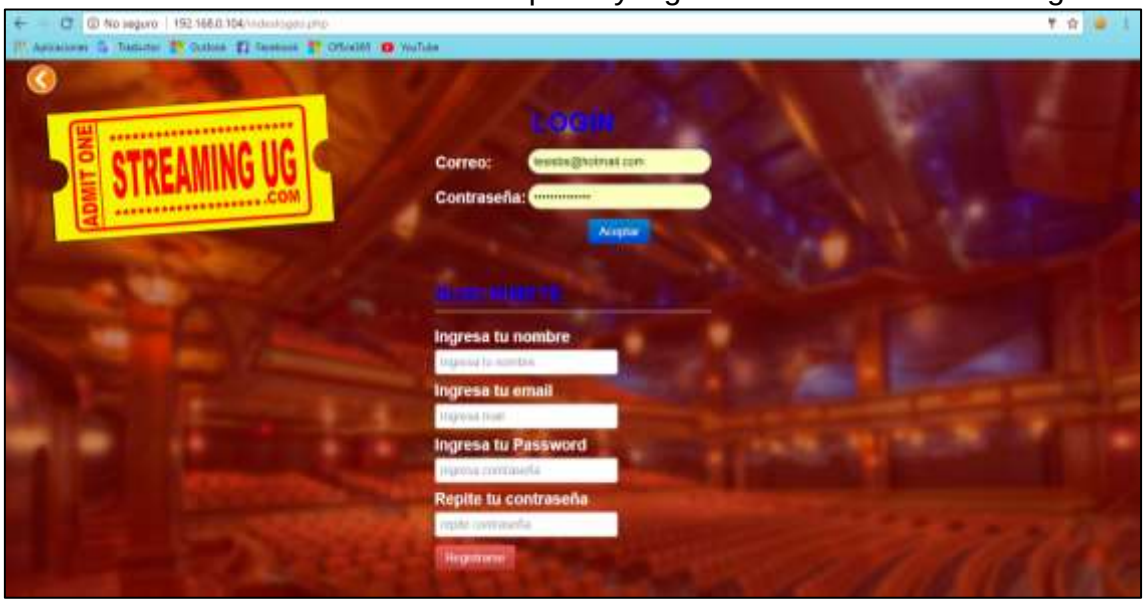
Para la creación del ambiente de prueba se desarrolló una interfaz web local como se muestra en el Gráfico 56, para la respectiva simulación de la suscripción de usuario.

Gráfico 56 Portada del inicio de la interfaz web del servidor Streaming

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

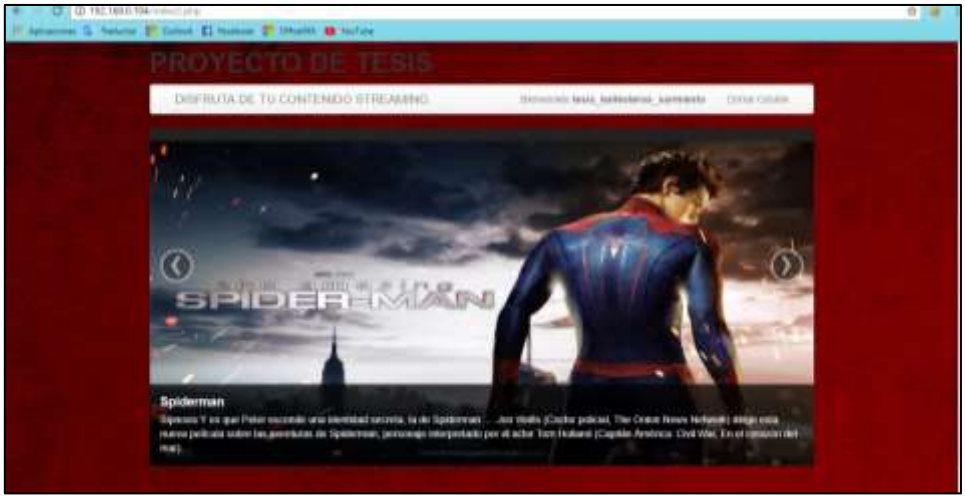
Una vez dado click en el botón entrar, se redirige al formulario de suscripción y logueo de credenciales como se indica el Gráfico 57, para iniciar el acceso al contenido multimedia almacenado en el servidor Streaming de prueba como se indica también el Gráfico 59 donde se muestra la sesión del usuario suscrito.

Gráfico 57 Formulario de suscripción y logueo del servidor Streaming



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 58 Sesión del usuario suscrito



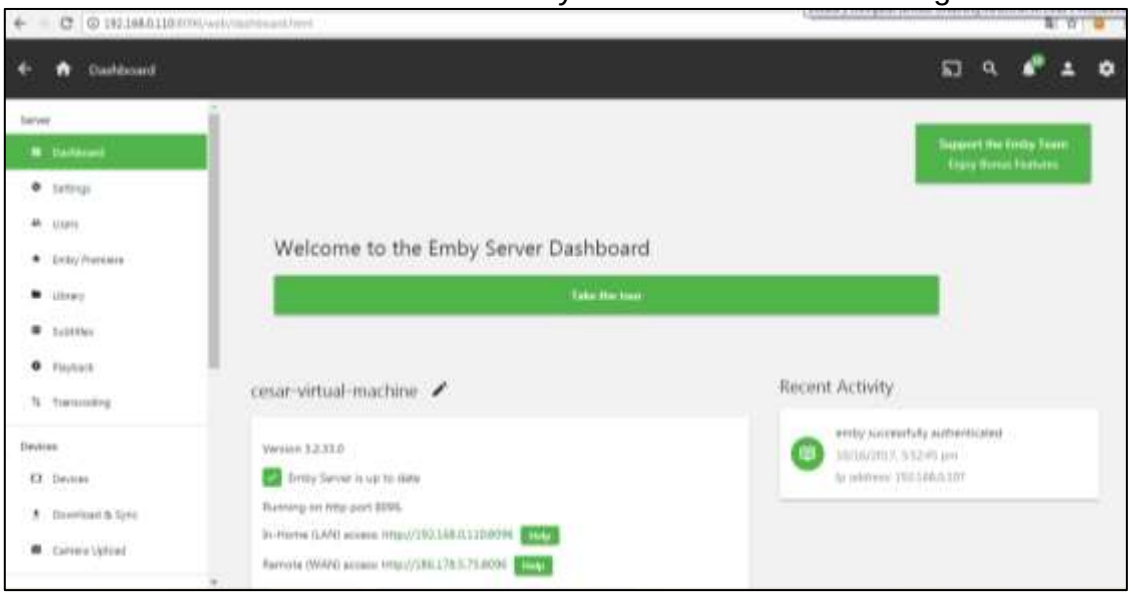
Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Una vez dado click en el enlace de disfruta tu contenido Streaming, se tendrá el acceso dashboard de Emby donde se podrá acceder al contenido multimedia como se indica el Gráfico 60.

Gráfico 59 Acceso al contenido Streaming

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 60 Dashboard de Emby-Media-Server en el navegador



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

ANEXO 2: TEST DE PENETRACIÓN

¿Qué es un test de penetración?

También es llamado como pentest, es un método de valorar y evaluar la seguridad de los equipos y las redes de comunicación simulando un ataque informático a un servidor o red desde una fuente externa o interna, consiste en un análisis activo de todos los dispositivos de la red para detectar cualquier vulnerabilidad o una falla en la configuración de los servidores o los equipos de seguridad.

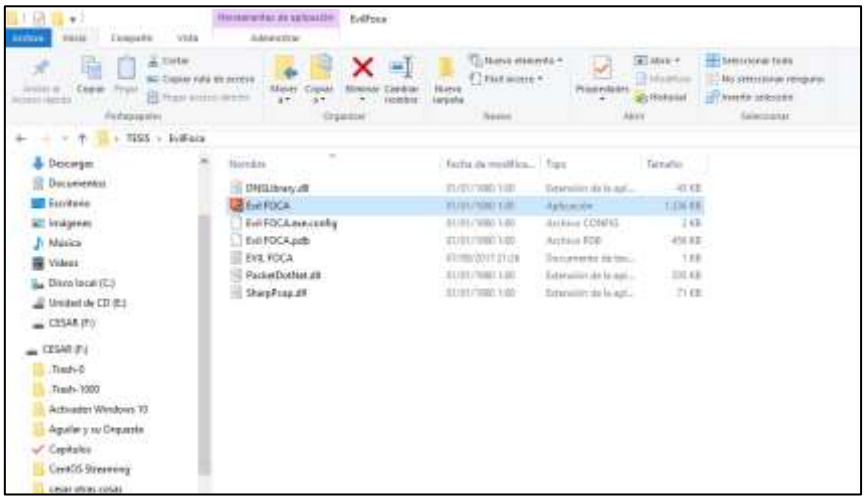
Herramientas a utilizar para realizar el pentest.

- Software: Evil foca.
- Wireshark.

EJECUTAR LOS SIGUIENTES PASOS:

- Desde el ordenador atacante, se inicia el software de ataque: Evil Foca.

Gráfico 61 Inicio de Evil Foca



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

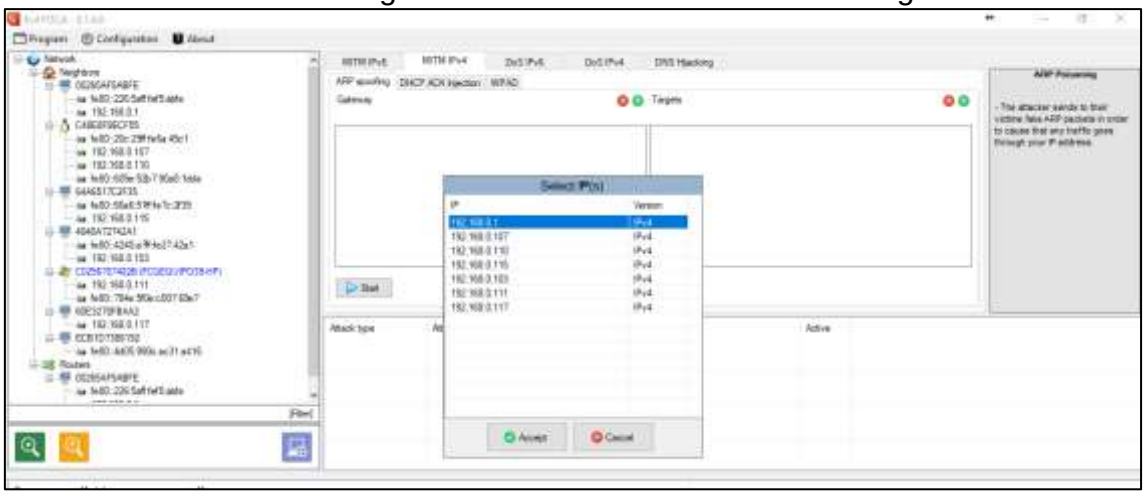
- Seleccionar la opción MITM IPV4 ataque (Man-in-the-middle).

Gráfico 62 MITM IPV4 ataque (Man-in-the-middle).

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Dar clic, en el botón + de color verde del primer target, se abrirá una ventana de direcciones IP, donde seleccionaremos la Ip del router de la red, 192.168.0.1/24, dar clic en aceptar.

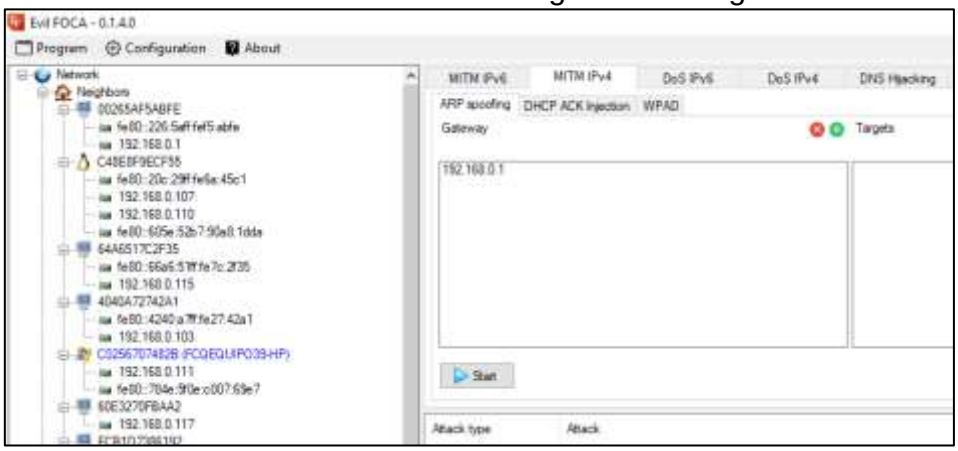
Gráfico 63 Asignación de direcciones IPs en el Target 1



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- La dirección del router se ubica en el target 1.

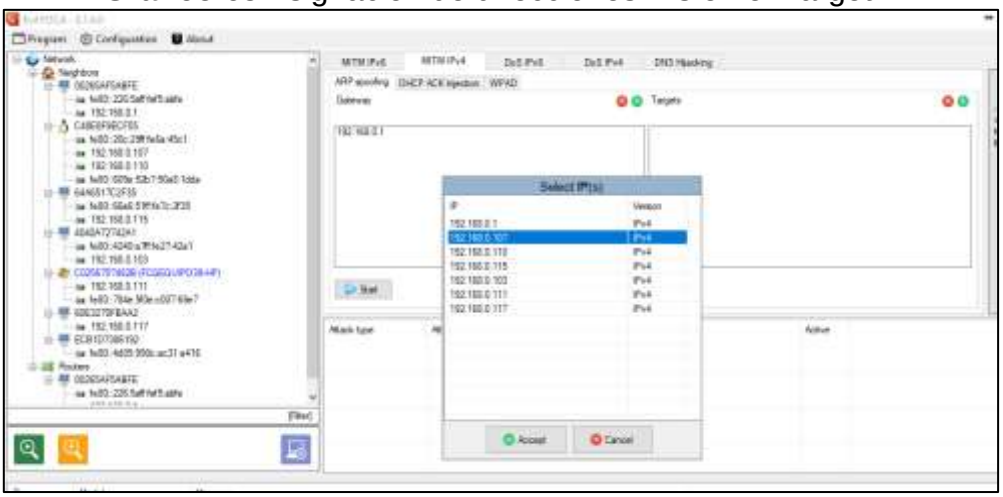
Gráfico 64 Dirección IP asignada al Target 1



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Dar clic, en el botón + de color verde del segundo target, se escogerá la dirección IP de la víctima 192.168.0.107/24, poner en aceptar para dar inicio al ataque MITM.

Gráfico 65 Asignación de direcciones IPs en el Target 2



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

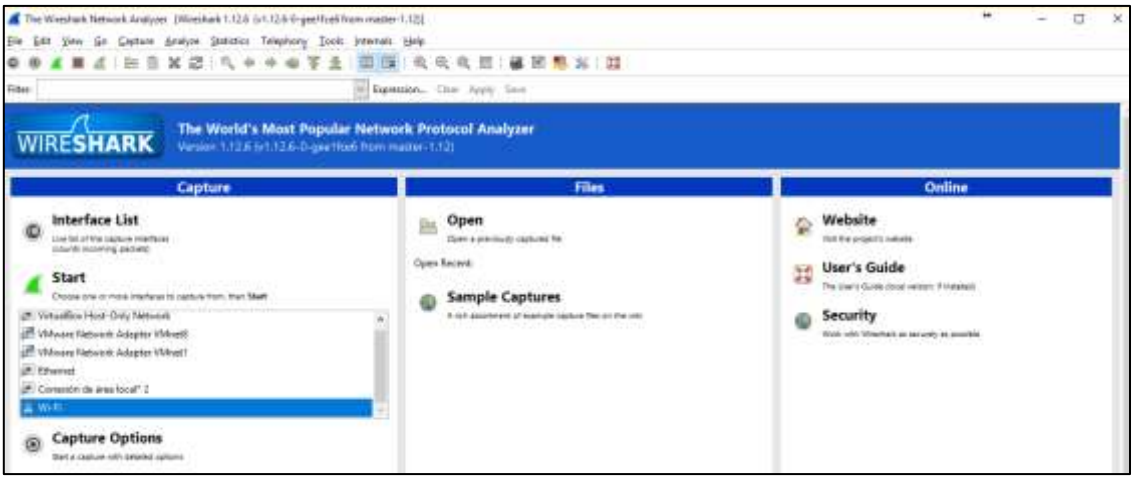
- Una vez que la dirección IP del router y la IP de la víctima estén ubicadas correctamente en los targets, se da click en Start para dar inicio al ataque.

Gráfico 66 Inicio del Ataque

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Dirigirse al analizador de trafico WIRESHARK, seleccionar la tarjeta de red inalámbrica, dar clic en Start para iniciar el análisis del tráfico.

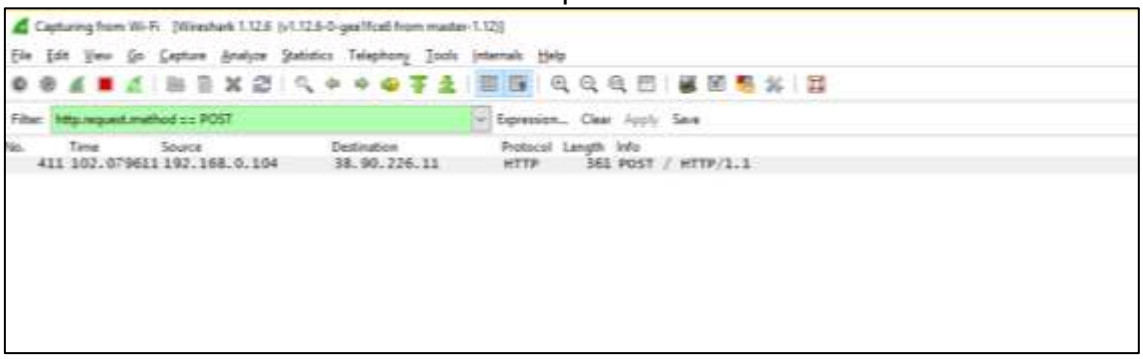
Gráfico 67 Inicio del Sniffer



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Una vez que el analizador de trafico Wireshark esté en marcha, se aplicara el filtro de captura **http.resquest.method==POST** donde este ayudara a la sustracción de las credenciales cuando el usuario se autentique en la interfaz web de la plataforma Streaming.

Gráfico 68 Captura del trafico



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Esperamos que el usuario se autentique desde la maquina victima

Gráfico 69 Espera de autenticación

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Una vez que el usuario se haya autenticado, se verifica en la parte inferior izquierda del Wireshark las credenciales capturadas del usuario logueado en el servidor Streaming.

Gráfico 70 Muestra de credenciales Capturadas

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Credenciales capturadas:
Correo: tesisbs@hotmail.com
Contraseña: networking2017

- Una vez capturadas las credenciales, hacer uso de las mismas desde la maquina atacante, para realizar el proceso del método de duplicación de sesión por medio de cookies.

DUPLICACION DE SESION POR MEDIO DE COOKIES EN GOOGLE CHROME.

Gráfico 71 Ingresar al dominio del servidor Streaming http://192.168.0.104/INI.html

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Autenticarse con las credenciales sustraídas durante el ataque.

Gráfico 72 Logueo de credenciales

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 73 Mensaje de éxito de autenticación

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

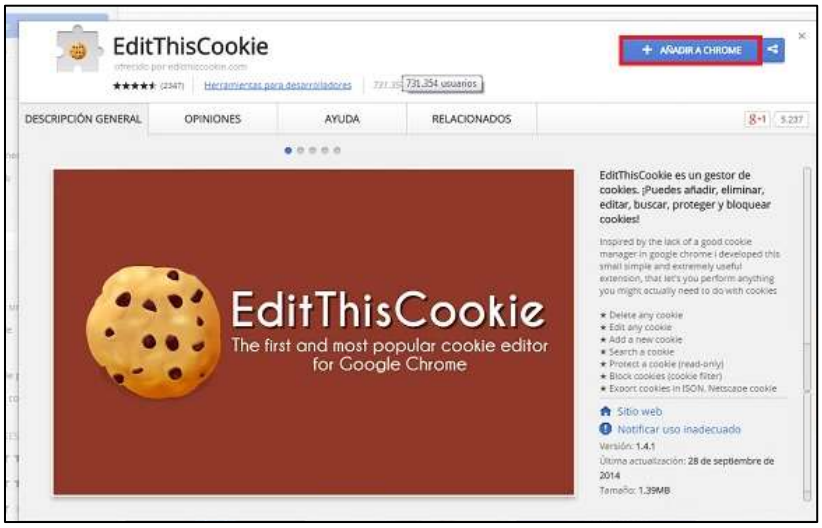
- Ingresar a la interfaz del servidor Streaming.

Gráfico 74 Acceso al servidor Streaming

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Instalar la extensión EditThisCookie en el navegador.

Gráfico 75 Instalación de la Extensión Edit-Cookie



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

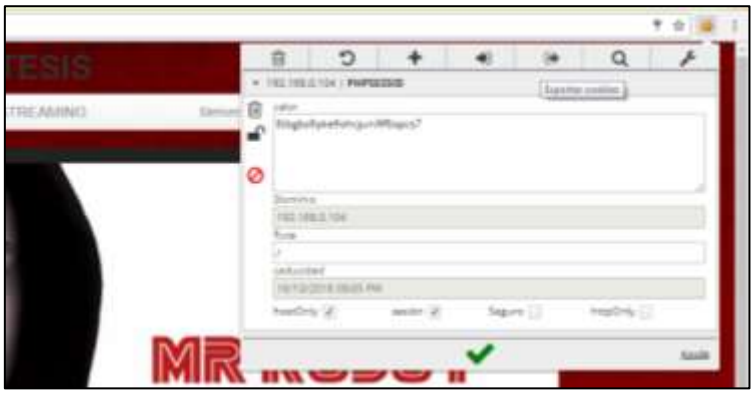
Gráfico 76 Selección de la cookie

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

EXTRACCION DE LA COOKIE DE SESION

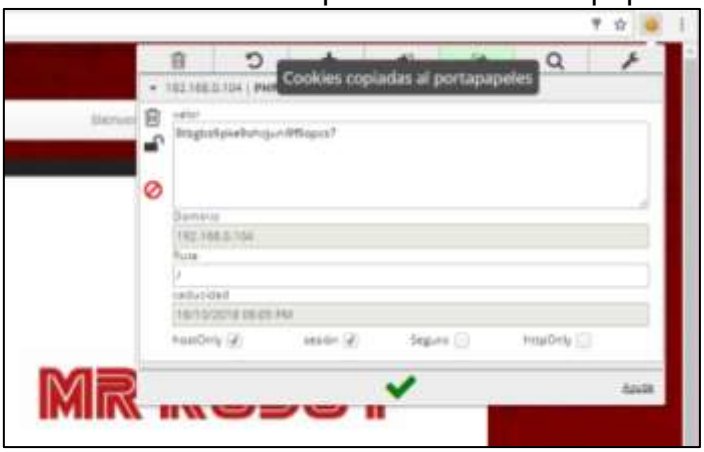
- Clic en el icono de la extensión EditThiscookie, seleccionar la opción de exportar la cookie de sesión para que sea almacena en el portapapeles y luego pegada en un documento de texto.

Gráfico 77 Proceso de extracción de cookies



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 78 Cookies copiadas en los cortapapeles



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 79 Cookie almacenada en bloc de notas

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

DUPLICACION DE SESION EN OTRO ORDENADOR

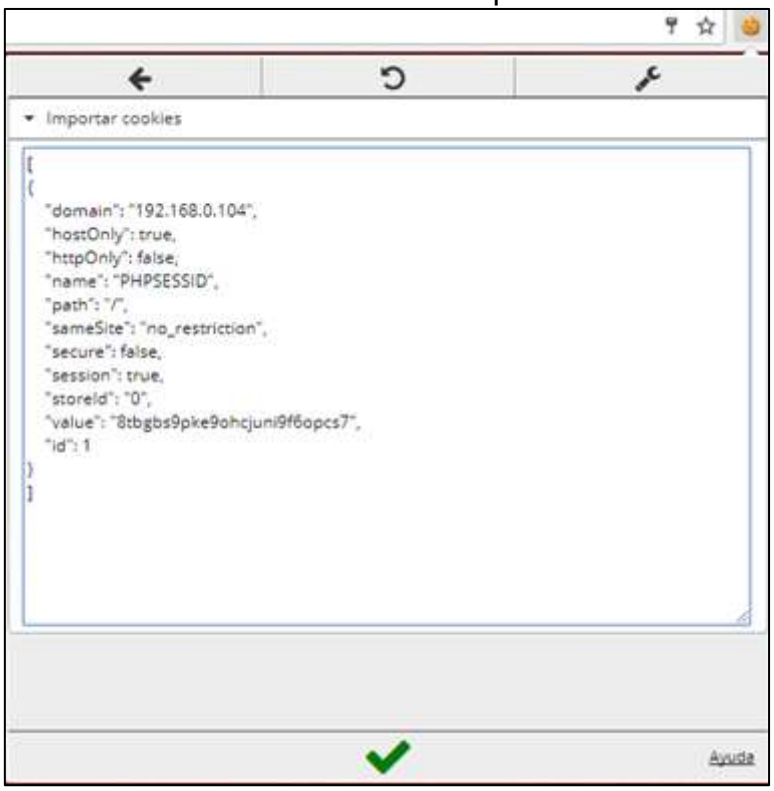
- Se realiza la inyección de la cookie obtenida, dar clic en el icono de la extensión EditThisCookie y poner en la opción de importar cookies.

Gráfico 80 Proceso de Importación de Cookie

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Pegar el código de la cookie anteriormente sustraída en el cuadro que se despliega, luego dar clic en el visto de color verde.

Gráfico 81 Cookie Importada



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

21.- ingresar al dominio de la sesión http://192.168.0.104/index2.php, dar Enter para que la duplicación se efectúe.

Gráfico 82 Acceso del servidor Streaming por medio de Google Chrone

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

<u>DUPLICACION DE SESION EN MOZILLA FIREFOX.</u>

Gráfico 83 Instalar el complemento de Firefox: **Edit Cookies.**

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

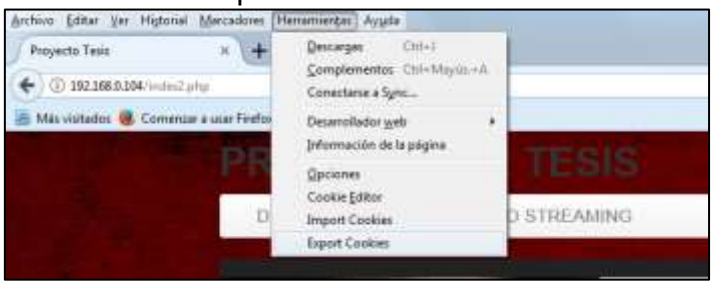
- Autenticarse con las credenciales obtenidas durante el ataque, ingresar a la interfaz del servidor Streaming.

Gráfico 84 Ingreso de credenciales por medio de Firefox

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Extracción de la cookie, dar clic en herramientas y escoger la opción: Export Cookies.

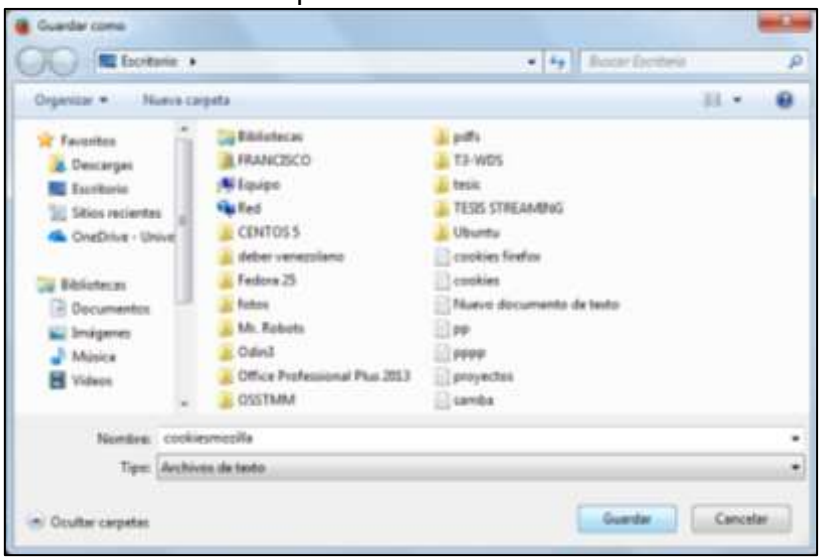
Gráfico 85 Exportación de cookies en Firefox



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Guardar la cookie extraída.

Gráfico 86 Ruta para almacenar la cookie en Firefox

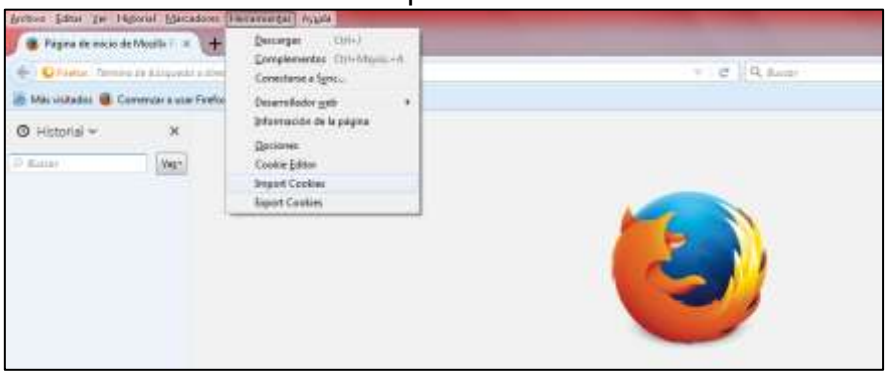


Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

DUPLICACION DE SESION EN OTRO ORDENADOR

- Dar clic en la opción herramientas, importar cookies.

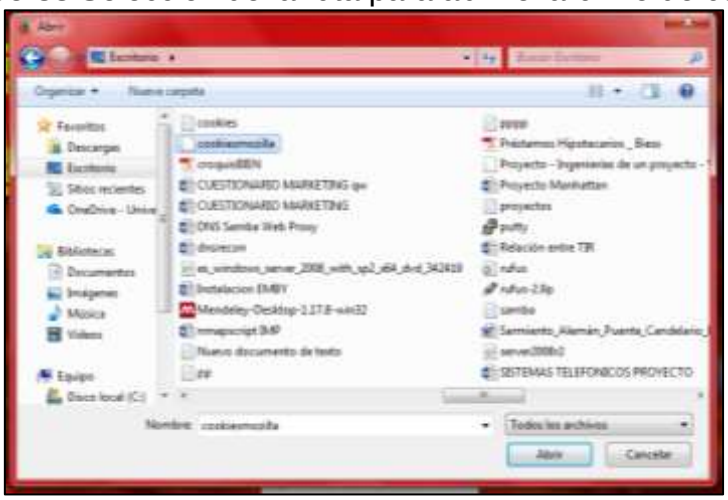
Gráfico 87 Proceso de Importación de cookies en Firefox



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Buscar la ruta del fichero.

Gráfico 88 Selección de la ruta para abrir el archivo de cookies



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 89 Aceptación de la cookie

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Se obtiene exitosamente la duplicación de sesión

Gráfico 90 Acceso al servidor Streaming desde Firefox

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

ANEXO 3: GUÍA DE BUENAS PRÁCTICAS ORIENTADAS AL USUARIO, PARA LA PROTECCIÓN DE SU INFORMACIÓN Y EVITAR ATAQUES DE DUPLICACIÓN DE SESIÓN POR COOKIES.

AUTORES:

Simón Cesar Ballesteros Correa.

Francisco Xavier Sarmiento Ronquillo

Objetivo General

Dar a conocer al usuario mecanismos de protección de la información, para evitar el robo de sesiones por cookies.

Objetivos Específicos

- Facilitar conocimientos al usuario sobre la información que almacenan las cookies.
- Proporcionar procedimientos sobre el buen uso del navegador Google Chrome y Mozilla Firefox, referente a la eliminación de información almacenada en los mismos.
- Dar a conocer el uso de la navegación incógnita en navegadores de internet.

¿QUE SON LAS COOKIES?

Las cookies son datos que recibe un navegador web junto con una página y que se almacenan en el ordenador del usuario.

Las cookies se utilizan para guardar las opciones de diseño que se realiza en una plataforma que puede contener: colores, imágenes, opciones, sonidos, etc. Además son aptos de recordar información de hábitos sobre la navegación que ha realizado el usuario, tienen la capacidad de memorizar las contraseñas cuando se inicia sesión en una web, para que, al acceder de nuevo a la página, no se tenga que volver a digitar el usuario y contraseña y tener así ya el dato de los gustos de navegación.[23]

El propósito vital de una cookie es reconocer al usuario almacenando su historial de actividad en un sitio web específico, de manera que se le pueda ofrecer el contenido más apropiado según sus hábitos.

Esto quiere decir que cada vez que se visita una página web por primera vez, se guarda una cookie en el navegador con un poco de información. Luego, cuando se visita nuevamente la misma página, el servidor pide la misma cookie para arreglar la configuración del sitio y hacer la visita del usuario tan personalizada como sea posible.

La especificación general de las cookies fue desarrollada por Netscape en el año de 1994 y hoy en día aún se puede encontrar este documento en la web, la última especificación de las cookies la encontramos en el documento RFC 6265 state management mechanism de abril del 2015

Ventajas de tener alojadas las cookies en tu navegador

Los ficheros o cookies proporcionan una navegación rápida, sencilla y personalizada, evitando que el usuario no vuelva a digitar las páginas que visita frecuentemente en vista de que él no se acuerde de dichas direcciones Web.[23]

Estas cookies son utilizadas para la realización de compras online. Si existe algún problema que impide terminar el proceso de transacción en línea, las cookies propias ayudarán a recordar los productos que el usuario tenía en su carrito de compras evitando que el usuario tenga que buscar los productos nuevamente.[23]

Desventajas de tener alojadas las cookies en tu navegador

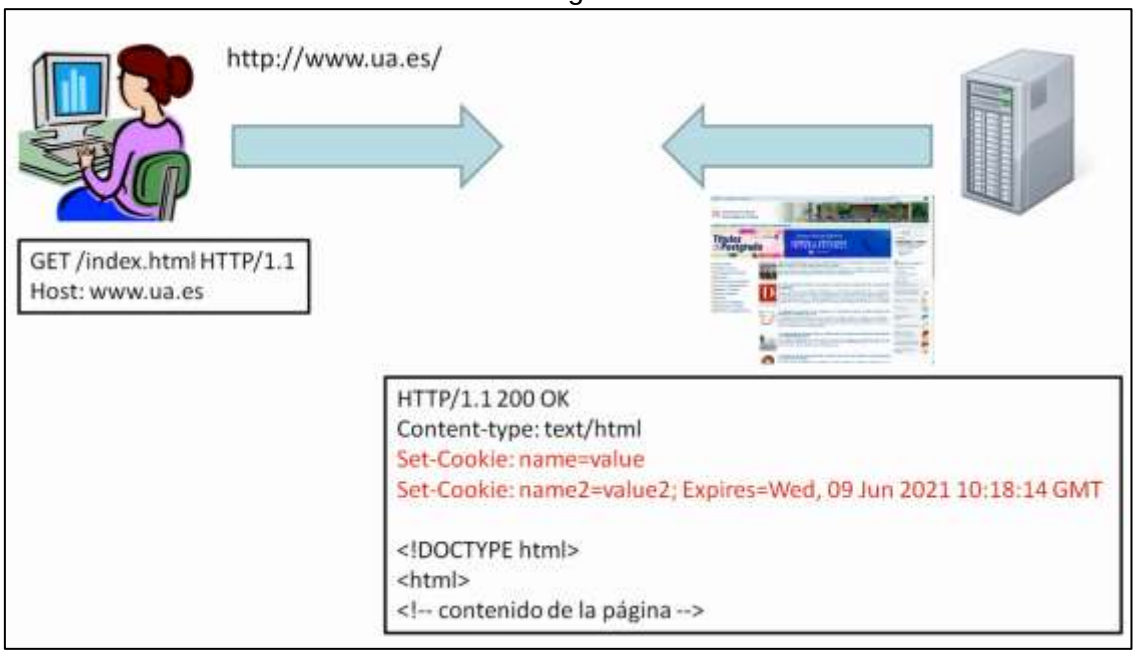
El problema principal de las cookies reside en que poseen la capacidad de almacenar cualquier tipo de información de carácter sensible, en la cual proteger la privacidad del usuario se vuelve una tarea compleja en vista que ellos no poseen los conocimientos sobre la navegación anónima. Esto conlleva que esa información confidencial que almacenan pueda ser accedida por piratas informáticos con la finalidad de causar daño a su objetivo o en beneficio propio.[23]

Estas cookies son creadas para detectar las páginas que visitan los usuarios durante la navegación por Internet, de este modo, aunque no tengan los datos personales, gracias a las pautas de navegación se puede deducir que la información de los usuarios se encuentra protegida.[23]

Como se envían las Cookies mediante el protocolo Http entre el cliente Y el servidor.

En primer lugar cuando un usuario quiere visitar una página web como por ejemplo **www.ua.es** el navegador se conecta al servidor web y la envía una petición http, luego el servidor web responde al navegador enviando una respuesta http que contiene la página solicitada en una seria de líneas pidiendo al navegador que almacene dos cookies.

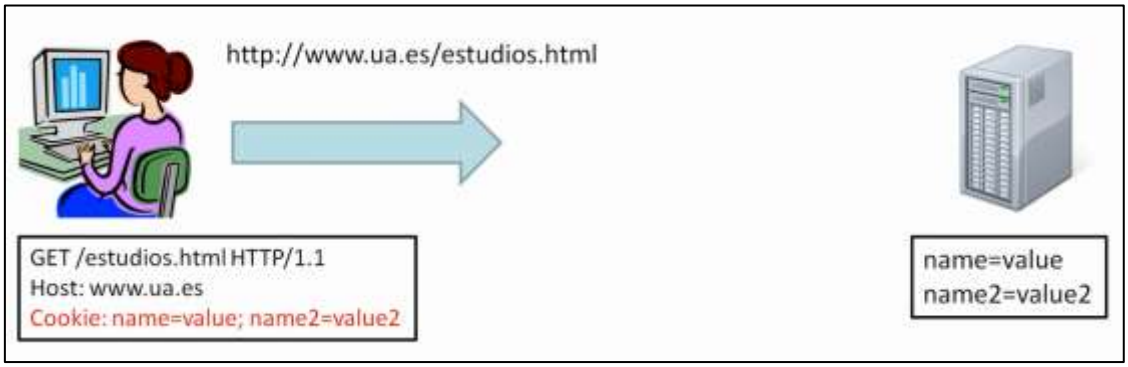
Gráfico 91 Origen de la cookie



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Cuando el usuario vuelve a visitar una página del mismo sitio web la petición que envía el navegador al servidor web incluirá las cookies que se hayan almacenado previamente, el navegador únicamente envía la pareja **nombre, valor,** el resto de atributos de la cookie no se envían, al recibir la petición el servidor web podrá leer las cookies y las podrá utilizar para crear la siguiente respuesta.

Gráfico 92 envío de cookies almacenadas



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Atributos de las Cookies.

Según la última especificación las cookies se componen de los siguientes atributos:

- **Una pareja nombre/valor:** es la que da la información de la cookie
- **Un dominio:** indica en que dominio se puede emplear la cookies, o a que dominio pertenece la cookie.
- **Una ruta:** limita el uso de la cookie a páginas que se encuentren en dicha ruta.
- **Fecha de caducidad o máxima edad:** indica hasta cuando la cookie es válida, es decir nos muestra la fecha de caducidad.
- **Una marca de solo conexión segura:** esto exige que la cookie sea enviada mediante un protocolo de encriptación.
- **Una marca de solo HTTP:** limita el uso de la cookie al protocolo HTTP.

<u>Como se representan los atributos de una Cookie en un mensaje Http.</u>

Aquí tenemos una directiva http **Set-Cookie** que es enviada por el servidor el cual ordena al navegador web que almacene esta cookie.

Gráfico 93 Cookie en un mensaje Http

```
Set-Cookie: ID=Gehwvyyb%20pnchyyb; Domain=docs.foo.com; Path=/privado; Expires=Wed, 13-Jan-2021 22:23:01 GMT; Secure; HttpOnly
```

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

En más detalle:

Gráfico 94 Cookie en un mensaje Http

```
Set-Cookie:  ID=Gehwvyyb%20pnchyyb;
             Domain=docs.foo.com;
             Path=/privado;
             Expires=Wed, 13-Jan-2021 22:23:01 GMT;
             Secure;
             HttpOnly
```

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Atributos encontrados en la directiva http Set-Cookie

- Se encontró la pareja **Nombre/valor.**
- Se encontró el atributo **Domain,** el cual indica que esta cookie solo se puede utilizar en el dominio indicado.
- Se encontró el atributo **Path,** el cual limita el uso de esta cookie a páginas que se encuentren dentro del directorio o ruta **/privado.**
- Se encontró el atributo **Expires**, el cual indica que esta cookie caducara el 13 de enero del año 2021 a las 22:23:01.
- Se encontró el atributo **Secure,** el cual indica que esta cookie solo se tiene que ser enviada a través de una comunicación segura y encriptada como puede ser https.
- Por último el atributo **HttpOnly,** indica que esta cookie solo es accesible a través del protocolo http y no a través de otros métodos como puede ser Java Script.

Podemos ver que los dos últimos atributos **Secure, HttpOnly** no llevan valores.

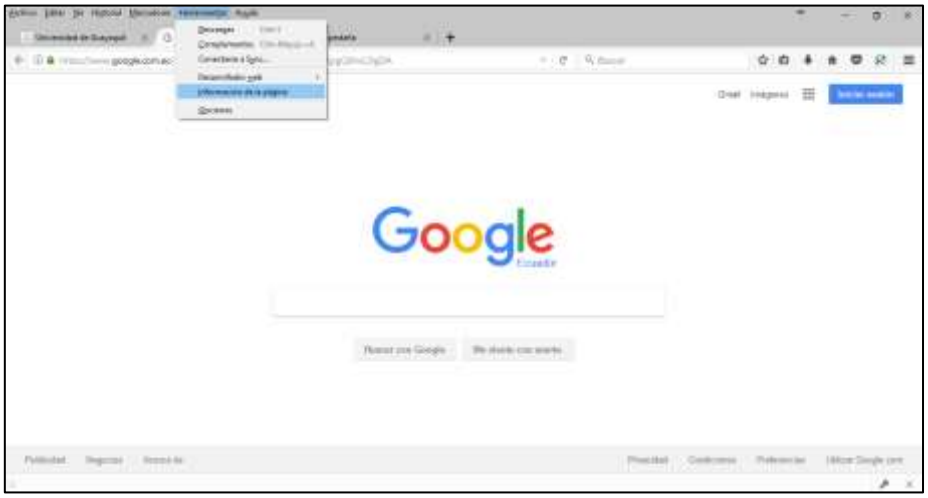
Hoy en día aunque no se tome en consideración la mayoría de los sitios web emplean cookies que almacenan todo tipo de información en los ordenadores.

Los navegadores modernos permiten visualizar las cookies que se emplean en un sitio web y si se quiere también permiten borrarlas, por ejemplo el buscador google emplea algunas cookies para almacenar información sobre las búsquedas que hayamos realizado y para almacenar las preferencias del usuario, sobre el idioma de búsqueda o el número de resultados a mostrar.

VISUALIZACION DE LAS COOKIES ALOJADAS EN EL NAVEGADOR MOZZILLA FIREFOX.

- Se selecciona en el menú la opción de Herramientas, clic en información de la página.

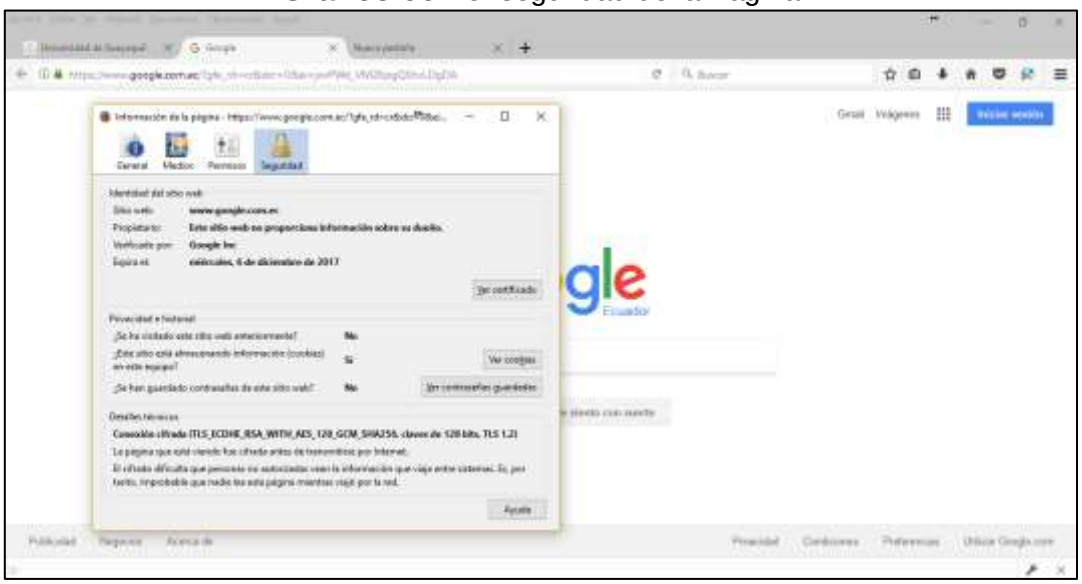
Gráfico 95 Visualización de las Cookies Mozilla Firefox



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- En la ventana que parece, ubicarse en la pestaña seguridad.

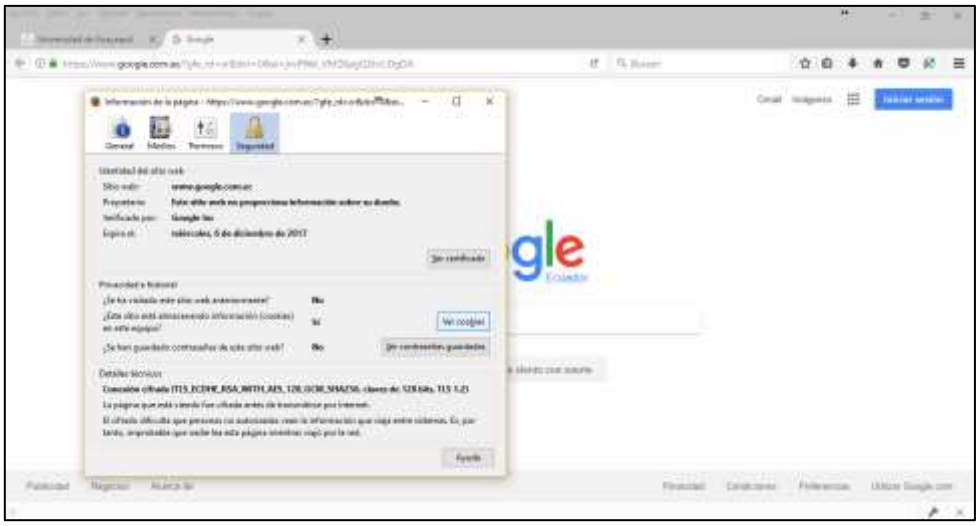
Gráfico 96 Ver seguridad de la Pagina



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Dar clic en el botón ver Cookies.

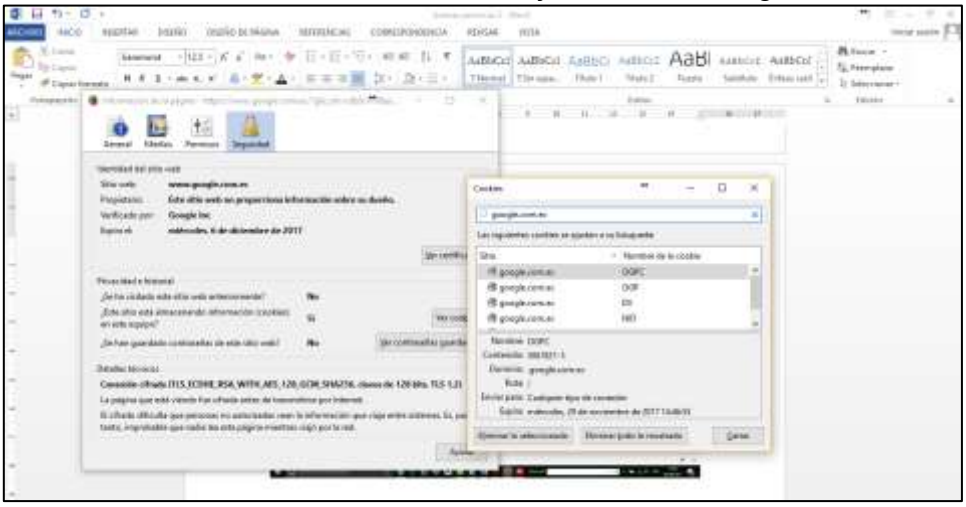
Gráfico 97 Visualización de las cookies



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Para cada cookie que se almacena se puede consultar sus atributos como dominio, ruta y fecha de caducidad que en este programa se llama expira.

Gráfico 98 Verificación de las cookies y los atributos según el dominio



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

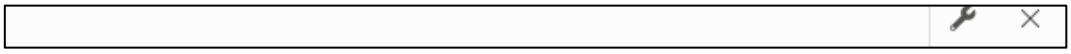
- Otra manera de visualizar las cookies activar la opción: Caja de Herramientas de desarrolladores.

Gráfico 99 Otra manera de visualizar las cookies

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

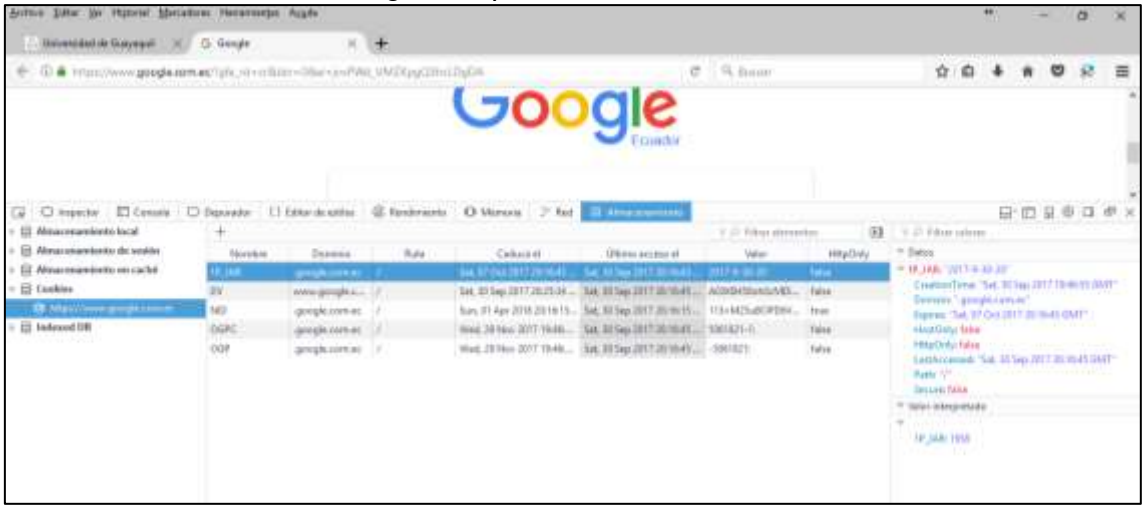
- Se activará en la parte inferior derecha una opción de llave, que al darle clic mostrará la información de las cookies almacenadas según su dominio.

Gráfico 100 Opción Herramientas



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 101 Segunda opción de visualización de las cookies

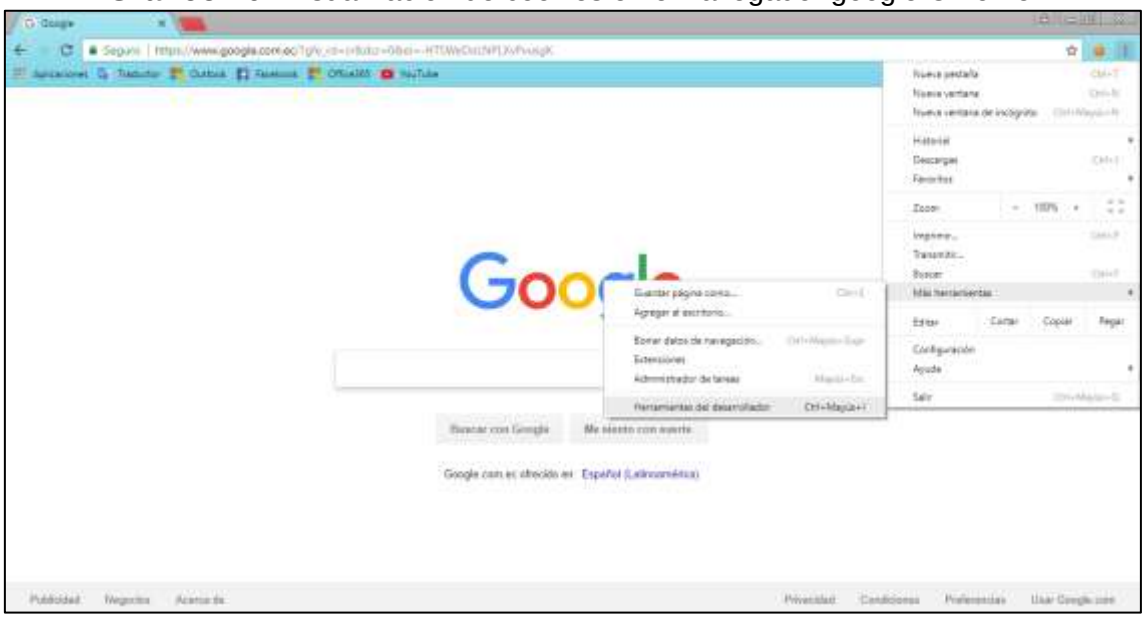


Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

VISUALIZACION DE LAS COOKIES ALOJADAS EN EL NAVEGADOR GOOGLE CHROME.

- Ubicarse en la opción Más herramientas, luego en la opción Herramientas del Desarrollador.

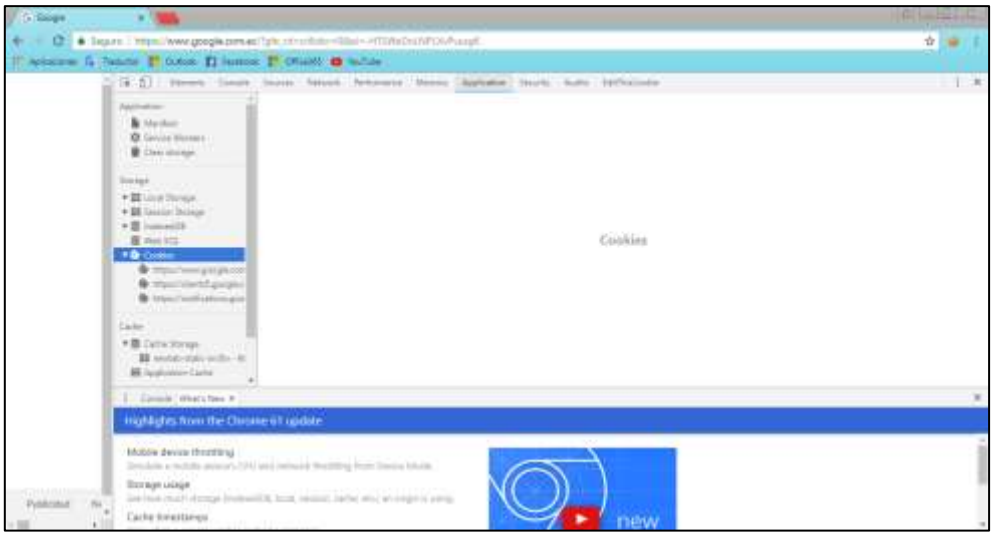
Gráfico 102 visualización de cookies en el navegador google Chrome



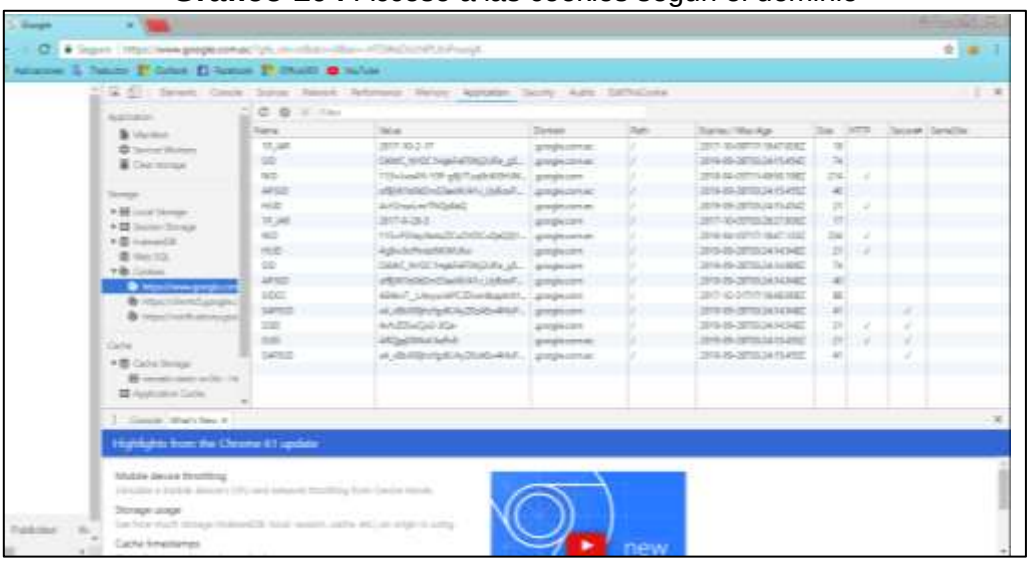
Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Dar clic en el menú la opción Application y seleccionar la pestaña cookies y el dominio del cual se quiere ver la cookies.

Gráfico 103 Acceso a las cookies de google Chrome



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento.
Gráfico 104 Acceso a las cookies según el dominio



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

COMO DESACTIVAR EL USO DE COOKIES Y QUE BENEFICIO SE TIENE AL REALIZAR ESTE PROCESO

Beneficio

El beneficio de realizar este proceso es que al momento de no aceptar cookies en el navegador de internet no se expone la información de sesión en donde puede ser espiada y capturada por piratas informáticos que realizan ataques asociados al robo de cookies.

Desventaja

No se monitoreara el sitio web y no se alertara errores que sufra dicho sitio.

DESACTIVAR EL USO DE COOKIES, MOZILLA FIREFOX

- Dar clic en herramientas y luego en opciones.

Gráfico 105 Desactivar Cookies Navegador Mozilla firefox

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

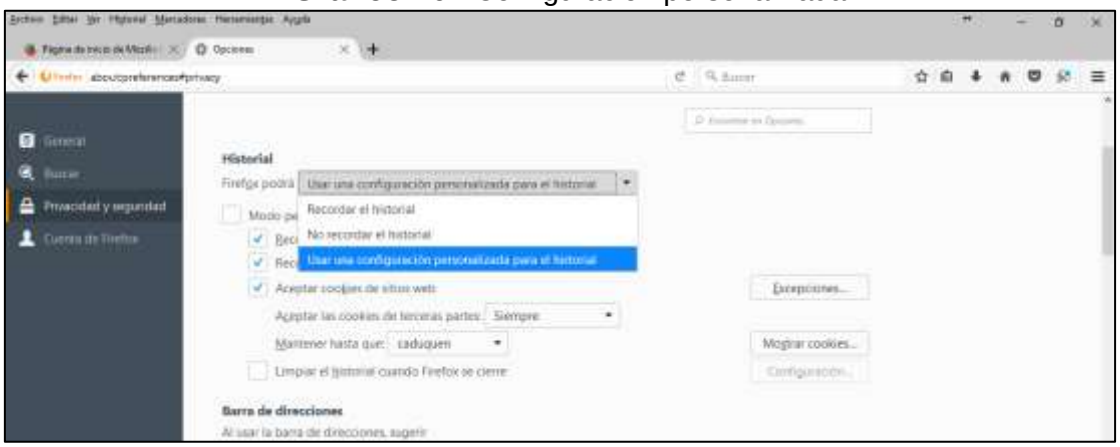
- Dar clic en la opción **Privacidad y seguridad**

Gráfico 106 Privacidad y Seguridad del navegador

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Luego se ubica en la opción Historial y después en el mensaje en Firefox podrá se escoge la opción Usar una configuración personalizada para el historial.

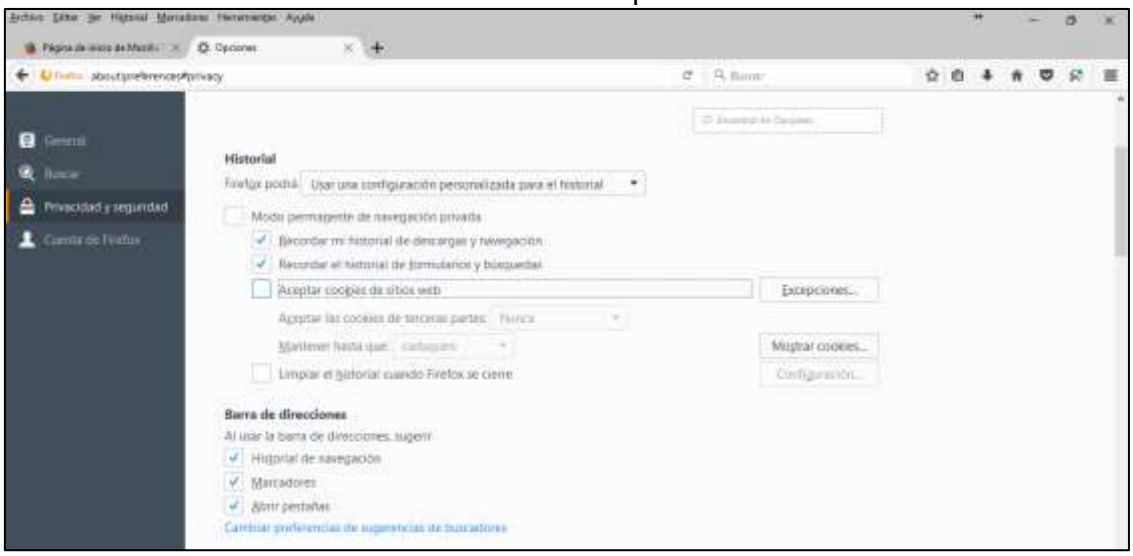
Gráfico 107 Configuración personalizada



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Desactivamos la casilla de Aceptar cookies de sitios web.

Gráfico 108 Desactivar opción de cookies



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento.

DESACTIVAR EL USO DE COOKIES, GOOGLE CHROME.

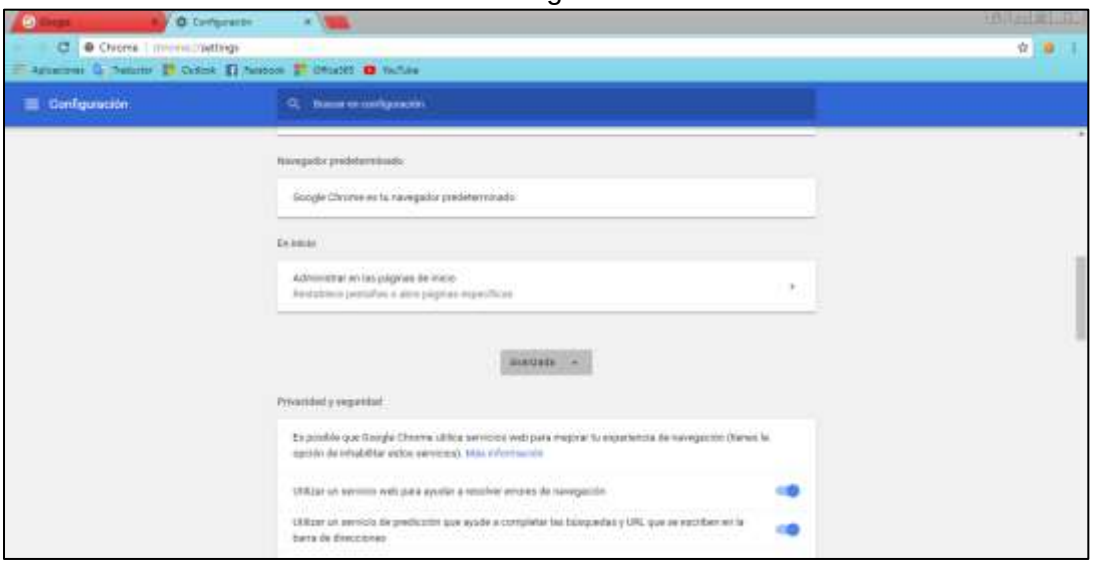
- Menú de opciones, Configuración

Gráfico 109 Desactivar cookies en Google Chrome

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Se da clic en Configuración Avanzada.

Gráfico 110 Configuración avanzada



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento.

- Se da clic en configuración de contenido, luego en Cookies.

Gráfico 111 Configuración de contenido

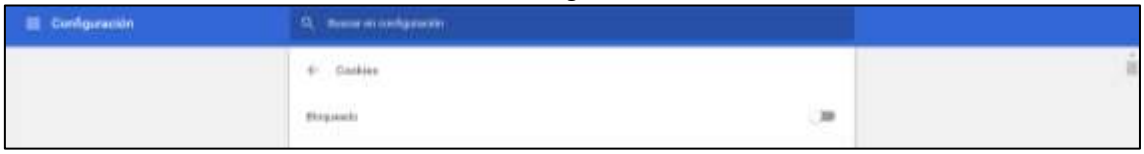
Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Se desactiva la opción permitir que todos los sitios guarden y lean datos de cookies

Gráfico 112 Desactivar la opción de cookies

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 113 Configuración de cookies



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

LIMPIEZA DEL HISTORIAL DE NAVEGACION

¿ES RECOMENDABLE LIMPIAR EL HISTORIAL DE NAVEGACION?

Si Fundamentalmente, para proteger la privacidad sobre todo si se accede a Internet de forma puntual en un ordenador que no es el nuestro o en un computador público como, por ejemplo, en una biblioteca, cyber café o demás lugares. Eliminar el historial de navegación es una tarea sencilla que solo lleva unos pocos segundos y permite borrar el rastro de las búsquedas. Pero limpiar el historial de navegación es especialmente de gran importancia y aconsejable si se ha rellenado algún formulario con los datos personales desde una PC que no es la propia, se debe tener en mucha consideración debido a que la información de carácter sensible puede verse afectada por atacantes maliciosos,

además, en dicho formulario si se ha realizado una compra e introducido datos bancarios, en ese caso, se debe borrar el historial del navegador de forma inmediata para que esos datos que fueren ingresados para efectuar transacciones en línea no queden almacenados en él y cualquier persona desconocida pueda acceder a ellos con el fin de beneficiarse económicamente o causar daño a su objetivo.

¿LAS COOKIES SE ELIMINAN AL BORRAR EL HISTORIAL DEL NAVEGADOR WEB?

La respuesta es SI

¿CÓMO BORRAR EL HISTORIAL DE NAVEGACIÓN EN GOOGLE CHROME?

Al tener acceso a internet y utilizar el navegador Google Chrome, se debe seguir los siguientes pasos, para la respectiva limpieza del historial de dicho navegador:

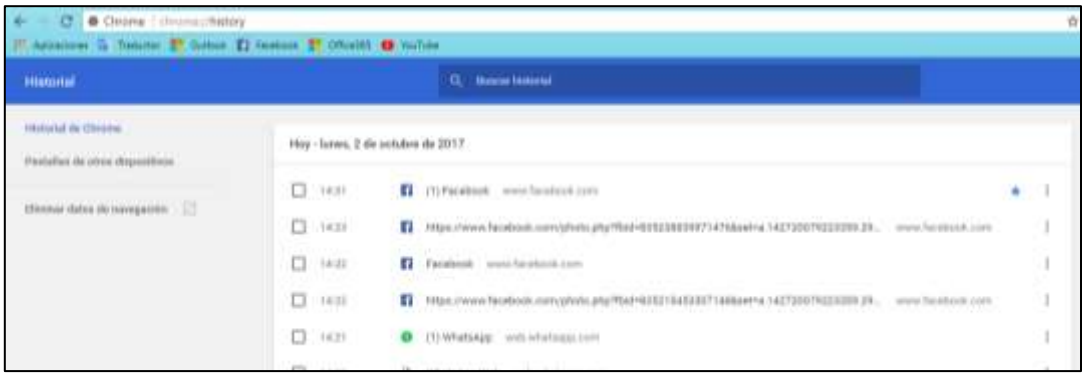
- En el primer paso se accede al menú que se ubica en la parte superior derecha de Chrome representado con un icono de tres puntos.
- Después, dar clic en el apartado Historial.

Gráfico 114 Apartado del Historial

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Por último pulsar clic en la opción eliminar

Gráfico 115 Eliminar cookies



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Luego escoger la opción eliminar desde el principio marcando todas las casillas.

Gráfico 116 Opción de eliminar cookies

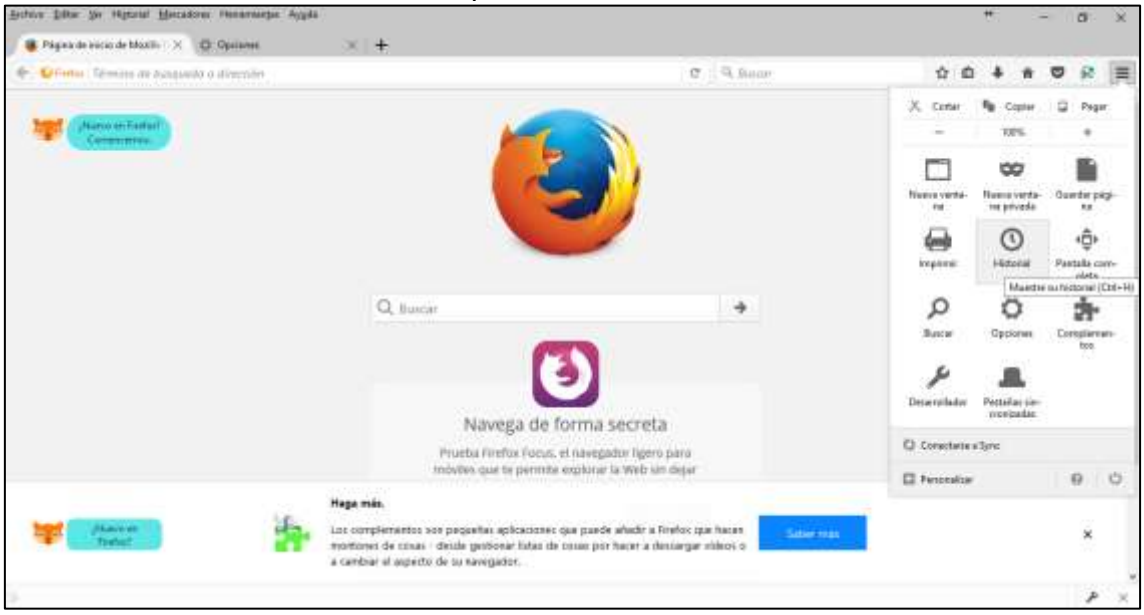
Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

¿CÓMO BORRAR EL HISTORIAL DE NAVEGACIÓN EN MOZZILA FIREFOX?

Al tener el acceso a internet y se utiliza el navegador Mozilla Firefox, se debe seguir los siguientes pasos para limpiar el historial de este navegador:

- Acceder al menú que está representado en la parte superior derecha de Mozilla Firefox con un icono de tres líneas cortas.
- Pulsar en el apartado Historial.

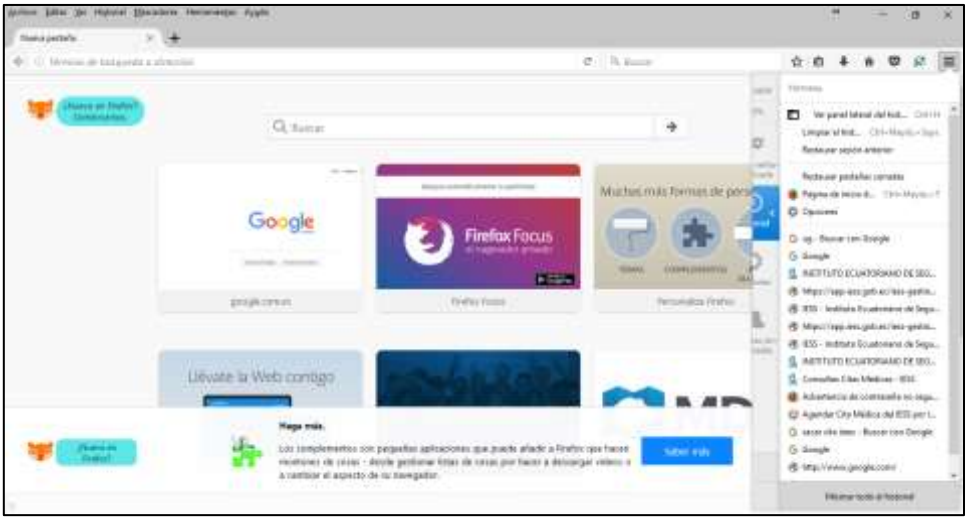
Gráfico 117 Apartado del Historial en Firefox



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Seleccionar la opción mostrar todo el historial.

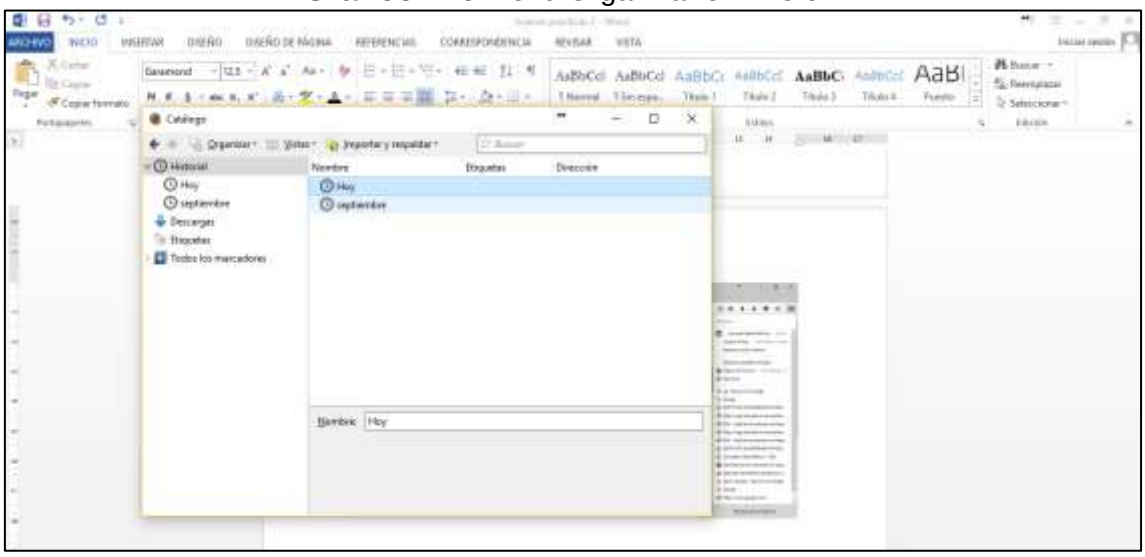
Gráfico 118 Mostrar el Historial en Firefox



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Por último se debe dirigir al menú organizar.

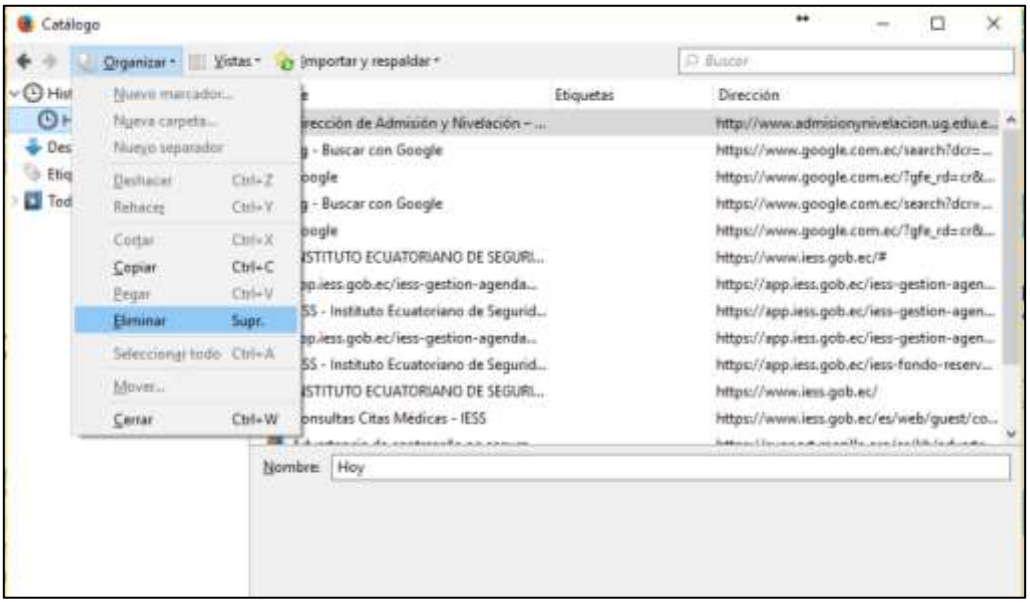
Gráfico 119 Menú Organizar en Firefox



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Escoger la opción eliminar.

Gráfico 120 Eliminar cookies en Firefox



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

USO DE LA NAVEGACION INCOGNITA

Entre las fórmulas más eficientes y útiles para lograr el objetivo planteado cabe mencionar la posibilidad que ofrecen los actuales navegadores web de permitir consultar Internet en modo privado o incógnito.

Mediante esta práctica funcional, los usuarios de la Red tienen la opción de navegar de forma mucho más segura y con mayor privacidad, ya que este modo evita que las páginas que visitamos sean guardadas en el historial de búsqueda del navegador y por tanto impide que se muestren.

Además, con el modo privado conseguimos que cuando cerramos la ventana, las cookies, contraseñas guardadas y otros datos locales de la sesión sean eliminados de forma automática. El único dato que se guardará serán los sitios favoritos que almacenemos y los archivos que descarguemos.

Navegar en este modo puede tener muchos usos prácticos. La más evidente, que permite acceder a Internet evitando que nadie acceda al equipo propio en donde pueda saber qué contenidos hemos estado consultando. Pero más allá de esto, existen también otras ventajas en el sentido del modo incógnito en la cual es una fantástica solución, por ejemplo, para acceder a Internet en un ordenador público o ajeno, de manera que las contraseñas que usemos para acceder al e-mail o a las redes sociales sean eliminadas al cerrar la sesión.

Por otra parte, navegar en modo incógnito también permitirá por ejemplo abrir de forma simultánea diferentes perfiles en cuentas de correo electrónico o redes sociales, algo que no es posible cuando navegamos en modo normal. De esta forma, podremos navegar en la cuenta de Gmail de la empresa a la que prestamos servicios y a la vez consultar también la propia cuenta en forma particular, aunque también sea del servicio de email de Google.

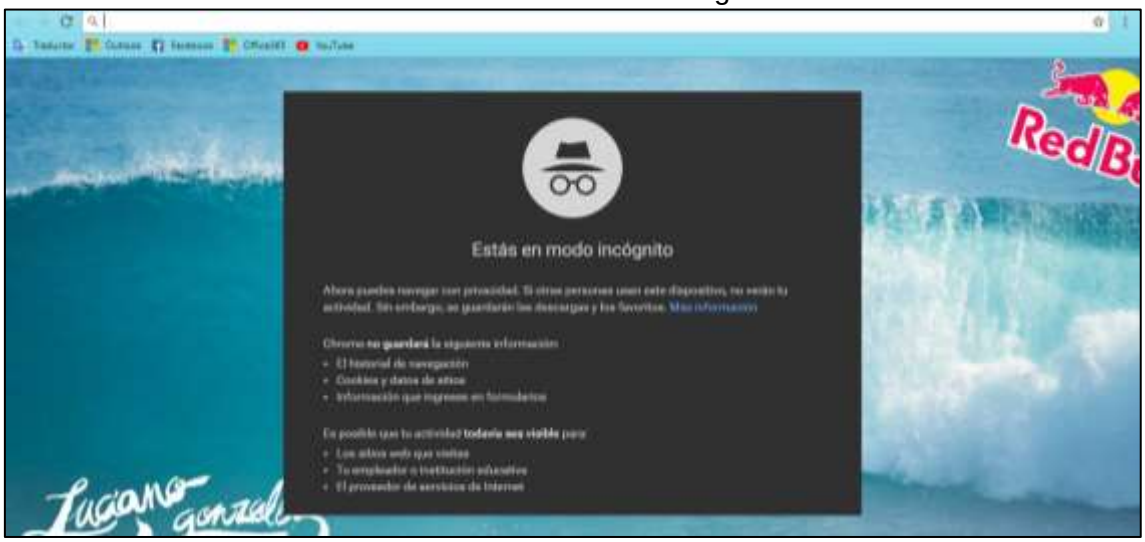
NAVEGACION INCOGNITA EN GOOGLE CHROME.

- **Presionar** Ctrl-Mayúsculas+N o seleccionar Nueva ventana de incógnito en las opciones que se despliegan al pulsar en el botón de menú representado por tres rayas horizontales en la parte superior derecha.

Gráfico 121 Nueva venta en incognito

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 122 Ventana incognito

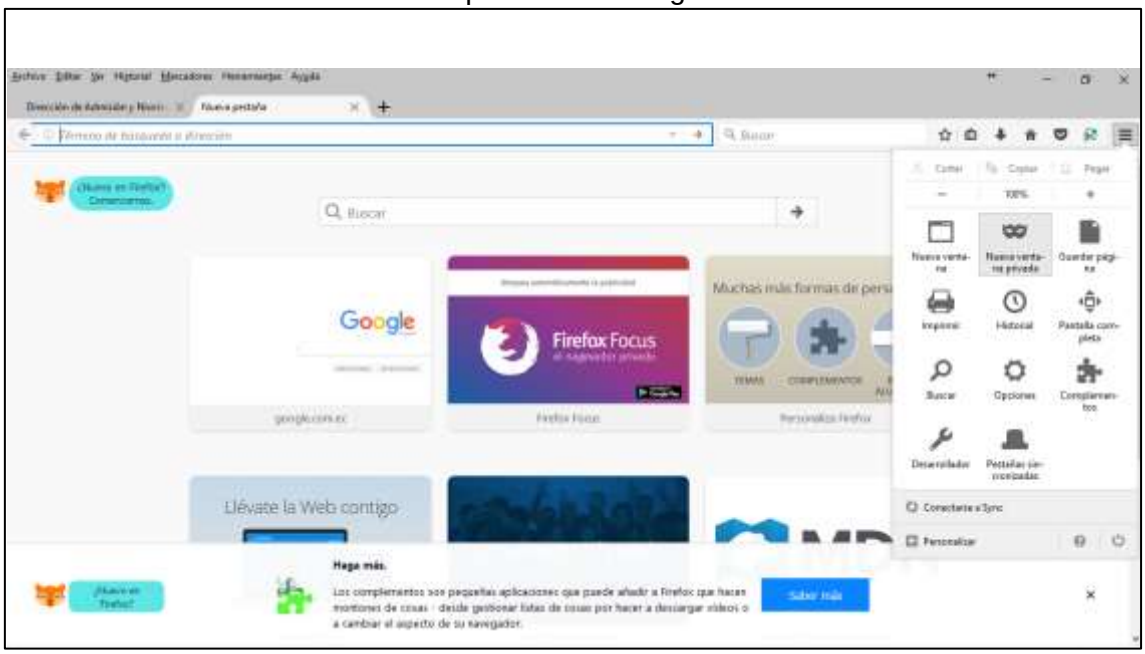


Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

NAVEGACION INCOGNITA EN MOZILLA FIREFOX.

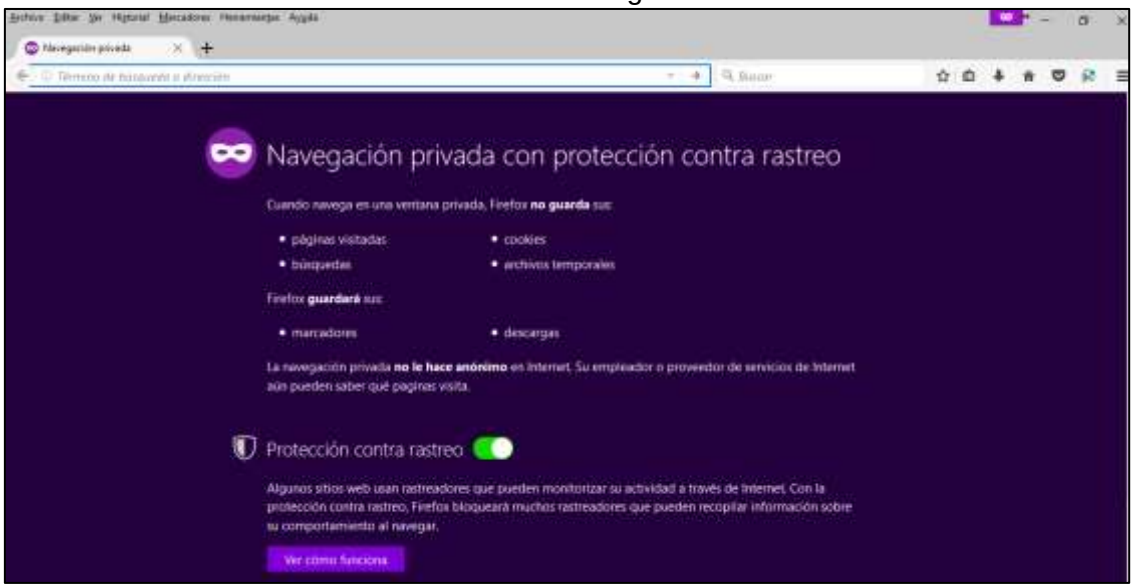
Presionar Ctrl+Mayúsculas+P o seleccionando Nueva ventana privada en las opciones que se despliegan al pulsar en el botón de menú representado por tres rayas horizontales en la parte superior derecha

Gráfico 123 opciones de incognito en Firefox



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 124 Modo incognito en Firefox



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

ALMACENAR CONTRASEÑAS EN EL NAVEGADOR

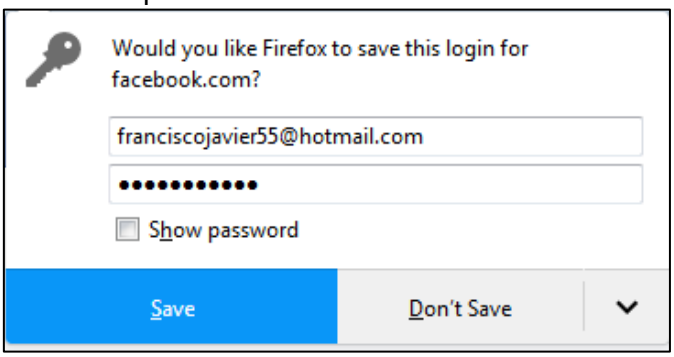
¿Es una práctica segura almacenar contraseñas en el navegador?

Los usuarios que hacen uso del internet, en algún momento, han visualizado el característico mensaje de ¿quieres que el navegador recuerde tu contraseña?**,** dicho mensaje aparece por pantalla, generalmente en la parte superior de la pantalla, tras registrarnos en algún servicio web.

Esta práctica, puede ser muy peligrosa si compartimos nuestro ordenador con otros usuarios, ya que cualquier usuario podría acceder a ellas o a la vez sufrir ataques de intrusión que podrían facilitar el robo de las contraseñas.

MOZILLA FIREFOX

Gráfico 125 Opciones de almacenar contraseñas en Firefox



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Como eliminar contraseñas en el caso de que alguna se halla guardado.

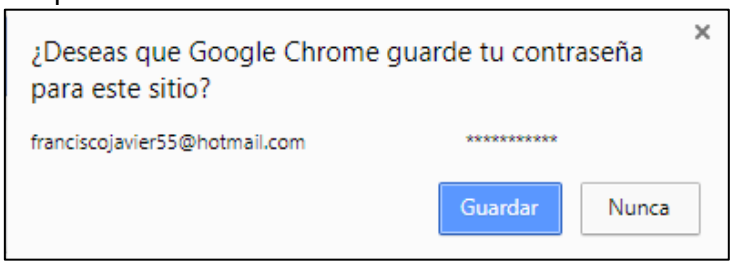
1. Abrir Firefox.
2. Haz clic en Herramientas y luego en Opciones.
3. Seleccionar el icono Seguridad.
4. Pulsar sobre Contraseñas guardadas.
5. Hacer clic en Eliminar.

Gráfico 126 Eliminación de contraseñas en Firefox

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

GOOGLE CHROME

Gráfico 127 Opciones de almacenamiento de contraseñas en Google Chrome



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Como eliminar contraseñas en el caso de que alguna se halla guardado.

1. Abrir Chrome.
2. Hacer clic en el icono del menú de Chrome.
3. Seleccionar Configuración.
4. Pulsar sobre el enlace Mostrar opciones avanzadas en la parte inferior de la página.
5. Desplazar con el cursor a la sección Contraseñas y formularios.

6. Hacer clic en el enlace Administrar contraseñas guardadas.
7. Eliminar las contraseñas memorizadas.

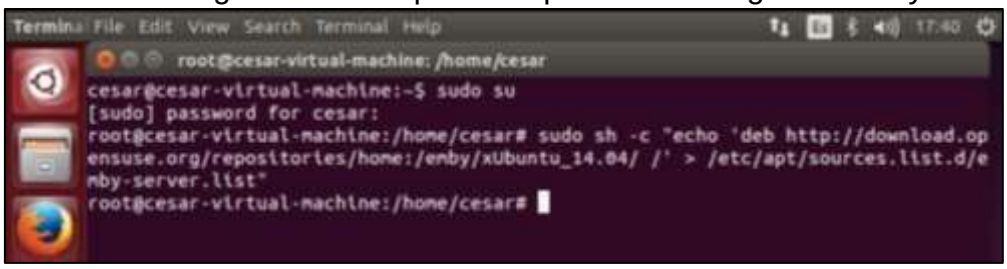
Gráfico 128 Eliminación de contraseñas en Google Chrome

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

ANEXO 1: MANUAL DE IMPLEMENTACIÓN DEL EMBY

Para iniciar la instalación de Emby-Media-Server se utilizó el sistema operativo Ubuntu con su versión 14.04, en donde se aplicó el comando sudo sh –c para agregar el link del repositorio del paquete Emby al sistema operativo como se muestra en el Gráfico 43.

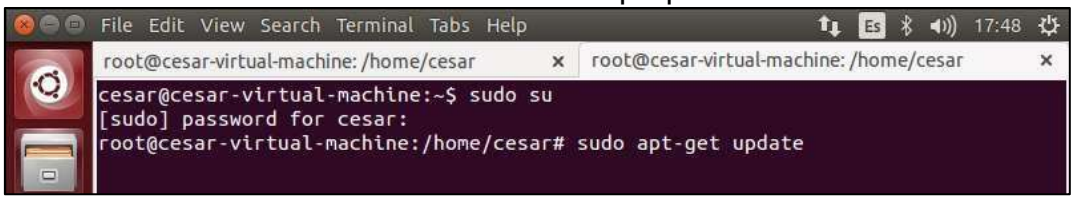
Gráfico 43 Asignación del repositorio para la descarga del Emby



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

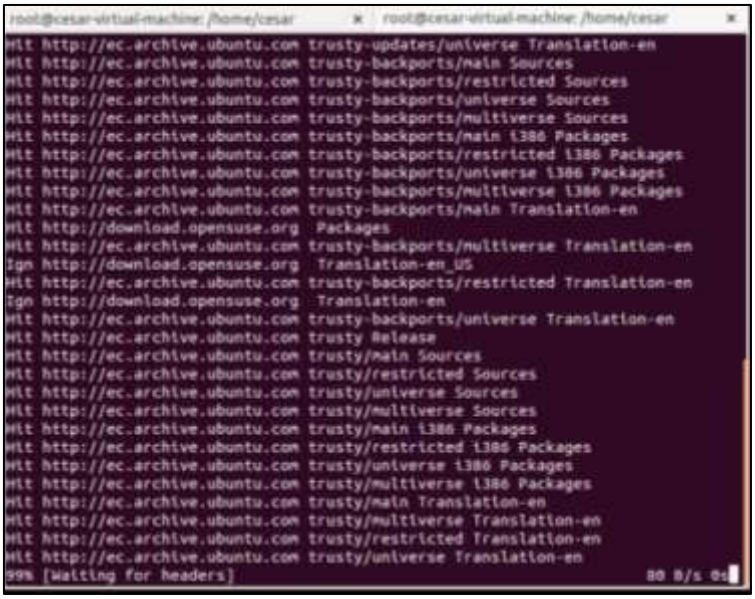
Una vez realizado el primero paso de la instalación de Emby-Media-Server se procede a actualizar los paquetes del sistema operativo Ubuntu como se muestra en el Gráfico 44 y 45.

Gráfico 44 Inicio de actualización de paquetes en Ubuntu



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

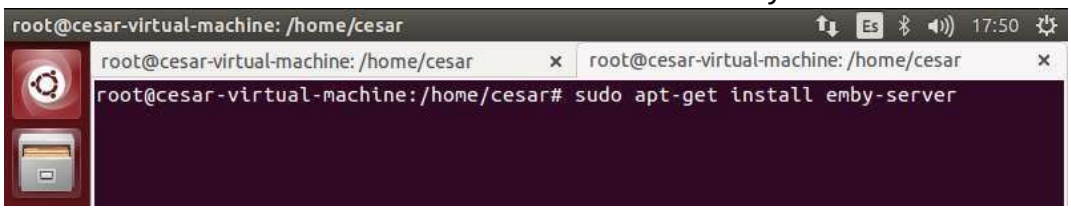
Gráfico 45 Finalización de actualización



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

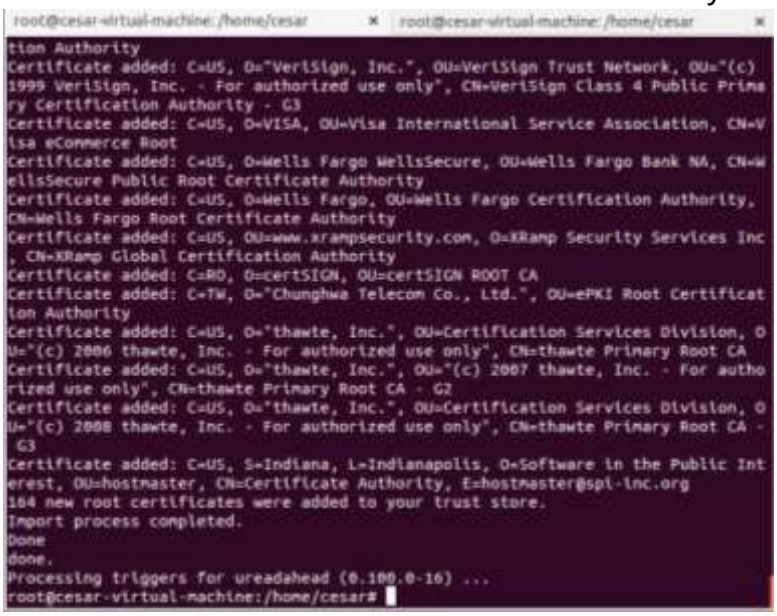
Después de haber realizado el proceso de actualización de paquetes en Ubuntu se inicia la instalación del servidor Emby como se indica en el Gráfico 46 y 47.

Gráfico 46 Inicio de instalación del Emby Server



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 47 Finalización de la instalación de Emby Server



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Una vez terminado el proceso de instalación de Emby-Media-Server, se comienza a instalar el servidor SSH en modo cliente como se muestra en el Gráfico 48 en la cual lo utilizaremos para la transferencia de archivo multimedia por medio de la herramienta WinSCP.

Gráfico 48 Instalación del servicio SSH en modo cliente

```
root@cesar-virtual-machine: /home/cesar    root@cesar-virtual-machine: /home/cesar
root@cesar-virtual-machine:/home/cesar# sudo apt-get install openssh-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  libpam-ssh keychain monkeysphere
The following packages will be upgraded:
  openssh-client
1 upgraded, 0 newly installed, 0 to remove and 655 not upgraded.
Need to get 576 kB of archives.
After this operation, 1.024 B of additional disk space will be used.
Get:1 http://ec.archive.ubuntu.com/ubuntu/ trusty-updates/main openssh-client i3
86 1:6.6p1-2ubuntu2.8 [576 kB]
Fetched 576 kB in 2s (218 kB/s)
(Reading database ... 167483 files and directories currently installed.)
Preparing to unpack .../openssh-client_1%3a6.6p1-2ubuntu2.8_i386.deb ...
Unpacking openssh-client (1:6.6p1-2ubuntu2.8) over (1:6.6p1-2ubuntu2) ...
Processing triggers for man-db (2.6.7.1-1) ...
Setting up openssh-client (1:6.6p1-2ubuntu2.8) ...
root@cesar-virtual-machine:/home/cesar#
```

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Después de instalar el servicio SSH en modo cliente, se comienza a instalar el servidor SSH Servidor como se muestra en el Gráfico 49 y 50 para el acceso desde una herramienta externa.

Gráfico 49 Instalación del servicio SSH en modo server

```
root@cesar-virtual-machine: /home/cesar    root@cesar-virtual-machine: /home/cesar
root@cesar-virtual-machine:/home/cesar# sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libck-connector0 ncurses-term openssh-sftp-server python-requests
  python-urllib3 ssh-import-id
Suggested packages:
  rssh molly-guard monkeysphere
The following NEW packages will be installed:
  libck-connector0 ncurses-term openssh-server openssh-sftp-server
  python-requests python-urllib3 ssh-import-id
0 upgraded, 7 newly installed, 0 to remove and 655 not upgraded.
Need to get 706 kB of archives.
After this operation, 3.902 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 50 Proceso de instalación del servicio SSH

```
root@cesar-virtual-machine: /home/cesar        root@cesar-virtual-machine: /home/cesar
Preparing to unpack .../openssh-server_1%3a6.6p1-2ubuntu2.8_i386.deb ...
Unpacking openssh-server (1:6.6p1-2ubuntu2.8) ...
Selecting previously unselected package python-urllib3.
Preparing to unpack .../python-urllib3_1.7.1-1ubuntu4_all.deb ...
Unpacking python-urllib3 (1.7.1-1ubuntu4) ...
Selecting previously unselected package python-requests.
Preparing to unpack .../python-requests_2.2.1-1ubuntu0.3_all.deb ...
Unpacking python-requests (2.2.1-1ubuntu0.3) ...
Selecting previously unselected package ssh-import-id.
Preparing to unpack .../ssh-import-id_3.21-0ubuntu1_all.deb ...
Unpacking ssh-import-id (3.21-0ubuntu1) ...
Processing triggers for man-db (2.6.7.1-1) ...
Processing triggers for ufw (0.34-rc-0ubuntu2) ...
Processing triggers for ureadahead (0.100.0-16) ...
Setting up libck-connector0:i386 (0.4.5-3.1ubuntu2) ...
Setting up ncurses-term (5.9+20140118-1ubuntu1) ...
Setting up openssh-sftp-server (1:6.6p1-2ubuntu2.8) ...
Setting up openssh-server (1:6.6p1-2ubuntu2.8) ...
Creating SSH2 RSA key; this may take some time ...
Creating SSH2 DSA key; this may take some time ...
Creating SSH2 ECDSA key; this may take some time ...
Creating SSH2 ED25519 key; this may take some time ...
ssh start/running, process 8753
Setting up python-urllib3 (1.7.1-1ubuntu4) ...
Setting up python-requests (2.2.1-1ubuntu0.3) ...
Setting up ssh-import-id (3.21-0ubuntu1) ...
Processing triggers for libc-bin (2.19-0ubuntu6) ...
Processing triggers for ufw (0.34-rc-0ubuntu2) ...
Processing triggers for ureadahead (0.100.0-16) ...
root@cesar-virtual-machine:/home/cesar#
```

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Una vez instalado el servicio SSH se procede a la configuración del archivo ssh_config por medio del comando Gedit que se encuentra ubicado en la ruta /etc/ssh.

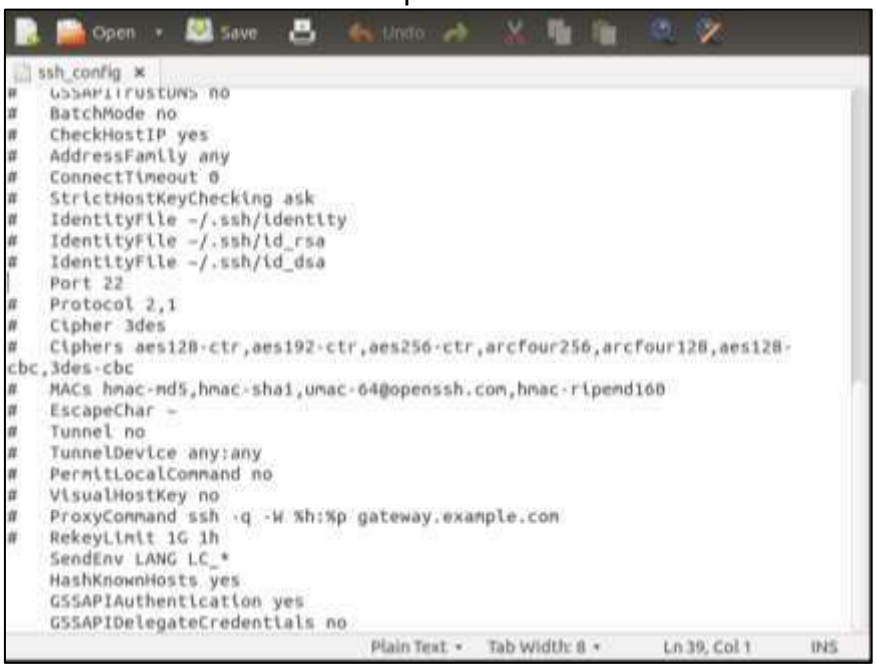
Gráfico 51 Acceso al archivo ssh_config

```
root@cesar-virtual-machine: /home/cesar        root@cesar-virtual-machine: /home/cesar
root@cesar-virtual-machine:/home/cesar# gedit /etc/ssh/ssh_config
```

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Una vez abierto el archivo ssh_config se ubica en la línea 39, se quita el numeral de dicha línea, habilitando el puerto 22 como se muestra en el Gráfico 52.

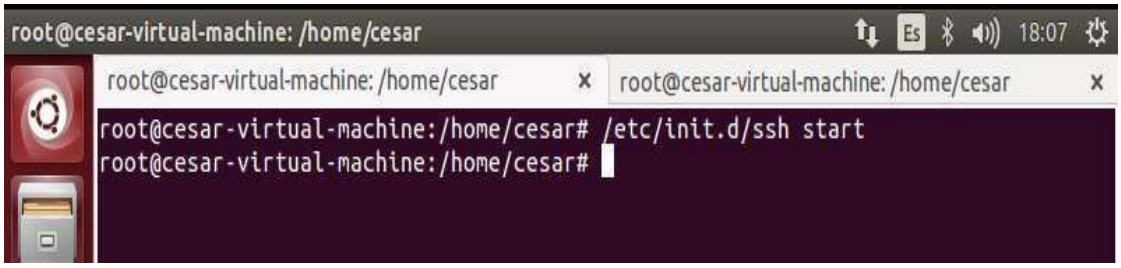
Gráfico 52 Verificación del puerto 22 del servicio SSH



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Una vez configurado el archivo ssh_config se procede a levantar el servicio de ssh como se indica el Gráfico 53.

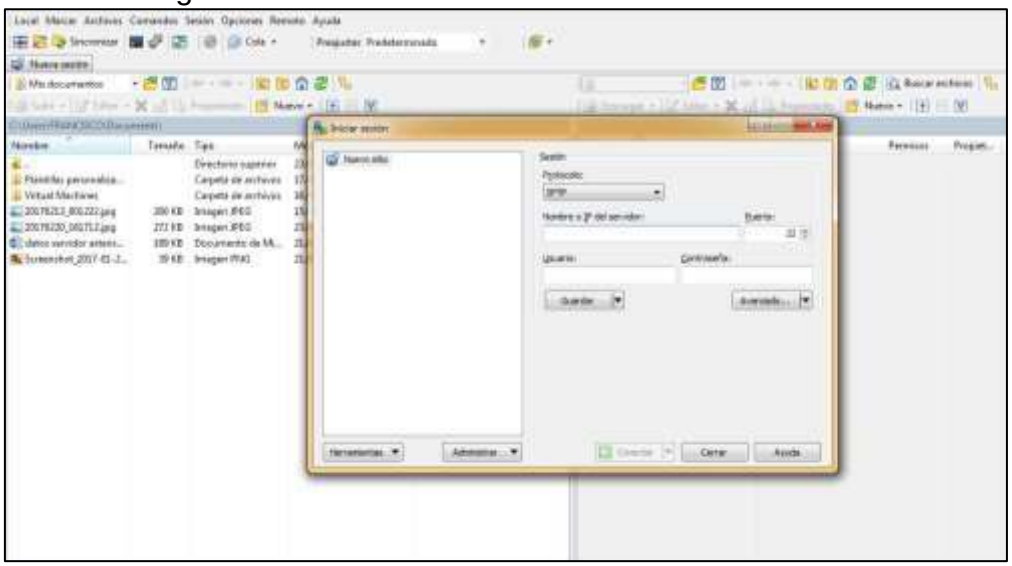
Gráfico 53 Levantamiento del servicio SSH



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Una vez levantado el servicio SSH se procede a loguear con las credenciales de Ubuntu en la herramienta WinSCP para la transferencia de contenido multimedia como se indica en el Gráfico 54.

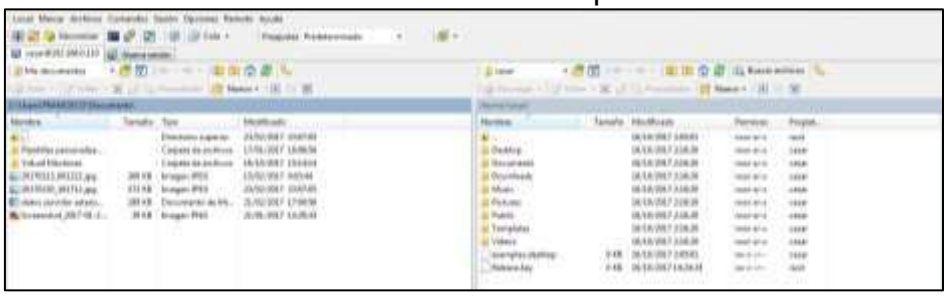
Gráfico 54 Logueo de las credenciales de Ubuntu mediante WinSCP



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Una vez establecido él logueo con las credenciales de Ubuntu con la herramienta WinSCP se procede a transferir el contenido multimedia desde el cliente al servidor.

Gráfico 55 Acceso al servidor de Ubuntu por medio WinSCP



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

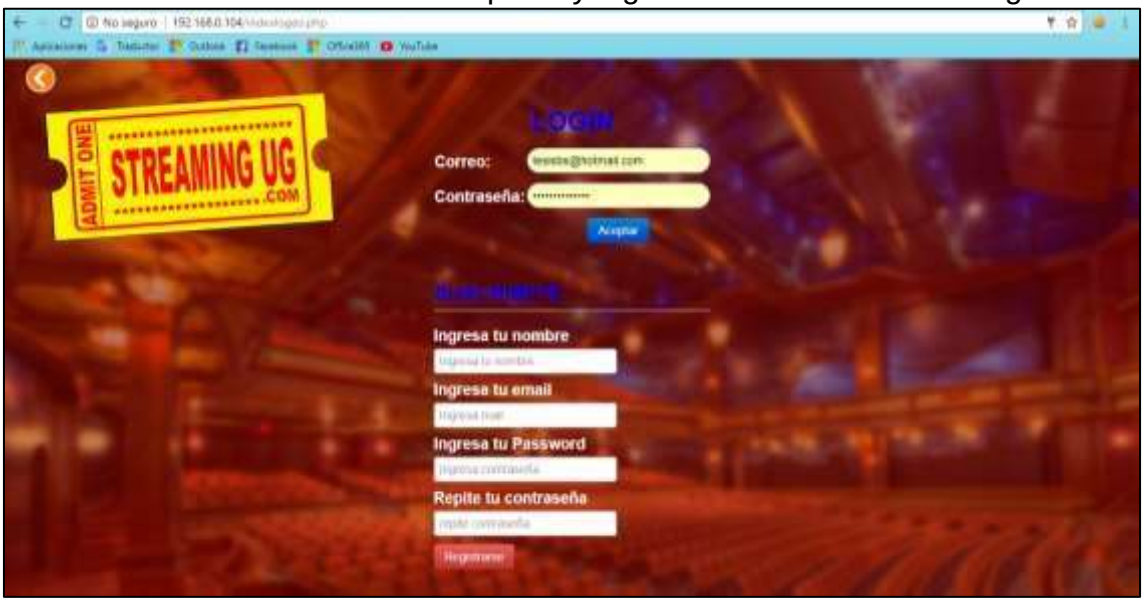
Para la creación del ambiente de prueba se desarrolló una interfaz web local como se muestra en el Gráfico 56, para la respectiva simulación de la suscripción de usuario.

Gráfico 56 Portada del inicio de la interfaz web del servidor Streaming

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

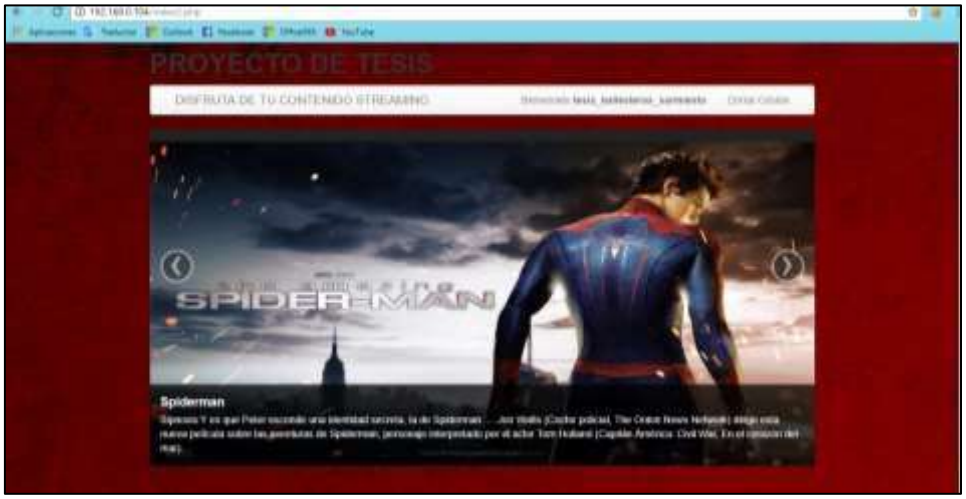
Una vez dado click en el botón entrar, se redirige al formulario de suscripción y logueo de credenciales como se indica el Gráfico 57, para iniciar el acceso al contenido multimedia almacenado en el servidor Streaming de prueba como se indica también el Gráfico 59 donde se muestra la sesión del usuario suscrito.

Gráfico 57 Formulario de suscripción y logueo del servidor Streaming



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 58 Sesión del usuario suscrito



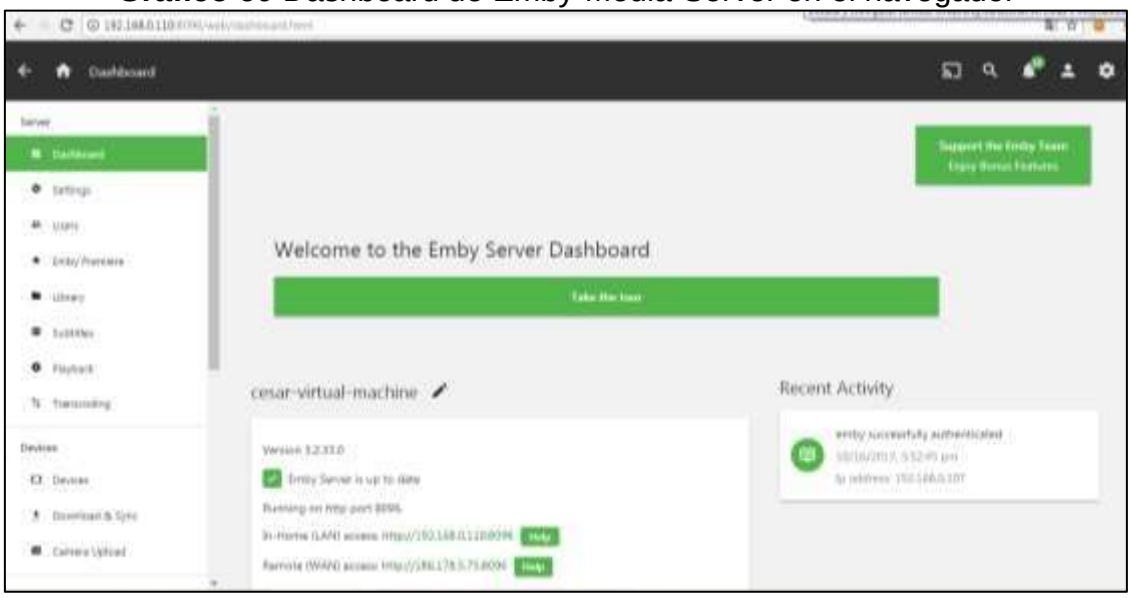
Fuente: Trabajo de Investigación

Una vez dado click en el enlace de disfruta tu contenido Streaming, se tendrá el acceso dashboard de Emby donde se podrá acceder al contenido multimedia como se indica el Gráfico 60.

Gráfico 59 Acceso al contenido Streaming

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 60 Dashboard de Emby-Media-Server en el navegador



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

ANEXO 2: TEST DE PENETRACIÓN

¿Qué es un test de penetración?

También es llamado como pentest, es un método de valorar y evaluar la seguridad de los equipos y las redes de comunicación simulando un ataque informático a un servidor o red desde una fuente externa o interna, consiste en un análisis activo de todos los dispositivos de la red para detectar cualquier vulnerabilidad o una falla en la configuración de los servidores o los equipos de seguridad.

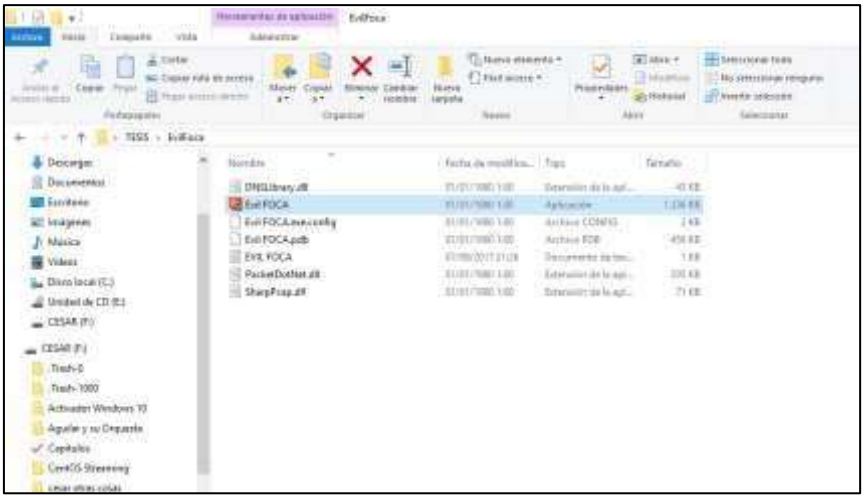
Herramientas a utilizar para realizar el pentest.

- Software: Evil foca.
- Wireshark.

EJECUTAR LOS SIGUIENTES PASOS:

- Desde el ordenador atacante, se inicia el software de ataque: Evil Foca.

Gráfico 61 Inicio de Evil Foca



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

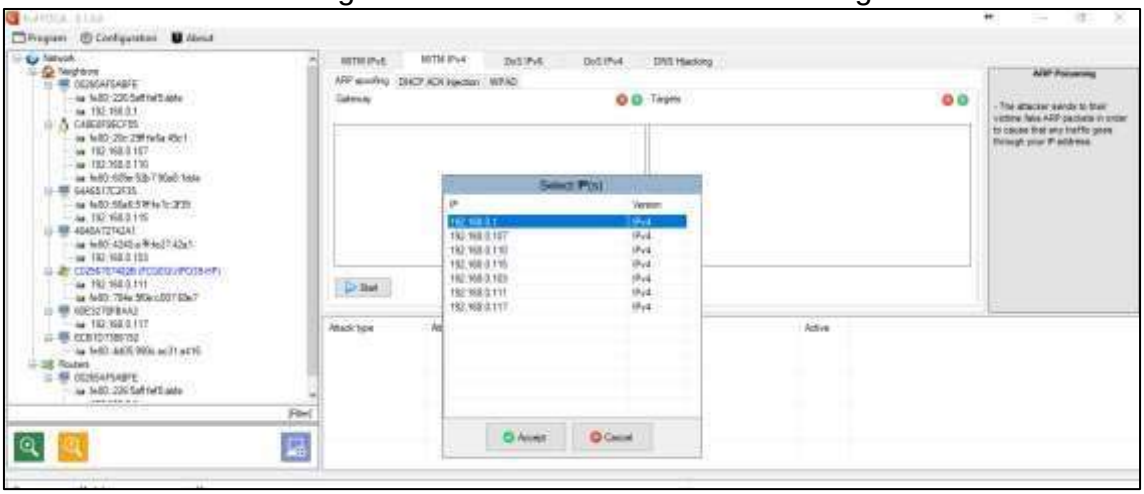
- Seleccionar la opción MITM IPV4 ataque (Man-in-the-middle).

Gráfico 62 MITM IPV4 ataque (Man-in-the-middle).

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Dar clic, en el botón + de color verde del primer target, se abrirá una ventana de direcciones IP, donde seleccionaremos la Ip del router de la red, 192.168.0.1/24, dar clic en aceptar.

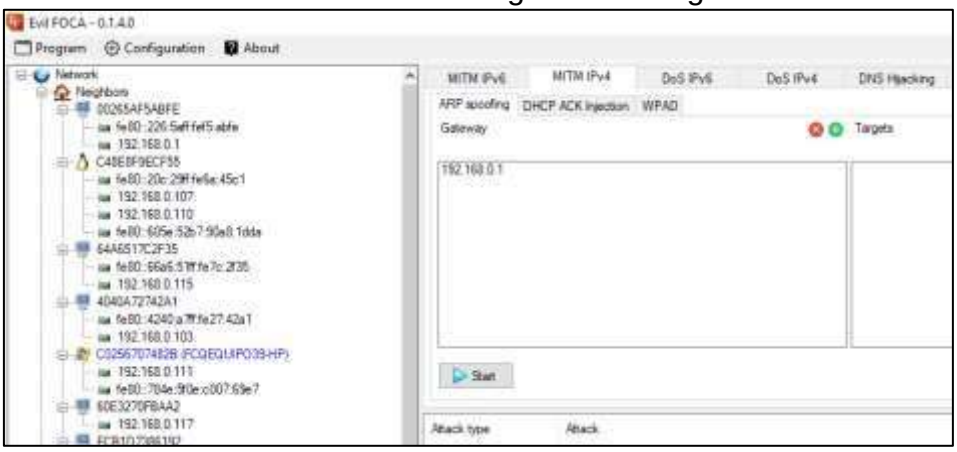
Gráfico 63 Asignación de direcciones IPs en el Target 1



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- La dirección del router se ubica en el target 1.

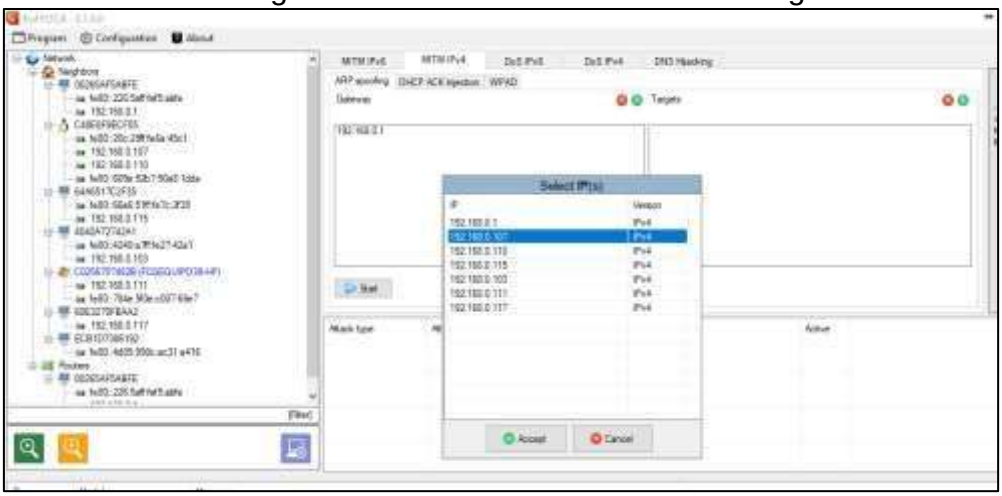
Gráfico 64 Dirección IP asignada al Target 1



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Dar clic, en el botón + de color verde del segundo target, se escogerá la dirección IP de la víctima 192.168.0.107/24, poner en aceptar para dar inicio al ataque MITM.

Gráfico 65 Asignación de direcciones IPs en el Target 2



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

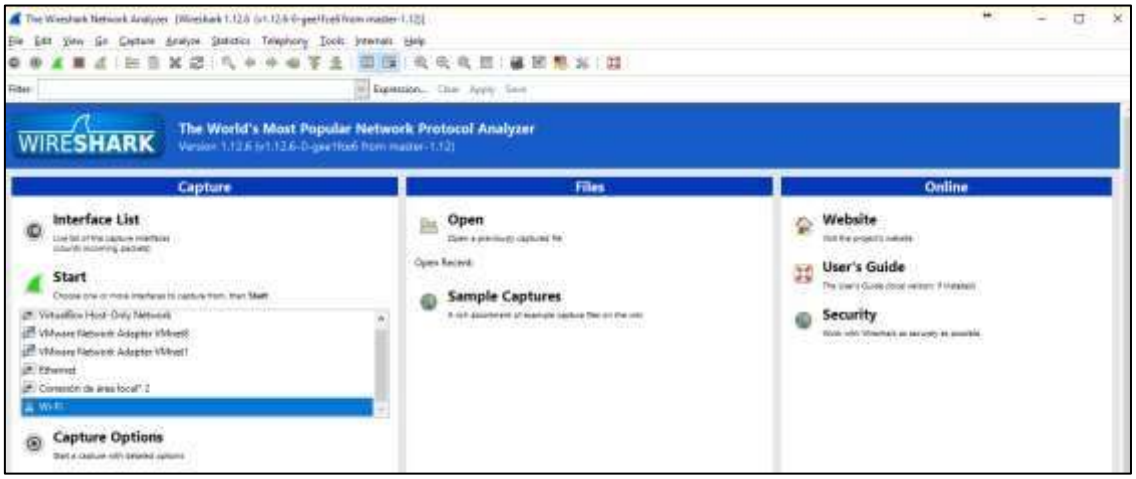
- Una vez que la dirección IP del router y la IP de la víctima estén ubicadas correctamente en los targets, se da click en Start para dar inicio al ataque.

Gráfico 66 Inicio del Ataque

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Dirigirse al analizador de trafico WIRESHARK, seleccionar la tarjeta de red inalámbrica, dar clic en Start para iniciar el análisis del tráfico.

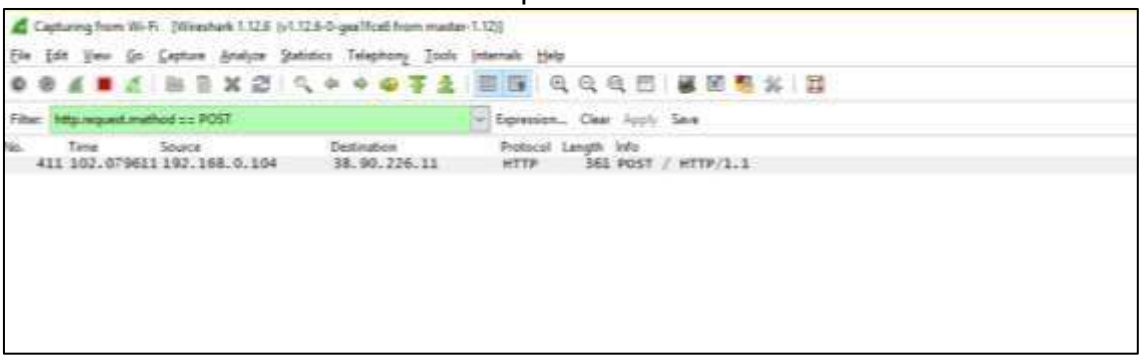
Gráfico 67 Inicio del Sniffer



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Una vez que el analizador de trafico Wireshark esté en marcha, se aplicara el filtro de captura **http.resquest.method==POST** donde este ayudara a la sustracción de las credenciales cuando el usuario se autentique en la interfaz web de la plataforma Streaming.

Gráfico 68 Captura del trafico



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

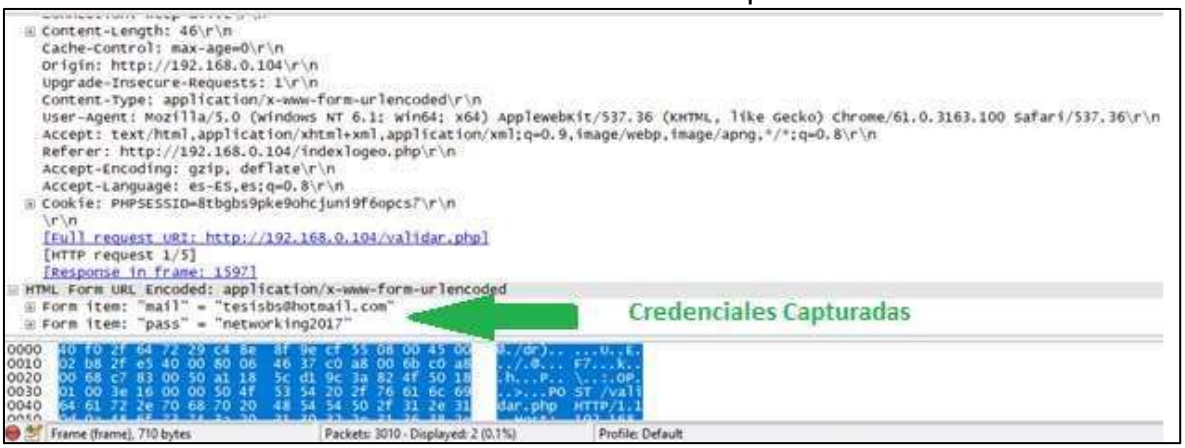
- Esperamos que el usuario se autentique desde la maquina victima

Gráfico 69 Espera de autenticación

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Una vez que el usuario se haya autenticado, se verifica en la parte inferior izquierda del Wireshark las credenciales capturadas del usuario logueado en el servidor Streaming.

Gráfico 70 Muestra de credenciales Capturadas



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Credenciales capturadas:
Correo: tesisbs@hotmail.com
Contraseña: networking2017

- Una vez capturadas las credenciales, hacer uso de las mismas desde la maquina atacante, para realizar el proceso del método de duplicación de sesión por medio de cookies.

DUPLICACION DE SESION POR MEDIO DE COOKIES EN GOOGLE CHROME.

Gráfico 71 Ingresar al dominio del servidor Streaming
http://192.168.0.104/INI.html

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Autenticarse con las credenciales sustraídas durante el ataque.

Gráfico 72 Logueo de credenciales

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 73 Mensaje de éxito de autenticación

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Ingresar a la interfaz del servidor Streaming.

Gráfico 74 Acceso al servidor Streaming

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Instalar la extensión EditThisCookie en el navegador.

Gráfico 75 Instalación de la Extensión Edit-Cookie

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

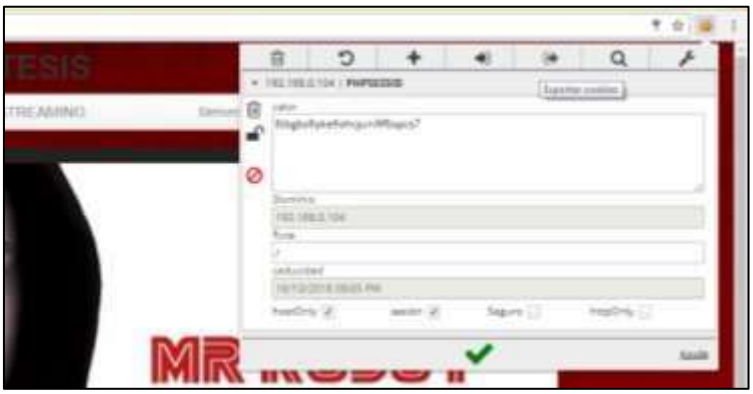
Gráfico 76 Selección de la cookie

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

EXTRACCION DE LA COOKIE DE SESION

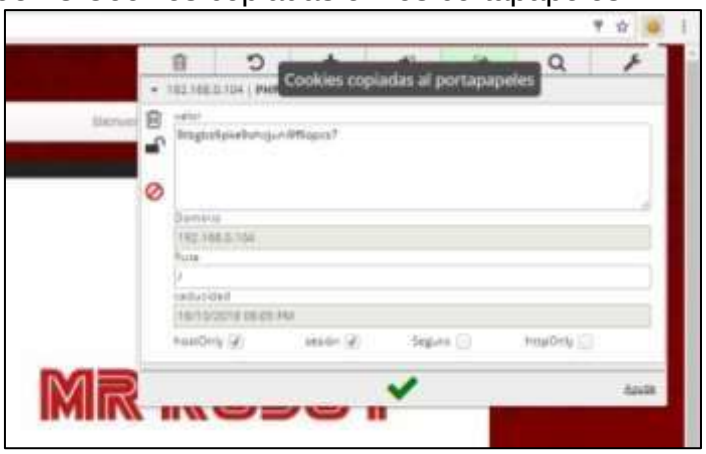
- Clic en el icono de la extensión EditThiscookie, seleccionar la opción de exportar la cookie de sesión para que sea almacena en el portapapeles y luego pegada en un documento de texto.

Gráfico 77 Proceso de extracción de cookies



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 78 Cookies copiadas en los cortapapeles



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 79 Cookie almacenada en bloc de notas

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

DUPLICACION DE SESION EN OTRO ORDENADOR

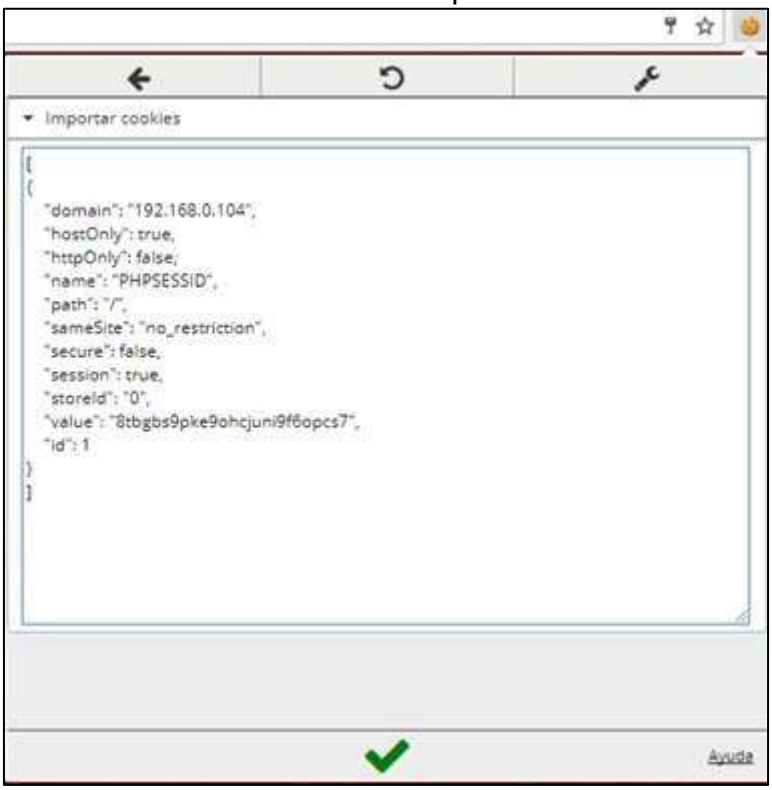
- Se realiza la inyección de la cookie obtenida, dar clic en el icono de la extensión EditThisCookie y poner en la opción de importar cookies.

Gráfico 80 Proceso de Importación de Cookie

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Pegar el código de la cookie anteriormente sustraída en el cuadro que se despliega, luego dar clic en el visto de color verde.

Gráfico 81 Cookie Importada



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

21.- ingresar al dominio de la sesión http://192.168.0.104/index2.php, dar Enter para que la duplicación se efectúe.

Gráfico 82 Acceso del servidor Streaming por medio de Google Chrone

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

<u>DUPLICACION DE SESION EN MOZILLA FIREFOX.</u>

Gráfico 83 Instalar el complemento de Firefox: **Edit Cookies.**

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

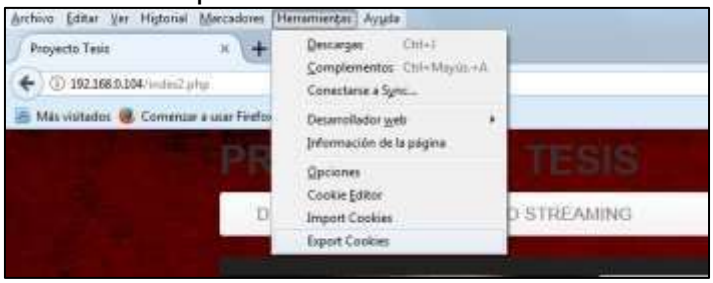
- Autenticarse con las credenciales obtenidas durante el ataque, ingresar a la interfaz del servidor Streaming.

Gráfico 84 Ingreso de credenciales por medio de Firefox

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Extracción de la cookie, dar clic en herramientas y escoger la opción: Export Cookies.

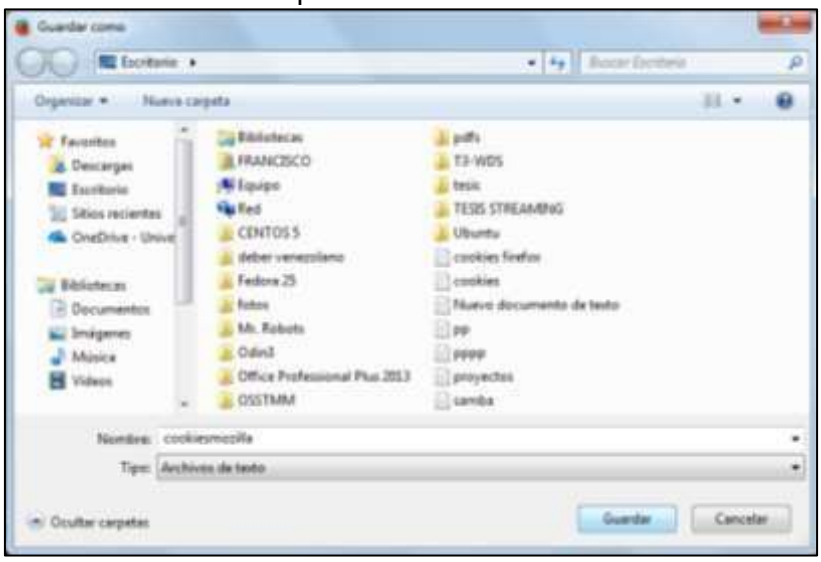
Gráfico 85 Exportación de cookies en Firefox



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Guardar la cookie extraída.

Gráfico 86 Ruta para almacenar la cookie en Firefox



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

DUPLICACION DE SESION EN OTRO ORDENADOR

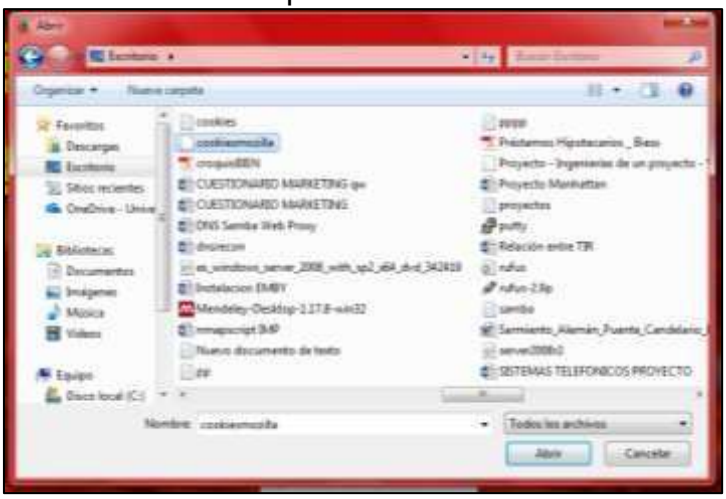
- Dar clic en la opción herramientas, importar cookies.

Gráfico 87 Proceso de Importación de cookies en Firefox

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Buscar la ruta del fichero.

Gráfico 88 Selección de la ruta para abrir el archivo de cookies



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 89 Aceptación de la cookie

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Se obtiene exitosamente la duplicación de sesión

Gráfico 90 Acceso al servidor Streaming desde Firefox

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

ANEXO 3: GUÍA DE BUENAS PRÁCTICAS ORIENTADAS AL USUARIO, PARA LA PROTECCIÓN DE SU INFORMACIÓN Y EVITAR ATAQUES DE DUPLICACIÓN DE SESIÓN POR COOKIES.

AUTORES:

Simón Cesar Ballesteros Correa.

Francisco Xavier Sarmiento Ronquillo

Objetivo General

Dar a conocer al usuario mecanismos de protección de la información, para evitar el robo de sesiones por cookies.

Objetivos Específicos

- Facilitar conocimientos al usuario sobre la información que almacenan las cookies.
- Proporcionar procedimientos sobre el buen uso del navegador Google Chrome y Mozilla Firefox, referente a la eliminación de información almacenada en los mismos.
- Dar a conocer el uso de la navegación incógnita en navegadores de internet.

¿QUE SON LAS COOKIES?

Las cookies son datos que recibe un navegador web junto con una página y que se almacenan en el ordenador del usuario.

Las cookies se utilizan para guardar las opciones de diseño que se realiza en una plataforma que puede contener: colores, imágenes, opciones, sonidos, etc.

Además son aptos de recordar información de hábitos sobre la navegación que ha realizado el usuario, tienen la capacidad de memorizar las contraseñas cuando se inicia sesión en una web, para que, al acceder de nuevo a la página, no se tenga que volver a digitar el usuario y contraseña y tener así ya el dato de los gustos de navegación.[23]

El propósito vital de una cookie es reconocer al usuario almacenando su historial de actividad en un sitio web específico, de manera que se le pueda ofrecer el contenido más apropiado según sus hábitos.

Esto quiere decir que cada vez que se visita una página web por primera vez, se guarda una cookie en el navegador con un poco de información. Luego, cuando se visita nuevamente la misma página, el servidor pide la misma cookie para arreglar la configuración del sitio y hacer la visita del usuario tan personalizada como sea posible.

La especificación general de las cookies fue desarrollada por Netscape en el año de 1994 y hoy en día aún se puede encontrar este documento en la web, la última especificación de las cookies la encontramos en el documento RFC 6265 state management mechanism de abril del 2015

Ventajas de tener alojadas las cookies en tu navegador

Los ficheros o cookies proporcionan una navegación rápida, sencilla y personalizada, evitando que el usuario no vuelva a digitar las páginas que visita frecuentemente en vista de que él no se acuerde de dichas direcciones Web.[23]

Estas cookies son utilizadas para la realización de compras online. Si existe algún problema que impide terminar el proceso de transacción en línea, las cookies propias ayudarán a recordar los productos que el usuario tenía en su carrito de compras evitando que el usuario tenga que buscar los productos nuevamente.[23]

Desventajas de tener alojadas las cookies en tu navegador

El problema principal de las cookies reside en que poseen la capacidad de almacenar cualquier tipo de información de carácter sensible, en la cual proteger la privacidad del usuario se vuelve una tarea compleja en vista que ellos no poseen los conocimientos sobre la navegación anónima. Esto conlleva que esa información confidencial que almacenan pueda ser accedida por piratas informáticos con la finalidad de causar daño a su objetivo o en beneficio propio.[23]

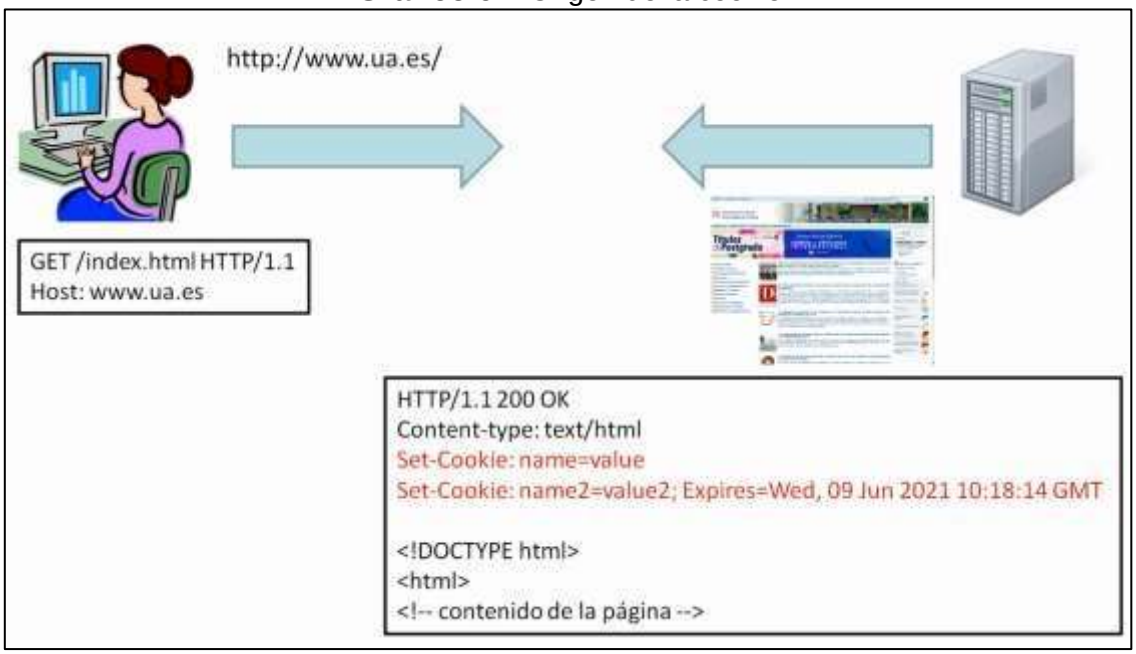
Estas cookies son creadas para detectar las páginas que visitan los usuarios durante la navegación por Internet, de este modo, aunque no tengan los datos personales, gracias a las pautas de navegación se puede deducir que la información de los usuarios se encuentra protegida.[23]

Como se envían las Cookies mediante el protocolo Http entre el cliente Y el servidor.

En primer lugar cuando un usuario quiere visitar una página web como por ejemplo **www.ua.es** el navegador se conecta al servidor web y la envía una petición http, luego el servidor web responde al navegador enviando una

respuesta http que contiene la página solicitada en una seria de líneas pidiendo al navegador que almacene dos cookies.

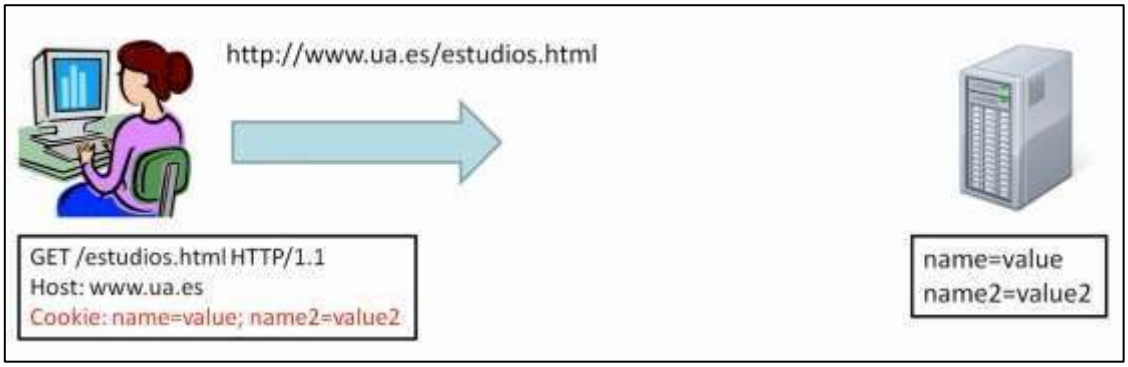
Gráfico 91 Origen de la cookie



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Cuando el usuario vuelve a visitar una página del mismo sitio web la petición que envía el navegador al servidor web incluirá las cookies que se hayan almacenado previamente, el navegador únicamente envía la pareja **nombre, valor,** el resto de atributos de la cookie no se envían, al recibir la petición el servidor web podrá leer las cookies y las podrá utilizar para crear la siguiente respuesta.

Gráfico 92 envío de cookies almacenadas



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Atributos de las Cookies.

Según la última especificación las cookies se componen de los siguientes atributos:

- **Una pareja nombre/valor:** es la que da la información de la cookie
- **Un dominio:** indica en que dominio se puede emplear la cookies, o a que dominio pertenece la cookie.
- **Una ruta:** limita el uso de la cookie a páginas que se encuentren en dicha ruta.
- **Fecha de caducidad o máxima edad:** indica hasta cuando la cookie es válida, es decir nos muestra la fecha de caducidad.
- **Una marca de solo conexión segura:** esto exige que la cookie sea enviada mediante un protocolo de encriptación.
- **Una marca de solo HTTP:** limita el uso de la cookie al protocolo HTTP.

Como se representan los atributos de una Cookie en un mensaje Http.

Aquí tenemos una directiva http **Set-Cookie** que es enviada por el servidor el cual ordena al navegador web que almacene esta cookie.

Gráfico 93 Cookie en un mensaje Http

```
Set-Cookie: ID=Gehwvyyb%20pnchyyb; Domain=docs.foo.com; Path=/privado; Expires=Wed, 13-Jan-2021 22:23:01 GMT; Secure; HttpOnly
```

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

En más detalle:

Gráfico 94 Cookie en un mensaje Http

```
Set-Cookie: ID=Gehwvyyb%20pnchyyb;
            Domain=docs.foo.com;
            Path=/privado;
            Expires=Wed, 13-Jan-2021 22:23:01 GMT;
            Secure;
            HttpOnly
```

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Atributos encontrados en la directiva http Set-Cookie

- Se encontró la pareja **Nombre/valor.**
- Se encontró el atributo **Domain,** el cual indica que esta cookie solo se puede utilizar en el dominio indicado.
- Se encontró el atributo **Path,** el cual limita el uso de esta cookie a páginas que se encuentren dentro del directorio o ruta **/privado.**
- Se encontró el atributo **Expires**, el cual indica que esta cookie caducara el 13 de enero del año 2021 a las 22:23:01.

- Se encontró el atributo **Secure,** el cual indica que esta cookie solo se tiene que ser enviada a través de una comunicación segura y encriptada como puede ser https.
- Por último el atributo **HttpOnly,** indica que esta cookie solo es accesible a través del protocolo http y no a través de otros métodos como puede ser Java Script.

Podemos ver que los dos últimos atributos **Secure, HttpOnly** no llevan valores.

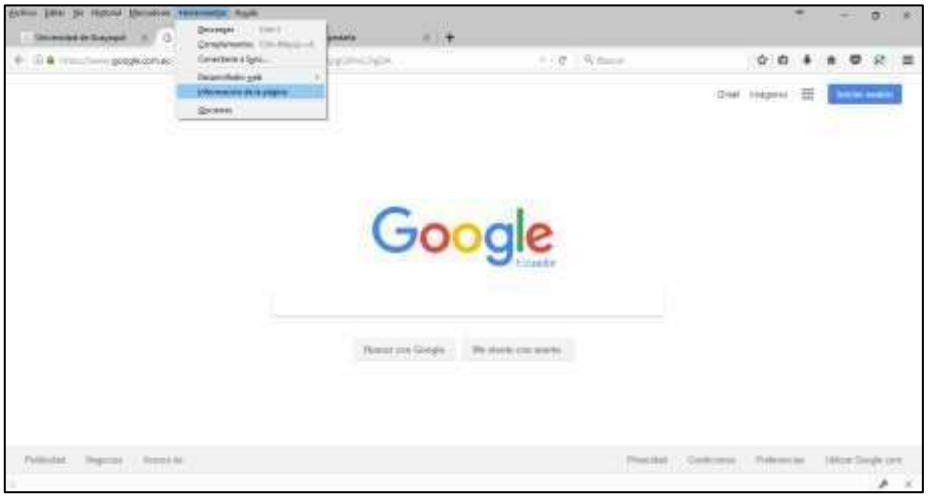
Hoy en día aunque no se tome en consideración la mayoría de los sitios web emplean cookies que almacenan todo tipo de información en los ordenadores.

Los navegadores modernos permiten visualizar las cookies que se emplean en un sitio web y si se quiere también permiten borrarlas, por ejemplo el buscador google emplea algunas cookies para almacenar información sobre las búsquedas que hayamos realizado y para almacenar las preferencias del usuario, sobre el idioma de búsqueda o el número de resultados a mostrar.

VISUALIZACION DE LAS COOKIES ALOJADAS EN EL NAVEGADOR MOZZILLA FIREFOX.

- Se selecciona en el menú la opción de Herramientas, clic en información de la página.

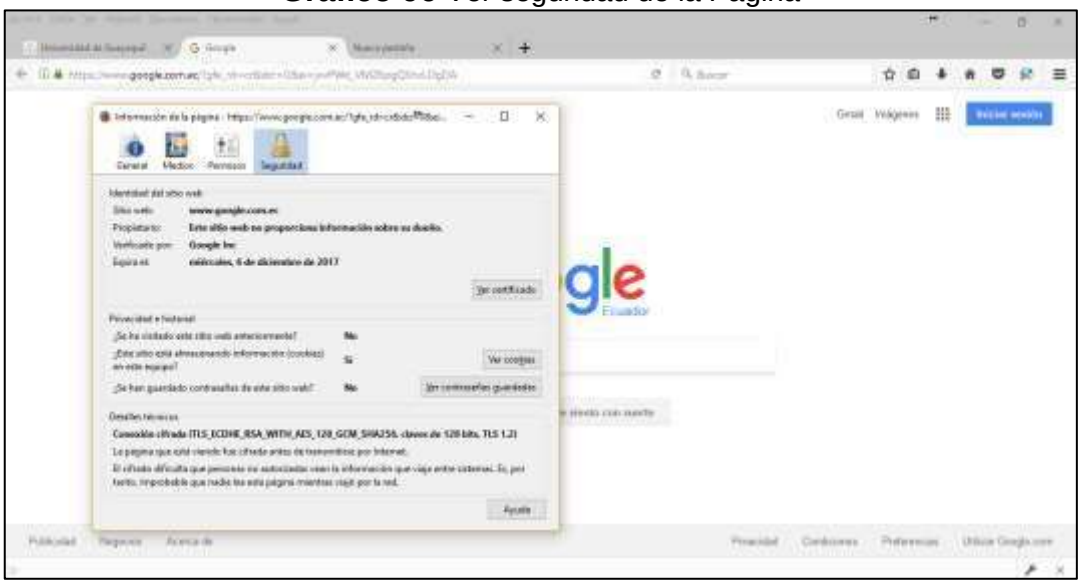
Gráfico 95 Visualización de las Cookies Mozilla Firefox



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- En la ventana que parece, ubicarse en la pestaña seguridad.

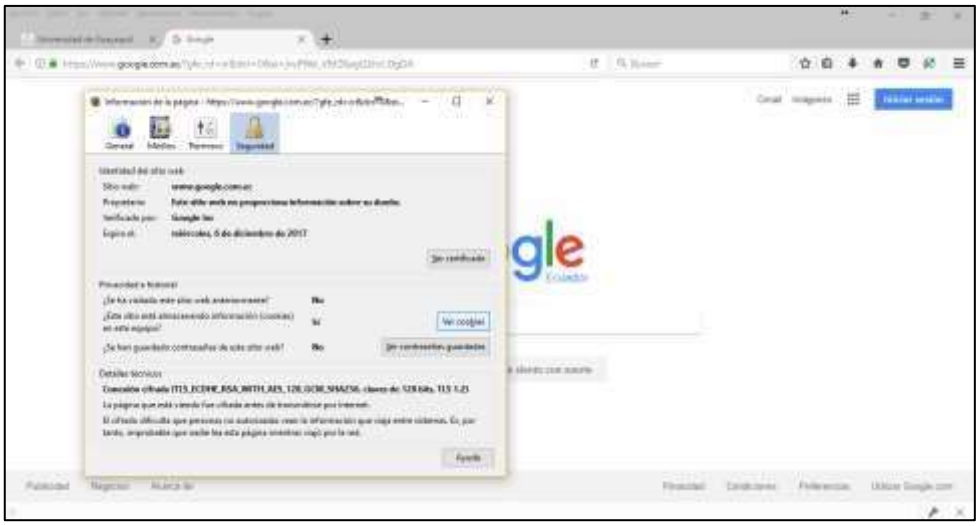
Gráfico 96 Ver seguridad de la Pagina



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Dar clic en el botón ver Cookies.

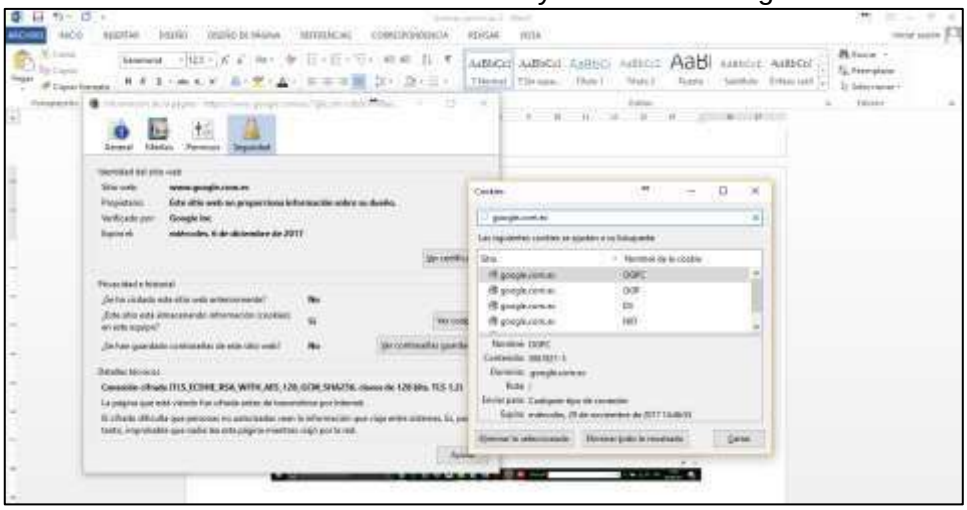
Gráfico 97 Visualización de las cookies



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Para cada cookie que se almacena se puede consultar sus atributos como dominio, ruta y fecha de caducidad que en este programa se llama expira.

Gráfico 98 Verificación de las cookies y los atributos según el dominio



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

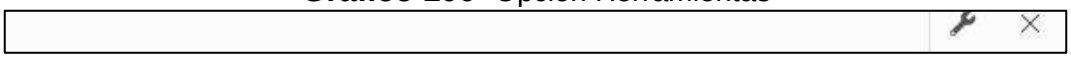
- Otra manera de visualizar las cookies activar la opción: Caja de Herramientas de desarrolladores.

Gráfico 99 Otra manera de visualizar las cookies

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

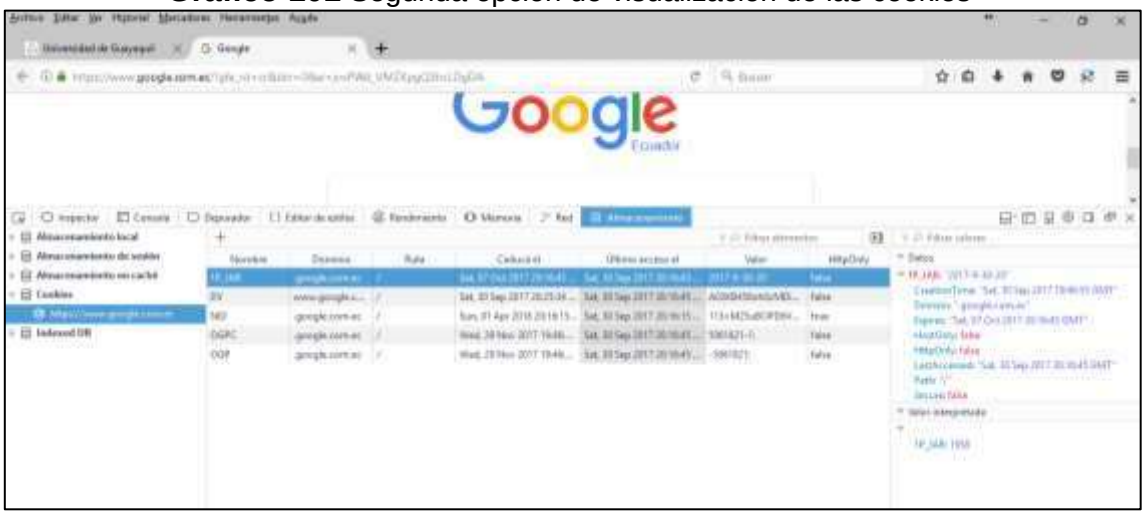
- Se activará en la parte inferior derecha una opción de llave, que al darle clic mostrará la información de las cookies almacenadas según su dominio.

Gráfico 100 Opción Herramientas



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 101 Segunda opción de visualización de las cookies

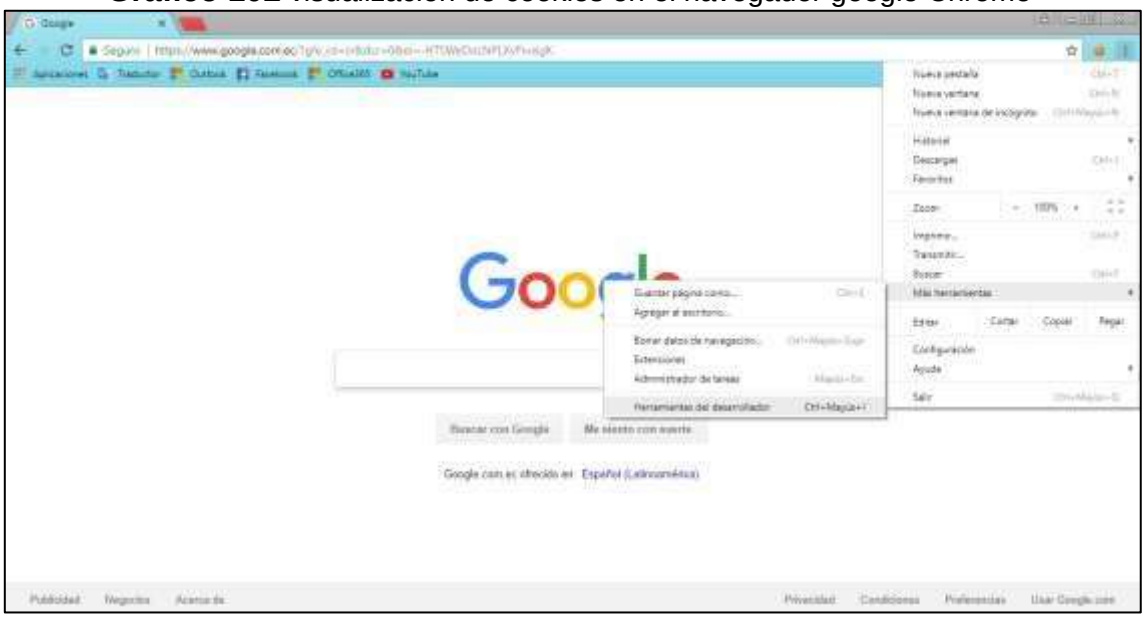


Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

VISUALIZACION DE LAS COOKIES ALOJADAS EN EL NAVEGADOR GOOGLE CHROME.

- Ubicarse en la opción Más herramientas, luego en la opción Herramientas del Desarrollador.

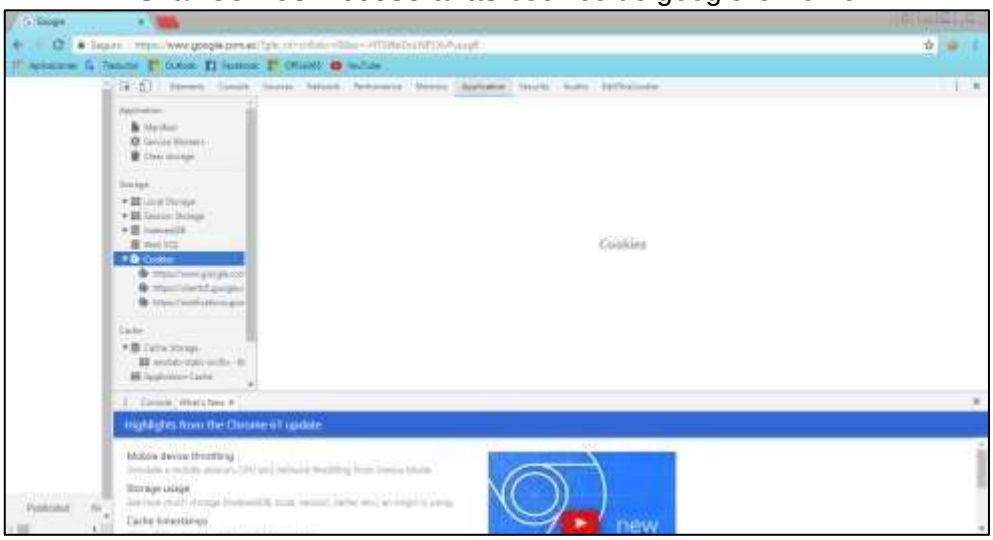
Gráfico 102 visualización de cookies en el navegador google Chrome



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

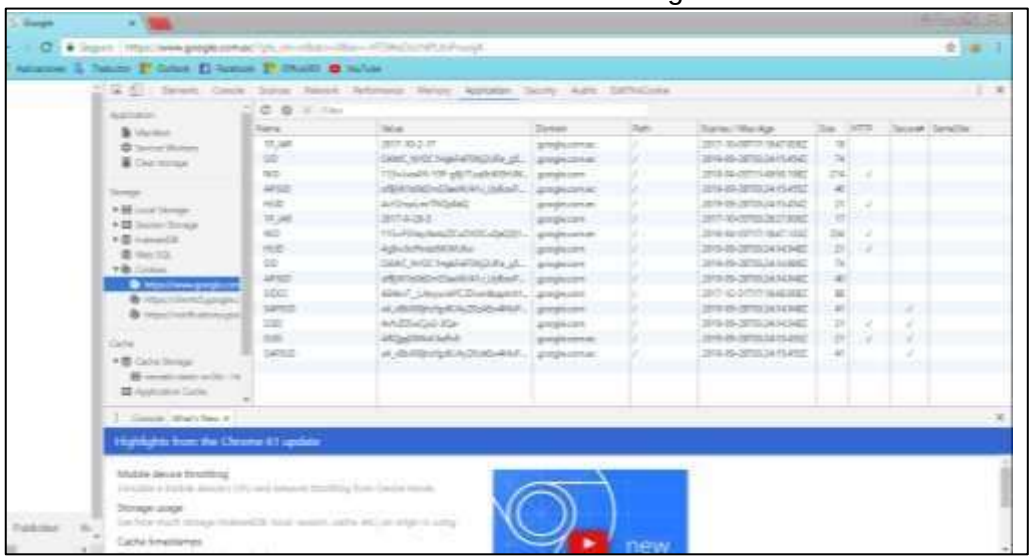
- Dar clic en el menú la opción Application y seleccionar la pestaña cookies y el dominio del cual se quiere ver la cookies.

Gráfico 103 Acceso a las cookies de google Chrome



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento.

Gráfico 104 Acceso a las cookies según el dominio



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

COMO DESACTIVAR EL USO DE COOKIES Y QUE BENEFICIO SE TIENE AL REALIZAR ESTE PROCESO

Beneficio

El beneficio de realizar este proceso es que al momento de no aceptar cookies en el navegador de internet no se expone la información de sesión en donde puede ser espiada y capturada por piratas informáticos que realizan ataques asociados al robo de cookies.

Desventaja

No se monitoreara el sitio web y no se alertara errores que sufra dicho sitio.

DESACTIVAR EL USO DE COOKIES, MOZILLA FIREFOX

- Dar clic en herramientas y luego en opciones.

Gráfico 105 Desactivar Cookies Navegador Mozilla firefox

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

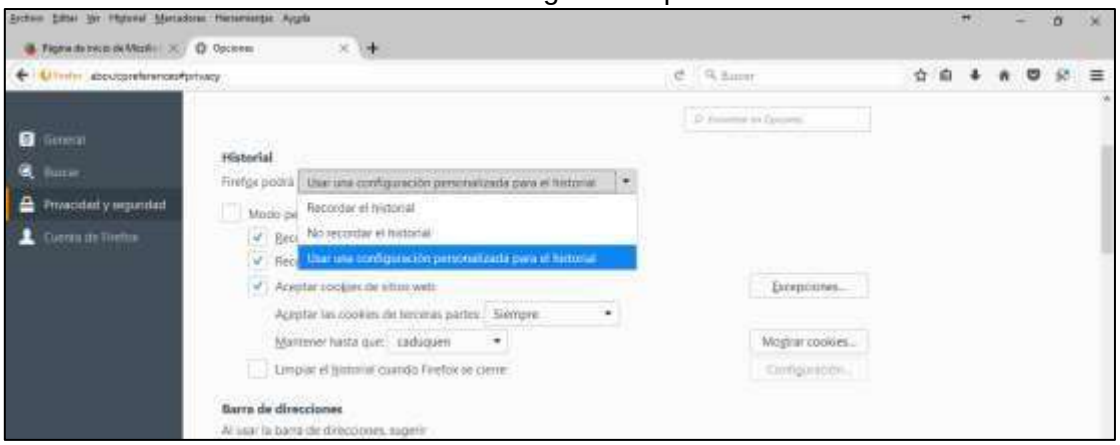
- Dar clic en la opción **Privacidad y seguridad**

Gráfico 106 Privacidad y Seguridad del navegador

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Luego se ubica en la opción Historial y después en el mensaje en Firefox podrá se escoge la opción Usar una configuración personalizada para el historial.

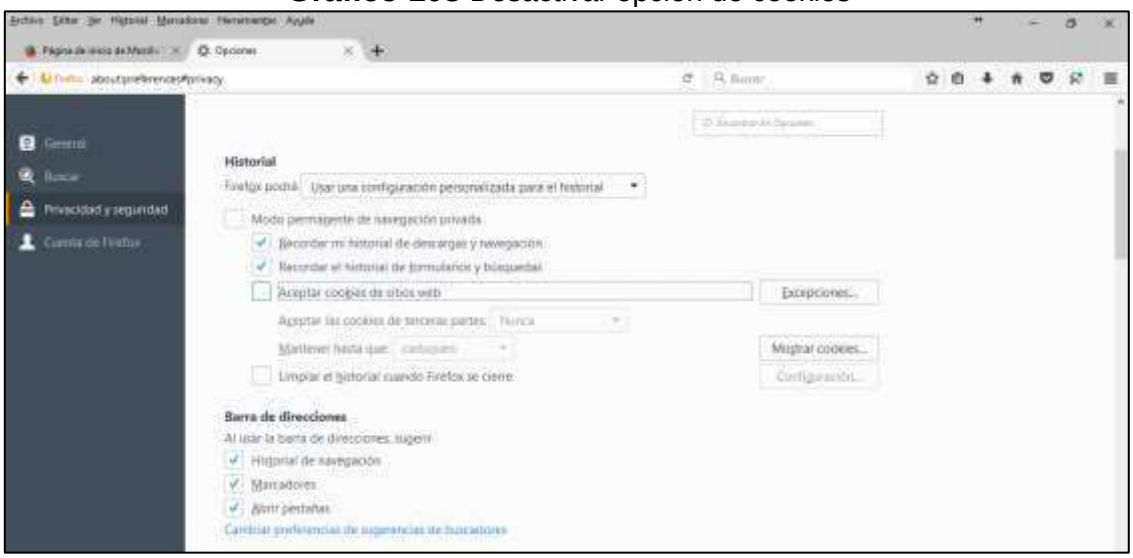
Gráfico 107 Configuración personalizada



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Desactivamos la casilla de Aceptar cookies de sitios web.

Gráfico 108 Desactivar opción de cookies



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento.

DESACTIVAR EL USO DE COOKIES, GOOGLE CHROME.

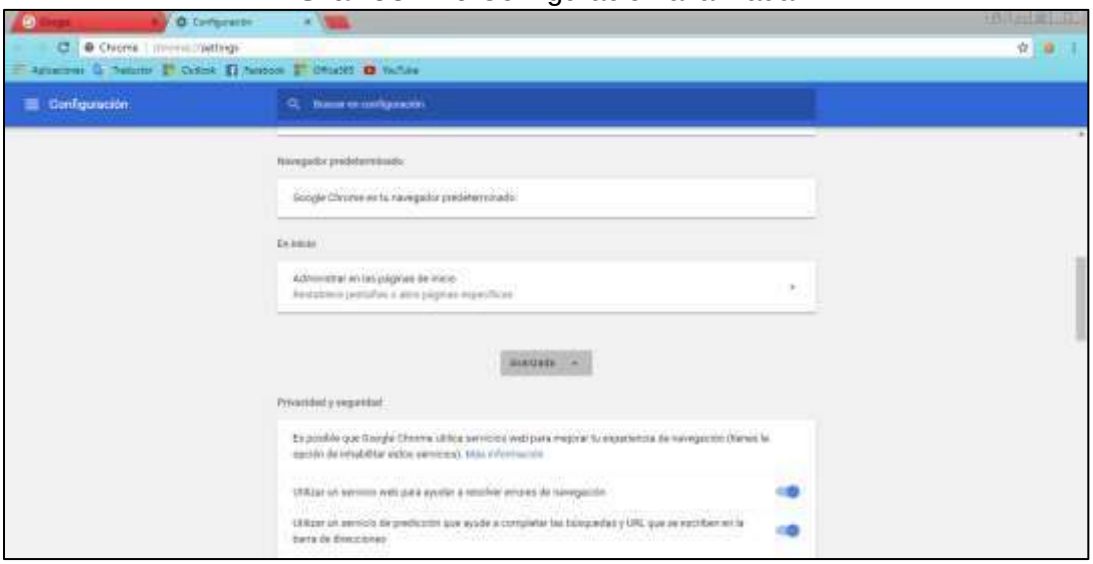
- Menú de opciones, Configuración

Gráfico 109 Desactivar cookies en Google Chrome

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Se da clic en Configuración Avanzada.

Gráfico 110 Configuración avanzada



Fuente: Trabajo de Investigación **Autores:** Simón Ballesteros – Francisco Sarmiento.

- Se da clic en configuración de contenido, luego en Cookies.

Gráfico 111 Configuración de contenido

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Se desactiva la opción permitir que todos los sitios guarden y lean datos de cookies

Gráfico 112 Desactivar la opción de cookies

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 113 Configuración de cookies

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

LIMPIEZA DEL HISTORIAL DE NAVEGACION

¿ES RECOMENDABLE LIMPIAR EL HISTORIAL DE NAVEGACION?

Si Fundamentalmente, para proteger la privacidad sobre todo si se accede a Internet de forma puntual en un ordenador que no es el nuestro o en un computador público como, por ejemplo, en una biblioteca, cyber café o demás lugares. Eliminar el historial de navegación es una tarea sencilla que solo lleva unos pocos segundos y permite borrar el rastro de las búsquedas. Pero limpiar el historial de navegación es especialmente de gran importancia y aconsejable si se ha rellenado algún formulario con los datos personales desde una PC que no es la propia, se debe tener en mucha consideración debido a que la información de carácter sensible puede verse afectada por atacantes maliciosos, además, en dicho formulario si se ha realizado una compra e introducido datos bancarios, en ese caso, se debe borrar el historial del navegador de forma inmediata para que esos datos que fueren ingresados para efectuar transacciones en línea no queden almacenados en él y cualquier persona desconocida pueda acceder a ellos con el fin de beneficiarse económicamente o causar daño a su objetivo.

¿LAS COOKIES SE ELIMINAN AL BORRAR EL HISTORIAL DEL NAVEGADOR WEB?

La respuesta es SI

¿CÓMO BORRAR EL HISTORIAL DE NAVEGACIÓN EN GOOGLE CHROME?

Al tener acceso a internet y utilizar el navegador Google Chrome, se debe seguir los siguientes pasos, para la respectiva limpieza del historial de dicho navegador:

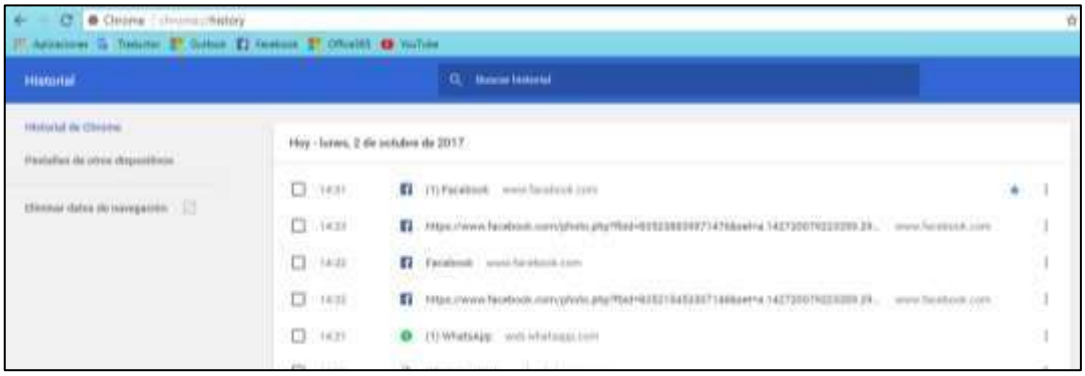
- En el primer paso se accede al menú que se ubica en la parte superior derecha de Chrome representado con un icono de tres puntos.
- Después, dar clic en el apartado Historial.

Gráfico 114 Apartado del Historial

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Por último pulsar clic en la opción eliminar

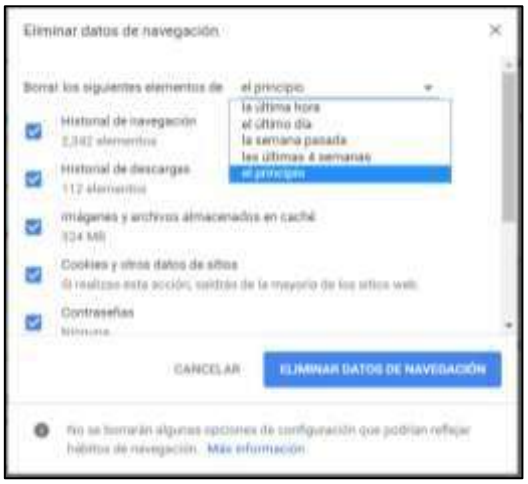
Gráfico 115 Eliminar cookies



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Luego escoger la opción eliminar desde el principio marcando todas las casillas.

Gráfico 116 Opción de eliminar cookies



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

¿CÓMO BORRAR EL HISTORIAL DE NAVEGACIÓN EN MOZZILA FIREFOX?

Al tener el acceso a internet y se utiliza el navegador Mozilla Firefox, se debe seguir los siguientes pasos para limpiar el historial de este navegador:

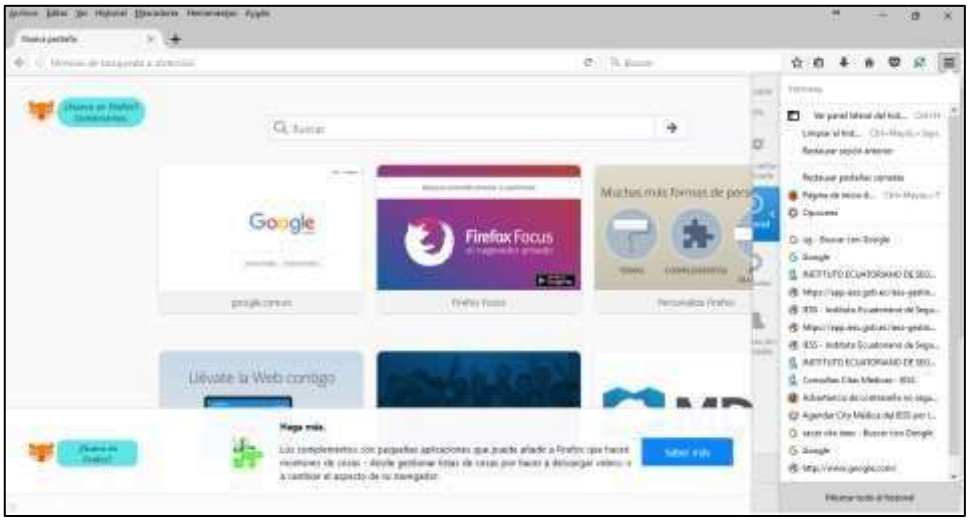
- Acceder al menú que está representado en la parte superior derecha de Mozilla Firefox con un icono de tres líneas cortas.
- Pulsar en el apartado Historial.

Gráfico 117 Apartado del Historial en Firefox

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Seleccionar la opción mostrar todo el historial.

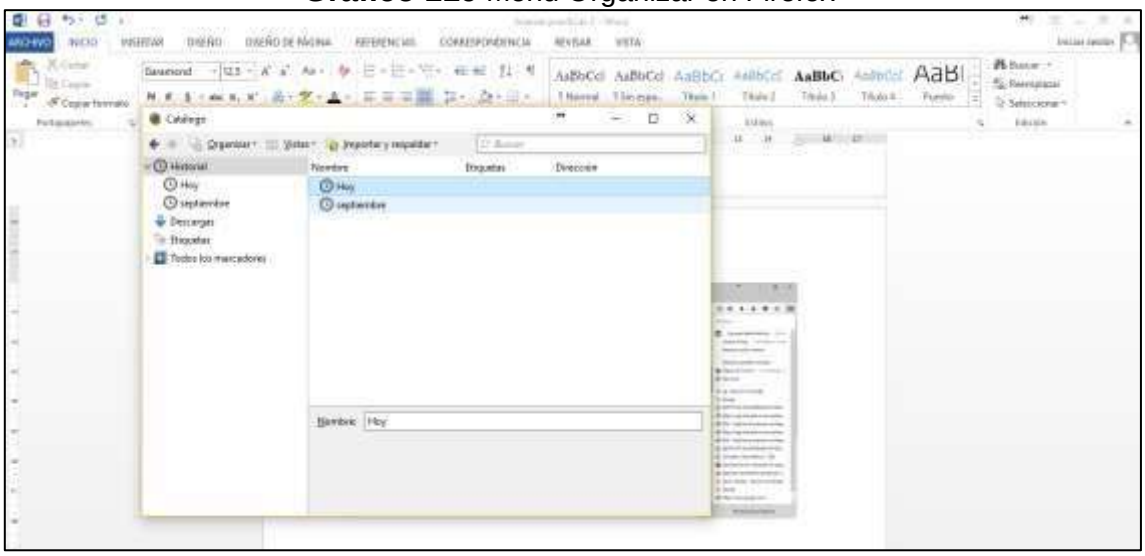
Gráfico 118 Mostrar el Historial en Firefox



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Por último se debe dirigir al menú organizar.

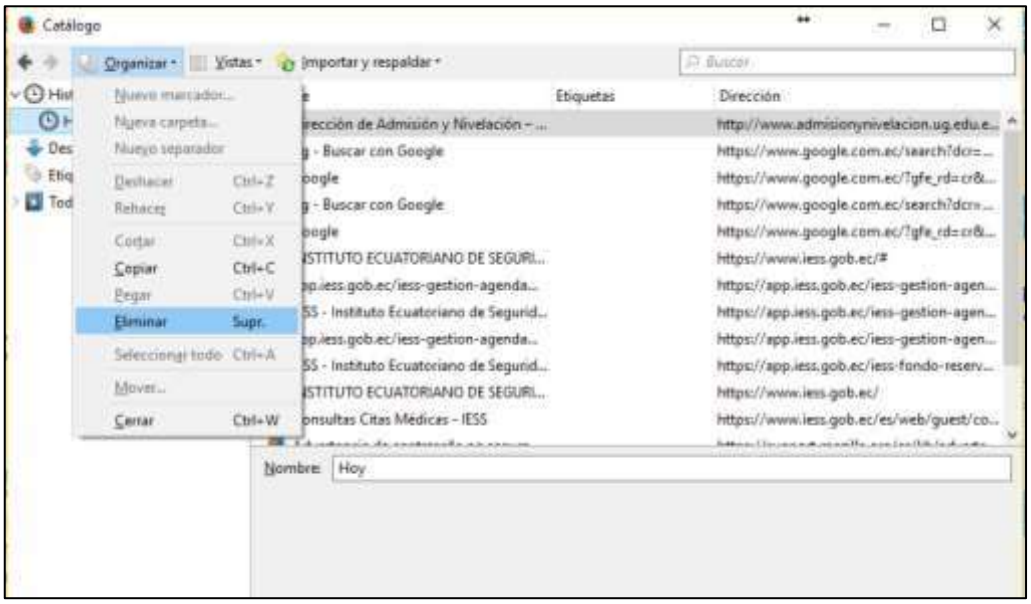
Gráfico 119 Menú Organizar en Firefox



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

- Escoger la opción eliminar.

Gráfico 120 Eliminar cookies en Firefox



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

USO DE LA NAVEGACION INCOGNITA

Entre las fórmulas más eficientes y útiles para lograr el objetivo planteado cabe mencionar la posibilidad que ofrecen los actuales navegadores web de permitir consultar Internet en modo privado o incógnito.

Mediante esta práctica funcional, los usuarios de la Red tienen la opción de navegar de forma mucho más segura y con mayor privacidad, ya que este modo evita que las páginas que visitamos sean guardadas en el historial de búsqueda del navegador y por tanto impide que se muestren.

Además, con el modo privado conseguimos que cuando cerramos la ventana, las cookies, contraseñas guardadas y otros datos locales de la sesión sean eliminados de forma automática. El único dato que se guardará serán los sitios favoritos que almacenemos y los archivos que descarguemos.

Navegar en este modo puede tener muchos usos prácticos. La más evidente, que permite acceder a Internet evitando que nadie acceda al equipo propio en donde pueda saber qué contenidos hemos estado consultando. Pero más allá de esto, existen también otras ventajas en el sentido del modo incógnito en la cual es una fantástica solución, por ejemplo, para acceder a Internet en un ordenador público o ajeno, de manera que las contraseñas que usemos para acceder al e-mail o a las redes sociales sean eliminadas al cerrar la sesión.

Por otra parte, navegar en modo incógnito también permitirá por ejemplo abrir de forma simultánea diferentes perfiles en cuentas de correo electrónico o redes sociales, algo que no es posible cuando navegamos en modo normal. De esta forma, podremos navegar en la cuenta de Gmail de la empresa a la que prestamos servicios y a la vez consultar también la propia cuenta en forma particular, aunque también sea del servicio de email de Google.

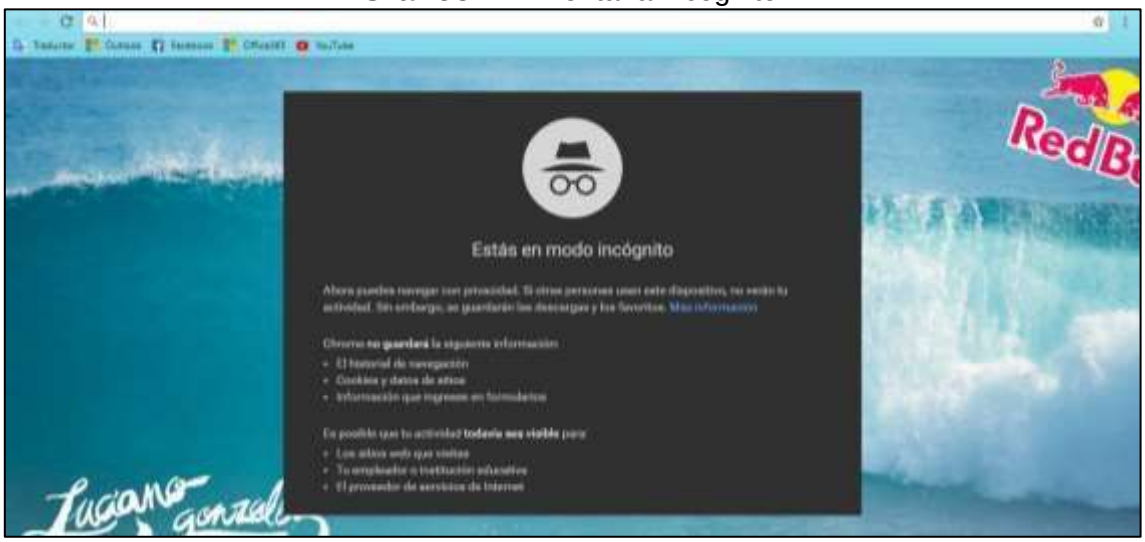
NAVEGACION INCOGNITA EN GOOGLE CHROME.

- **Presionar** Ctrl-Mayúsculas+N o seleccionar Nueva ventana de incógnito en las opciones que se despliegan al pulsar en el botón de menú representado por tres rayas horizontales en la parte superior derecha.

Gráfico 121 Nueva venta en incognito

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 122 Ventana incognito



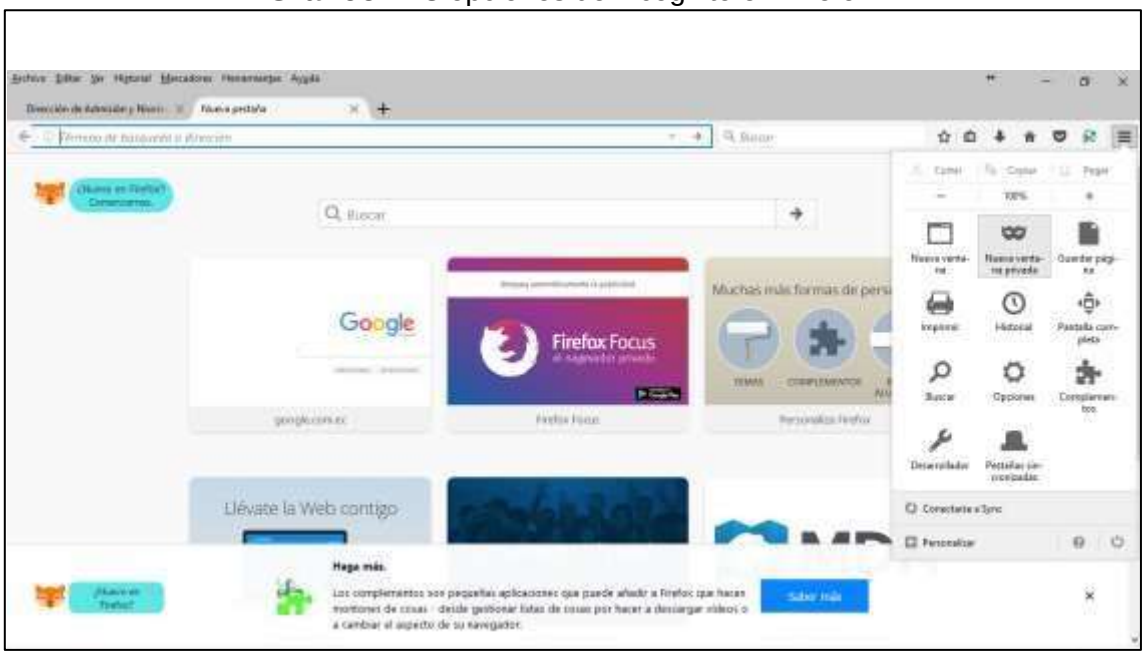
Fuente: Trabajo de Investigación

Autores: Simón Ballesteros – Francisco Sarmiento

NAVEGACION INCOGNITA EN MOZILLA FIREFOX.

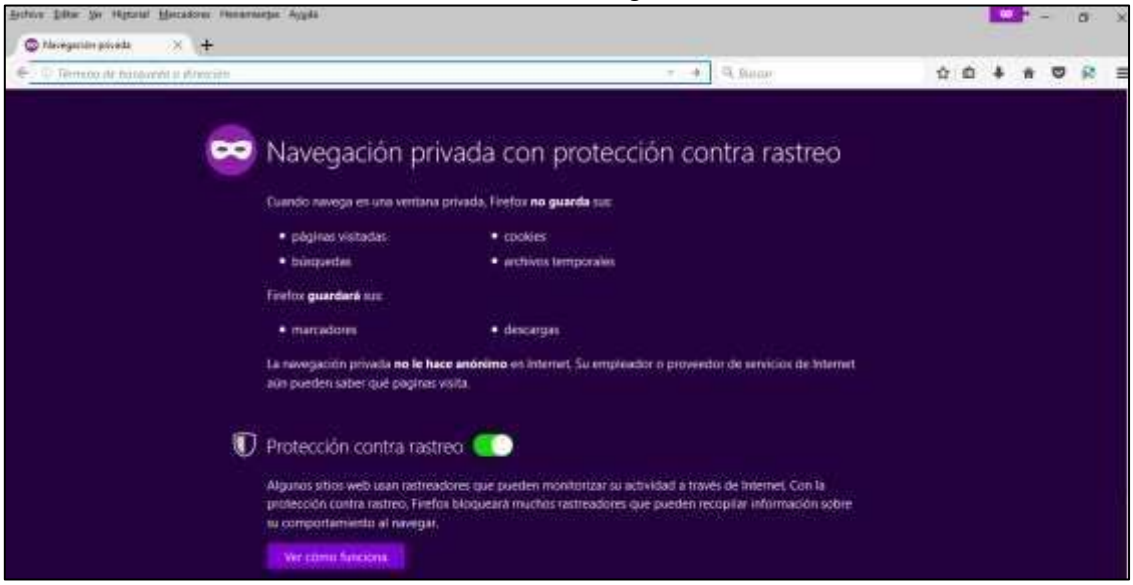
Presionar Ctrl+Mayúsculas+P o seleccionando Nueva ventana privada en las opciones que se despliegan al pulsar en el botón de menú representado por tres rayas horizontales en la parte superior derecha

Gráfico 123 opciones de incognito en Firefox



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Gráfico 124 Modo incognito en Firefox



Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

ALMACENAR CONTRASEÑAS EN EL NAVEGADOR

¿Es una práctica segura almacenar contraseñas en el navegador?

Los usuarios que hacen uso del internet, en algún momento, han visualizado el característico mensaje de ¿quieres que el navegador recuerde tu contraseña?,

dicho mensaje aparece por pantalla, generalmente en la parte superior de la pantalla, tras registrarnos en algún servicio web.

Esta práctica, puede ser muy peligrosa si compartimos nuestro ordenador con otros usuarios, ya que cualquier usuario podría acceder a ellas o a la vez sufrir ataques de intrusión que podrían facilitar el robo de las contraseñas.

MOZILLA FIREFOX

Gráfico 125 Opciones de almacenar contraseñas en Firefox

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Como eliminar contraseñas en el caso de que alguna se halla guardado.

1. Abrir Firefox.
2. Haz clic en Herramientas y luego en Opciones.
3. Seleccionar el icono Seguridad.
4. Pulsar sobre Contraseñas guardadas.
5. Hacer clic en Eliminar.

Gráfico 126 Eliminación de contraseñas en Firefox

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

GOOGLE CHROME

Gráfico 127 Opciones de almacenamiento de contraseñas en Google Chrome

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento

Como eliminar contraseñas en el caso de que alguna se halla guardado.

1. Abrir Chrome.
2. Hacer clic en el icono del menú de Chrome.
3. Seleccionar Configuración.
4. Pulsar sobre el enlace Mostrar opciones avanzadas en la parte inferior de la página.
5. Desplazar con el cursor a la sección Contraseñas y formularios.
6. Hacer clic en el enlace Administrar contraseñas guardadas.
7. Eliminar las contraseñas memorizadas.

Gráfico 128 Eliminación de contraseñas en Google Chrome

Fuente: Trabajo de Investigación
Autores: Simón Ballesteros – Francisco Sarmiento