UNIVERSIDAD NACIONAL DE LOJA

Facultad de la Energía, las Industrias y los Recursos Naturales no Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

"Revisión sistemática de literatura: Análisis de la Seguridad Informática en los sistemas VoIP"

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

AUTOR:

Lauro Ibán Japa Ávila

DIRECTOR:

Ing. Ángel Freddy Ganazhapa Malla, Mg. Sc.

LOJA - ECUADOR

2019

Certificación del director

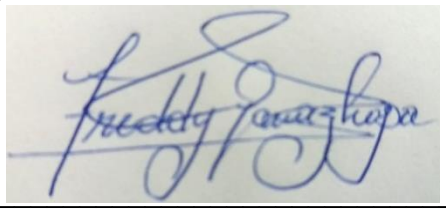
Ing. Ángel Freddy Ganazhapa Malla, Mg. Sc.
DOCENTE DE LA CARRERA DE INGENIERÍA EN SISTEMAS, DE LA FACULTAD DE ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES DE LA UNIVERSIDAD NACIONAL DE LOJA.

CERTIFICA:

Haber asesorado y revisado detenida y minuciosamente durante todo su desarrollo, el proyecto de titulación, titulado: **"REVISIÓN SISTEMÁTICA DE LITERATURA: ANÁLISIS DE LA SEGURIDAD INFORMÁTICA EN LOS SISTEMAS VOIP".** Realizado por el postulante Lauro Ibán Japa Ávila, cumple con los requisitos establecidos por las normativas para la graduación en la Universidad Nacional de Loja.

Por lo tanto, autorizo proseguir los trámites legales pertinentes para su presentación y defensa.

Loja, 08 de agosto de 2019

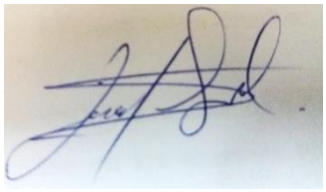


Ing. Ángel Freddy Ganazhapa Malla, Mg. Sc.
DIRECTOR DE TESIS

Autoría

Yo **LAURO IBÁN JAPA ÁVILA,** declaro ser autor del presente trabajo de tesis y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi tesis en el Repositorio Institucional - Biblioteca Virtual.

Firma: 

Cedula: 190561323

Fecha: 2/10/2019

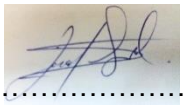
CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTOR, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.

Yo **LAURO IBÁN JAPA ÁVILA**, declaro ser auto de la tesis titulada "**REVISIÓN SISTEMÁTICA DE LITERATURA: ANÁLISIS DE LA SEGURIDAD INFORMÁTICA EN LOS SISTEMAS VoIP**", como requisito para optar al grado de **INGENIERO EN SISTEMAS;** autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos, muestre al mundo la producción Intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional:

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de la tesis que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los dos días del mes de octubre del dos mil diecinueve.



Firma: …….
Autor: Lauro Ibán Japa Ávila
Cedula: 1900561323
Dirección: yacuambi (Quito y Zamora)
Correo Electrónico: lauroj_99@yahoo.es
Teléfono: 072194064 **Celular:** 0991553628

DATOS COMPLEMENTARIOS

Director de Tesis: Ing. Ángel Freddy Ganazhapa Malla, Mg. Sc.
Tribunal de Grado: Ing. Valeria del Rosario Herrera Salazar, Mg. Sc.
Ing. José Oswaldo Guamán Quinche, Mg Sc.
Dr. Roberth Gustavo Figueroa Díaz, Mg. Sc.

Agradecimiento

Quiero dejar presente mi agradecimiento más sincero a las autoridades y docentes de la Universidad Nacional de Loja y de la Carrera de Ingeniería en Sistemas quienes con profesionalismo han compartido sus conocimientos, colaborado personalmente y facilitado las instalaciones para la realización del presente trabajo.

También agradecer al director del presente trabajo de titulación, Ing. Ángel Freddy Ganazhapa Malla, por su dedicada dirección y brindado una excelente asesoría durante el desarrollo del presente trabajo.

EL AUTOR

Dedicatoria

El presente trabajo de graduación dedico con todo cariño a mis queridos padres, hermanos y amigos; que incondicionalmente, me han guiado y apoyado aún en las circunstancias más difíciles, y me motivan a seguir superándome cada día más, a quienes les debo todo mi esfuerzo y dedicación.

.

Lauro Ibán

Índice de Contenidos

Índice General

Índice de Figuras

Índice de Tablas

a. Título

“**Revisión sistemática de literatura: Análisis de la Seguridad Informática en los sistemas VoIP**”

b. Resumen

Uno de los mayores temas de interés en la informática es el referente a la seguridad de la información, es por este motivo que la seguridad en los sistemas de comunicación VoIP asume un rol fundamental para en lo posible mitigar e inhibir ciertas vulnerabilidades.

En el presente trabajo investigativo se ha realizado una revisión sistemática de literatura sobre el tema de seguridad en los sistemas de comunicación basadas en el protocolo VoIP, para lo cual se ha hecho uso de una metodología base propuesta por Bárbara Kitchenham, con algunas modificaciones planteadas por el Departamento de Informática de la Universidad Castilla-La Mancha, para revisiones sistemáticas en trabajos de fin de carrera del campo Informático.

Se ha realizado una selección minuciosa de artículos científicos sobre seguridad VoIP, de acuerdo con parámetros establecidos tales como año de publicación, relevancia del tema, entre otros; luego se realizó un análisis comparativo y extracción de las conclusiones más destacadas de cada uno de ellos, con la finalidad de obtener una síntesis detallada de los artículos seleccionados.

Finalmente se han presentado los resultados del análisis indicando las vulnerabilidades más recurrentes existentes en los sistemas VoIP; así como los diferentes tipos de amenazas y ataques más frecuentes.

Summary

One of the topics of greatest interest in information technology is information security, it is for this reason that security in VoIP communication systems assumes a fundamental role in the possible mitigation and inhibition of certain vulnerabilities.

In this research work a systematic review of literature on the topic of safety in communication systems based on the VoIP protocol has been carried out, for which we have made use of a base methodology proposed by Barbara Kitchenham, with some modifications proposed by the Department of Informatics of the University Castilla-La Mancha, for systematic reviews in end-of-career assignments in the computer field.

A careful selection of scientific articles on VoIP security has been made, according to established parameters such as year of publication, relevance of the topic, among others; a comparative analysis was then carried out and the most outstanding conclusions were drawn from each of them, in order to obtain a detailed synthesis of the selected articles.

Finally, the results of the analysis have been presented, indicating the most recurrent vulnerabilities existing in VoIP systems, as well as the different types of threats and most frequent attacks.

c. Introducción

Debido a la gran utilización de los servicios VoIP, las vulnerabilidades se han hecho más evidentes; los problemas que presentan las redes VoIP son en gran medida similares a los problemas de seguridad de las redes de datos. Estas vulnerabilidades implican escaneos a dispositivos SIP (Session Initiation Protocol), denegación de servicios (DoS), intercepción de llamadas, entre otros [1].

Para garantizar la calidad de la comunicación y ofrecer a los usuarios la certeza de intercambiar información de una manera segura, se busca cada vez nuevos mecanismos que permitan contrarrestar estas amenazas. En este contexto, el presente trabajo de investigación pretende brindar información a aquellas personas interesadas en la seguridad de los sistemas VoIP.

La Revisión Sistemática de Literatura se ha realizado siguiendo la metodología propuesta por Bárbara Kitchenham, la cual ha guiado en todas las etapas desde la selección de documentación bibliográfica sobre seguridad de redes VoIP, continuando con la realización de un estudio comparativo, hasta obtener una síntesis de la información más relevante del tema de seguridad VoIP.

d. Revisión de Literatura

1. Comunicación VoIP

El protocolo VoIP (Voice over Internet Protocol) es un método para hacer llamadas telefónicas por Internet o a través de redes privadas. Las llamadas tradicionales deben atravesar una serie de conmutadores y circuitos, que son propiedad de las compañías telefónicas, que controlan el proceso y las tarifas [2]. Esta tecnología une dos mundos: la transmisión de voz y la de datos [3].

La tecnología VoIP transporta la voz y datos, previamente procesada, encapsulándola en paquetes para enviar a través de la infraestructura de Internet. Con esto se consigue una única red homogénea a través del cual se puede enviar todo tipo de información ya sea voz, video o datos. VoIP es una tecnología insegura por estar basada en el protocolo IP. Considerando que en cada una de las capas del modelo de red se comparte voz y datos, las debilidades de cada nivel es una posible vulnerabilidad que puede afectar la transmisión VoIP [3].

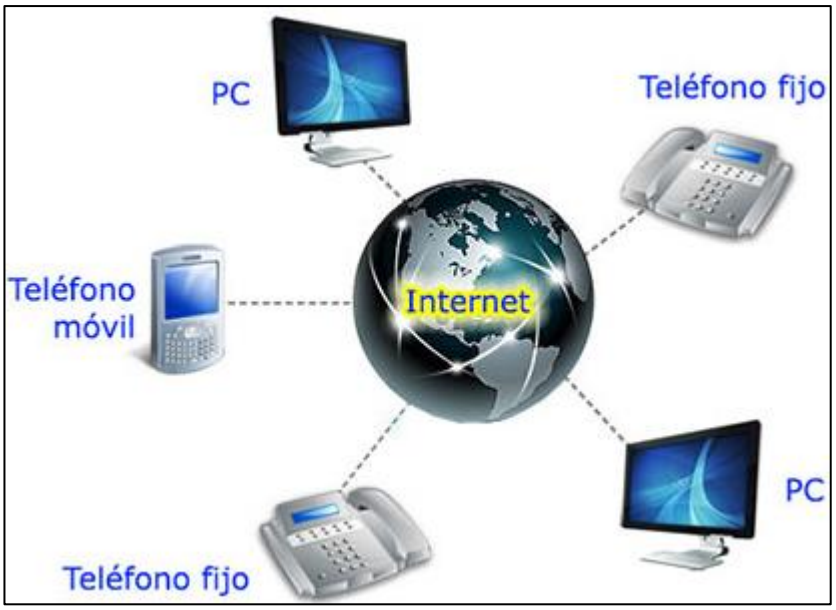


Figura 1. Esquema de comunicaciones basadas en VoIP [3].

El uso de VoIP permite, tanto a empresas como a usuarios particulares, lograr un considerable ahorro de costos, especialmente en llamadas de larga distancia [2].

Desde el punto de vista técnico, VoIP es un método de comunicación que emplea las normas H.323 o SIP (Session Initiation Protocol), ambas ampliamente difundidas. Las dos se encargan de enrutar conversaciones de voz a través de Internet o de redes basadas en IP y definen protocolos inspirados en los sistemas telefónicos tradicionales.

Los protocolos de señalización reemplazan las funciones de las centralitas privadas ordinarias PBX (Private Branch Exchange) y funcionan en servidores PBX IP con software de aplicaciones, como Elastix, Asterisk, Cisco Call Manager, entre otros. El segundo tipo, los protocolos multimedia, definen los protocolos utilizados entre dos endpoints o dispositivos telefónicos VoIP. Se han encontrado vulnerabilidades de VoIP en el software de gestión de llamadas, los protocolos de señalización y multimedia y en los propios dispositivos telefónicos [2].

En la telefonía VoIP se utiliza un IP PBX, lo que significa que es un servidor que se ejecuta en una computadora.

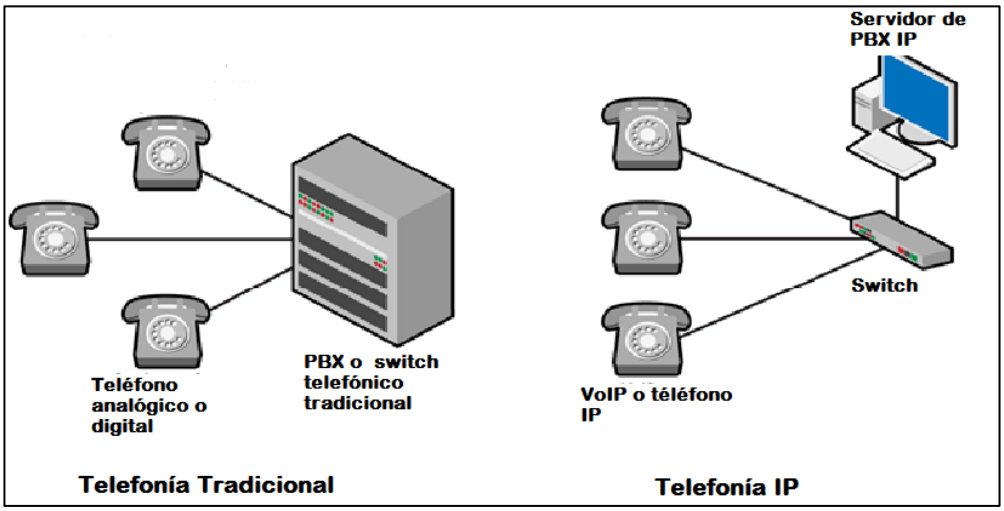


Figura 2. Telefonía tradicional y telefonía IP [3].

También vale la pena mencionar que, dado que el Protocolo de Internet puede ejecutarse y funciona en casi todos los tipos de arquitectura de comunicación de capa baja, la Voz sobre IP también puede hacerlo [4].

1.1. Procesos de la comunicación VoIP

El proceso de la comunicación VoIP consta de la ejecución de los tres procesos siguientes [5]:

1.1.1. Señalización

La operación de señalización se encarga de establecer y finalizar las llamadas. El proceso de señalización es el encargado de administrar ciertas funcionalidades del sistema, como la transferencia de llamadas, desvío a buzón de voz, llamadas en espera, entre otros. Los protocolos de señalización más utilizados son: Session Initial Protocol (SIP), Inter Asterisk eXchange (IAX2) y H.323. También, existen protocolos propietarios tales como SCCP (Skinny Call Control Protocol) de Cisco, MGCP (Media Gateway Control Protocol), entre otros.

1.1.2. Transporte y Codificación

Una vez establecida la llamada, la voz codificada en formato digital se transmite en un flujo de paquetes, de manera segmentada. Recibidos los paquetes, deben reordenarse (el protocolo IP no garantiza la entrega de paquetes de forma ordenada) y decodificarse (transformarse del formato digital al formato analógico, de manera que permita reproducir la información de audio mediante un altavoz). El protocolo encargado del transporte y codificación es Real-time Transfer Protocol (RTP), aunque el protocolo IAX2 incluye también este proceso como una de sus tareas, a través de mini frames, ya que IAX2 es especialmente un protocolo de señalización.

1.1.3. Control de medios (Gateway control):

Una comunicación VoIP puede ser dirigida hacia una red telefónica convencional, de manera que los paquetes de voz codificados deben transportarse a través de la red telefónica tradicional hasta llegar al receptor. Para esto, los paquetes de voz deben ser traducidos al formato soportado por la telefonía tradicional. Los gateways son los dispositivos encargados de esta traducción. Se ejecuta un proceso denominado control de medios para decidir el gateway a utilizarse.

Generalmente los protocolos de control de medios usados son MGCP (Media Gateway Control Protocol) y Megaco (Media Gateway Control).

1.2. Componentes de la comunicación VoIP

Una red VoIP abierta posee los siguientes componentes [3]:

1.2.1. LAN-WAN

El principal componente es la infraestructura de red conformada por todos los componentes necesarios como: Switch con soporte de VLAN (802.1 q) y QoS (802.1 p). WAN con soporte QoS.

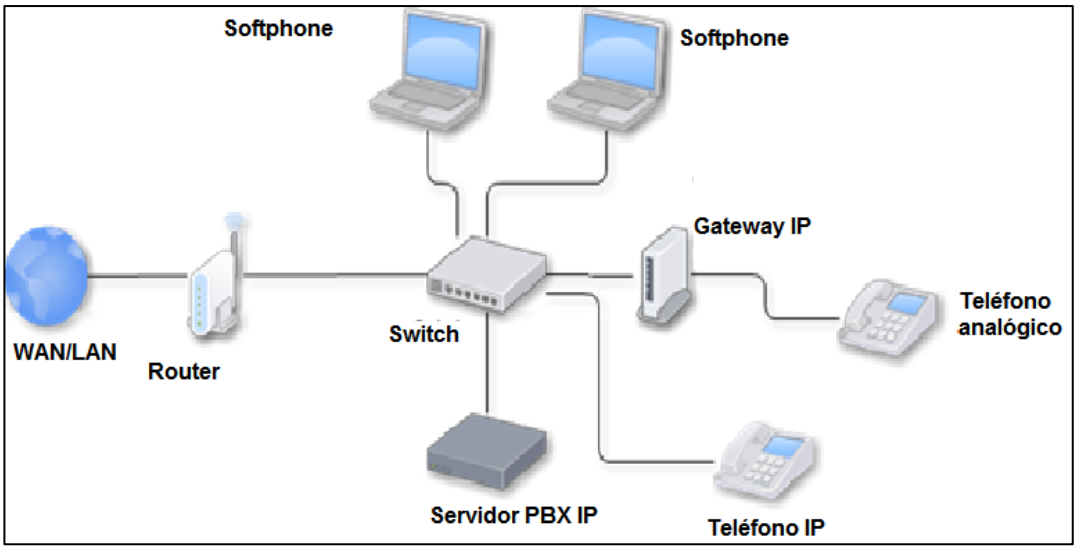


Figura 3. Compontes de un sistema VoIP [3].

1.2.2. IP-PBX

Es el encargado de administrar las llamadas entrantes, salientes e internas con autonomía sobre cualquier otra central telefónica. Provee de contestadoras automáticas, buzón de voz, entre otros servicios sin costo para la red privada de telefonía.

Un IP-PBX puede ser un hardware, pero estas tareas también pueden ser desempeñadas por software, como por ejemplo Elastix, Asterisk, entre otros.

1.2.3. Gateway IP

Sistema que permite la integración con elementos de telefonía tradicional (PBX o Líneas RTB). Generalmente las pasarelas son dispositivos de hardware con un adaptador que permita conectarse entre la red telefónica convencional y las redes VoIP; además, facilitar que los terminales pertenecientes a otro tipo de redes puedan interoperar adecuadamente [5].

1.2.4. Terminales

Son llamados también agente o cliente. Puede ser dispositivos hardware o también un software. En hardware se puede utilizar un teléfono IP con soporte SIP o H323 o un teléfono analógico con un adaptador que permita conectar a la red IP. También se puede utilizar cualquier aplicación (softphone) que se ejecuta en un computador y emule a un teléfono [5].

1.2.5. Controlador de medios (Media Gateway Controller o MGC)

Conocido también con el nombre de softswitch. Es un componente de software, que generalmente viene incorporado como funcionalidad en los gateways y permite configurar un gateway maestro que pueda gestionar un conjunto de (gateways) esclavos.

1.2.6. Guardián (Gatekeeper)

Es un software capaz de funcionar en diferentes sistemas operativos y es el encargado del control del procesamiento de las llamadas en redes que utilizan H323, acortando el ancho de banda que puede utilizar una llamada e incluso puede controlar el horario en que pueden realizar dichas llamadas. Un gatekeeper funciona solamente para el protocolo de señalización H323, ya que otros protocolos de señalización tienen sus equivalentes como el router SIP. Para garantizar un balance de carga o redundancia pueden existir varios guardianes.

1.2.7. Unidad de Control Multipunto (MCU)

Es un dispositivo de hardware o software que permite las conexiones multipunto en la red. Es decir, permite las llamadas de audio y video a través de la red VoIP. Está conformada de dos partes: el procesador multipunto (MP) que es el encargado de realizar las funciones de combinación de medios (audio, video o datos) y el controlador multipunto (MC) que proporciona la capacidad de negociación.

1.2.8. Mensajería y otros

Elementos de valor añadido como: Buzón de Voz (VM), respuesta de voz interactiva (IVR), integración de telefonía informática (CTI), distribuidor automático de llamadas (ACD), entre otros.

1.3. Sistemas VoIP más utilizados

Dentro de los sistemas de comunicación VoIP encontramos privativos y open source, a continuación, se describen los más utilizados.

1.3.1. Asterisk

Asterisk es un framework gratuito y de código abierto para construir aplicaciones de comunicaciones, convirtiendo una computadora ordinaria en un servidor de comunicaciones. Alimenta los sistemas IP PBX, las puertas de enlace VoIP, los servidores de conferencia y otras soluciones personalizadas. Es utilizado por pequeñas empresas, grandes empresas, call centers, operadores y agencias gubernamentales en todo el mundo [6].

Hoy en día, hay más de un millón de sistemas de comunicaciones basados en Asterisk en uso, en más de 170 países. La mayoría de las veces implementado por integradores y desarrolladores de sistemas, puede convertirse en la base de un sistema de teléfono comercial completo, o se utiliza para mejorar y ampliar un sistema existente, o para cerrar una brecha entre sistemas [6].

1.3.1.1. Ventajas que proporciona Asterisk

Algunas ventajas de usar Asterisk son [7]:

- Es un software gratuito, y el código fuente está disponible para el que lo desee.
- Puede utilizarse en cualquier sistema compatible con Linux
- Es compatible con cualquier tipo de terminales que contengan señalización SIP, IAX o H.323, que son los tres protocolos más usados en la actualidad.
- Pertenece a la empresa Digium quien garantiza el funcionamiento de Asterisk y ofrece soporte técnico para sus versiones.
- Cualquier detección de fallo de seguridad, es rápidamente publicado.

1.3.1.2. Arquitectura

A continuación se muestra un diagrama simplificado destinado a ilustrar las relaciones de algunos componentes principales entre sí y con entidades fuera de Asterisk. Es útil comprender cómo un componente puede relacionarse con otros componentes fuera de Asterisk, ya que Asterisk no suele funcionar sin conectividad o interacción con otros dispositivos de red o archivos en el sistema local [6].

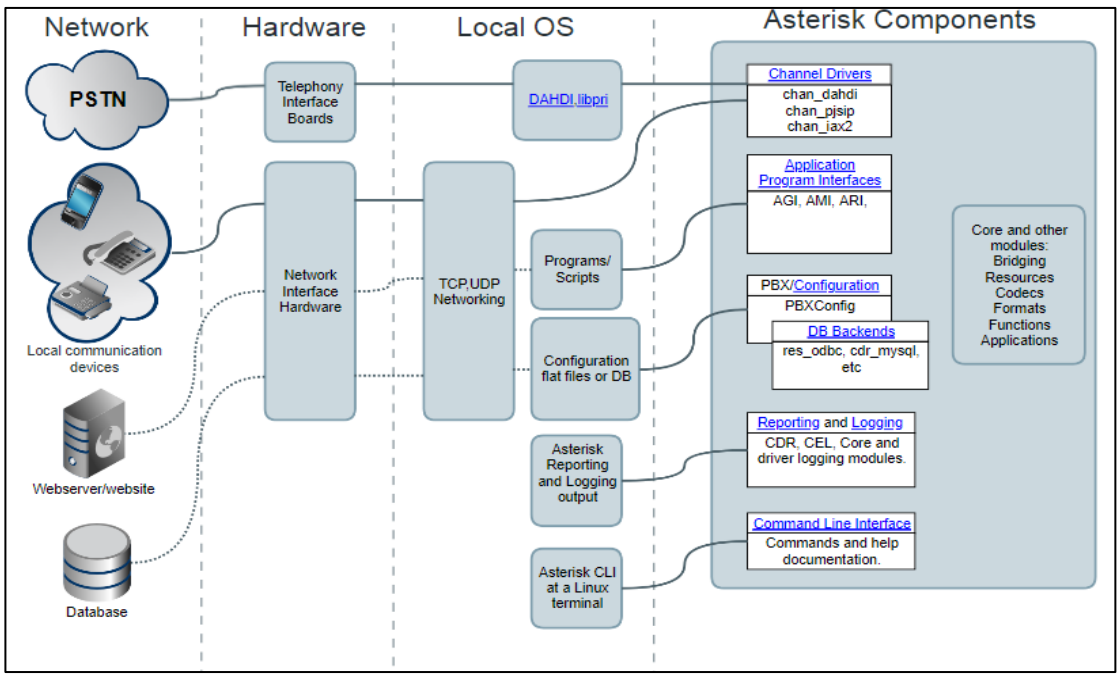


Figura 4. Arquitectura del Sistema Asterisk [6].

Desde un punto de vista arquitectónico, Asterisk se compone de muchos módulos diferentes. Esta modularidad le brinda una cantidad casi ilimitada de flexibilidad en el diseño de un sistema basado en Asterisk. El administrador de Asterisk tiene la opción de elegir qué módulos cargar y la configuración de cada módulo. Cada módulo que carga proporciona diferentes capacidades al sistema. Por ejemplo, un módulo podría permitir que su sistema Asterisk se comunique con líneas telefónicas analógicas, mientras que otro podría agregar capacidades de reporte de llamadas [6].

Asterisk tiene un núcleo que puede interactuar con muchos módulos. Los módulos denominados controladores de canal proporcionan canales que siguen el plan de marcación de Asterisk para ejecutar el comportamiento programado y facilitar la comunicación entre dispositivos o programas externos. Los canales a menudo utilizan una infraestructura de puente para interactuar con otros canales [6].

1.3.1.2.1. El núcleo

El corazón de cualquier sistema Asterisk es el núcleo. Entre muchas funciones del núcleo, lee los archivos de configuración, incluido el plan de marcación y carga todos los demás módulos y distintos componentes que proporcionan más funcionalidad.

El núcleo carga y construye el plan de marcado, que es la lógica de cualquier sistema Asterisk. El plan de marcado contiene una lista de instrucciones que Asterisk debe seguir para saber cómo manejar las llamadas entrantes y salientes en el sistema.

1.3.1.2.2. Módulos

Aparte de la funcionalidad proporcionada por el núcleo de Asterisk, los módulos proporcionan todas las demás funciones. La fuente de muchos módulos se distribuye con Asterisk, aunque otros módulos pueden estar disponibles a través de miembros de la comunidad o incluso de negocios que hacen módulos comerciales. Los módulos distribuidos con Asterisk se pueden construir opcionalmente cuando se construye Asterisk [6].

Los módulos no solo se construyen opcionalmente, sino que también puede afectar en el tiempo de carga si se cargarán, el orden de carga o incluso descargarlos / cargarlos

durante el tiempo de ejecución. La mayoría de los módulos son configurables independientemente y tienen sus propios archivos de configuración. Algunos módulos tienen soporte para que la configuración se lea de forma estática o dinámica (en tiempo real) desde los backends de la base de datos [6].

1.3.2. Elastix

Elastix es un sistema de código abierto para el establecimiento comunicaciones unificadas. Bajo este concepto, el objetivo de Elastix es el de incorporar todos los medios y alternativas de comunicación existentes en el ámbito empresarial, en una única solución [8].

El proyecto Elastix se inició como una interfaz de reportación para llamadas de Asterisk y fue liberado en marzo del 2006. Posteriormente el proyecto evolucionó hasta convertirse en una distro basada en Asterisk.

Debido a que la telefonía es el medio tradicional que ha liderado las comunicaciones durante el siglo XX, muchas empresas y usuarios centralizan sus requerimientos únicamente en sus necesidades de establecer telefonía en su organización confundiendo distros de comunicaciones unificadas con equipos destinados a ser centrales telefónicas. Sin embargo, Elastix no solamente provee telefonía, sino que integra otros medios de comunicación para hacer más eficiente y productivo su entorno de trabajo [8].

1.3.2.1. Características

Con Elastix puede crear el PBX ideal para su negocio cualquiera que sea su tamaño o requerimientos; puede elegir como implementarlo dependiendo de sus necesidades y la de su negocio sobre su plataforma de comunicaciones. Ya sea que quiera un PBX Linux on-premise, instalarlo en Windows, o prefiera alojar su sistema telefónico en la nube.

- PBX Multi-plataforma: funciona con Windows, Linux o en la nube.
- On-premise: funciona en un Mini PC de bajo costo o máquina virtual.
- En la Nube: Google, Amazon o OVH manteniendo el control.
- Softphones para Windows y Mac.

- Funcionalidades UC: presencia, chat, fax y buzón de voz a correo electrónico.
- Conferencia web WebRTC integrada.
- Clientes para Smartphones Android y iOS.
- Función Click2Call desde cualquier navegador.
- Tareas de administración del PBX automatizadas.

1.3.3. Issabel

Issabel es un software gratuito y de código abierto que le permite unificar sus comunicaciones con complementos que lo ayudarán a satisfacer la necesidad que desee, puede desarrollarlo o esperar a que la comunidad lo haga [9].

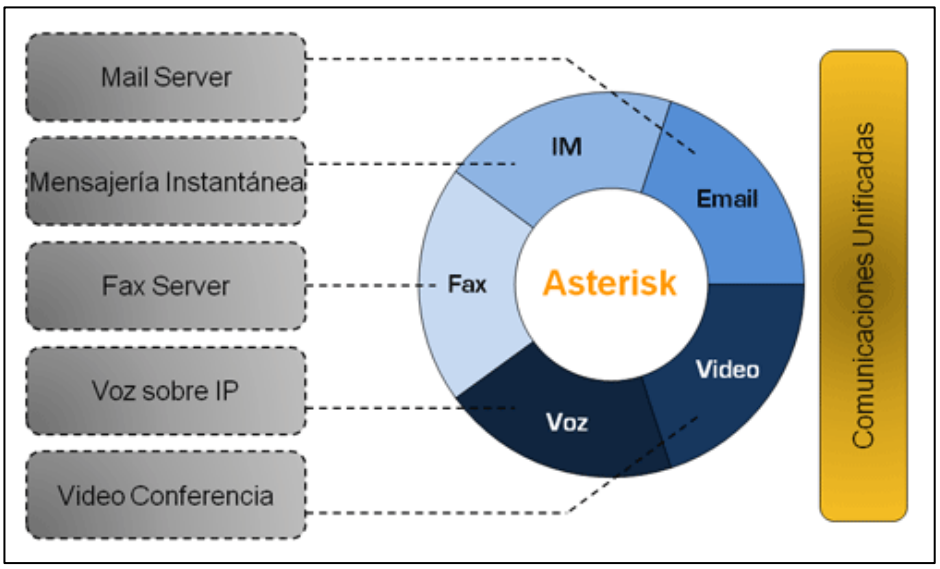


Figura 5. Características de Issabel [9].

1.3.3.1. Características

Issabel tiene muchas funcionalidades que la convierten en una de las más completas plataformas de comunicaciones, una de las más importantes es un módulo de call center el cual incorpora un marcador automático progresivo predictivo que lo convierte en uno de los mejores en su género. Algunas de las características básicas del sistema ISSABEL incluyen:

- Correo de Voz
- Fax-a-email

- Soporte para softphones
- Interfase de configuración Web
- Sala de conferencias virtuales
- Grabación de llamadas
- Least Cost Routing
- Roaming de extensiones
- Interconexión entre PBXs
- Identificación del llamante
- Reportación avanzada

2. Seguridad en las comunicaciones VoIP

La seguridad informática en los sistemas VoIP es uno de los aspectos muy importantes para garantizar la protección de los usuarios de cualquier tipo de amenazas y ataques.

2.1. Aspectos de seguridad en los distintos protocolos de VoIP.

La mayoría de los proveedores de servicio reconocen que las redes VoIP de extremo a extremo constituirán la tecnología soporte de las telecomunicaciones del futuro, sin embargo, para que esto sea efectivamente cierto, se deben considerar requerimientos claves que aseguran la equivalencia con la RTPC actual, especialmente en cuanto a la calidad ya alcanzada por la antigua red. Entre estos requerimientos se encuentra la selección del protocolo de señalización.

Para una solución VoIP se han desarrollado numerosos protocolos de señalización, entre los que se encuentran [10]:

- Protocolos de señalización de accesos a los servicios, tales como SIP (Protocolo de Inicialización de Sesión), H.323, entre otros.
- Protocolos de señalización de servicios en la red, tales como SIP, SIP-T (SIP para Teléfonos), BICC (Bearer Independent Call Control), entre otros.
- Protocolos de control de dispositivos, tales como MEGACO/H.248, MGCP (Media Gateway Control Protocol), entre otros.

La selección del protocolo a utilizar en la red del Proveedor de Servicios depende del conjunto de estos que serán ofrecidos y del equipamiento disponible para proveer estos servicios.

2.1.1. MEGACO/H.248

El IETF (Internet Engineering Task Force) comenzó a trabajar en MEGACO como protocolo de compromiso entre MGCP y MDCP (Media Device Control Protocol). En junio de 1999, el Grupo de Trabajo MEGACO de IETF y la UIT -T divulgaron un único documento que describía un protocolo estándar (MEGACO/H.248) para la interconexión entre los Controladores de Pasarelas de Medios (MGCs) y las Pasarelas de Medios (MGs). Se prevé que gane la aceptación de la industria como el estándar oficial para las arquitecturas de pasarelas descompuestas.

MEGACO (RFC 3525) recomienda mecanismos de seguridad que pueden estar en mecanismos de transporte subyacentes, tales como IPsec (Internet Protocol Security). H.248 va a un paso adelante al requerir que las implementaciones del protocolo H.248 implementen IPsec si el sistema operativo subyacente y la red de transporte soportan IPsec. Se requieren implementaciones del protocolo usando IPv4 para poner en práctica el esquema AH (Authentication Header) interno. H.248 plantea que la implementación utilizando el encabezado AH proporcionará un conjunto mínimo de algoritmos para el chequeo de integridad usando llaves manuales (en correspondencia con la RFC 2402).

2.1.2. Protocolo SIP

SIP es un protocolo especificado por IETF para iniciar una sesión de comunicación de dos vías. Es un protocolo del nivel de aplicación, es decir, se desacopla de la capa del protocolo por el que se transporta.

Este puede ser transportado por TCP (Transmission Control Protocol), UDP o SCTP (Stream Control Transmission Protocol). UDP (User Datagram Protocol) se puede utilizar para disminuir el encabezamiento adicional y para aumentar velocidad y eficiencia. TCP puede ser utilizado si SSL/TLS se incorpora para los servicios de seguridad.

El protocolo de transmisión de control de la trama SCTP ofrece resistencia creciente a los ataques del DoS (Denied of Service) a través de un método de intercambio de 4 vías, es multi-home, o sea cada punto extremo SCTP puede ser conocido por múltiples direcciones IP, siendo el enrutamiento para una dirección independiente de todas las otras, si una ruta se hace no alcanzable, otra será utilizada. Además, permite opcionalmente bundling (múltiples mensajes de usuarios) en un único paquete SCTP.

Los servicios de seguridad adicionales se pueden utilizar con SCTP vía RFC 3436 (TLS sobre SCTP) o 3554 (SCTP sobre IPSec). A diferencia de H.323, solo se utiliza un puerto en SIP (en H.323 se puede también utilizar un camino que utilice un solo puerto para el caso de llamadas enrutadas directamente). El valor por defecto de este puerto es 5060.

La codificación en texto de SIP hace más fácil de analizar utilizando herramientas estándar. No obstante, algunos nuevos requerimientos son puestos en el firewall en una red de VoIP basada en SIP. Primero, los firewalls deben tener estado (stateful) y monitorear el tráfico SIP para determinar que puertos RTP deben ser abiertos y hacerlos disponibles a cualquier dirección. Esta responsabilidad es similar a la tarea de los firewalls en una red basada en H.323, excepto que el establecimiento de la llamada y las cabeceras que analizan es mucho más simple. Otro tema de VoIP basado en SIP, encontramos los firewalls asociado al tráfico de RTP y a llamadas entrantes. Como con H.323, el problema grande para SIP son los NATs.

2.1.3. Protocolo H.323

H.323 es una especificación de ITU (International Telecommunication Union) para la comunicación de audio y video a través de redes de paquetes. H.323 es actualmente un estándar general, que abarca varios protocolos, incluyendo H.225, H.245, H.235 y otros.

Una red H.323 se compone de varios puntos finales (terminales), de una pasarela y posiblemente de un gatekeeper, de una Unidad de control de Multipunto (MCU). El gatekeeper es el componente principal en los sistemas H.323. Proporciona resolución de direcciones y control del ancho de banda. La pasarela sirve como puente entre la red H.323 y el mundo exterior donde (posiblemente) los dispositivos no utilicen H.323. Esto incluye redes SIP y redes tradicionales PSTN (Public Switched Telephone Network) [10].

El proceso de establecimiento de una llamada VoIP basado en H.323 es complejo. Este tiene diversos protocolos asociados con formularios de comunicación con las más complejas formas de comunicación, incluyendo H.332 (grandes conferencias), H.450.1, H.450.2 y H.450.3 (servicios suplementarios), H.235 (seguridad) y H.246 (interoperabilidad con los servicios de conmutación de circuito) [30]. La autentificación se puede también realizar en cada punto en el proceso de establecimiento de la llamada utilizando claves simétricas o con un secreto compartido a priori. El uso de estos protocolos y/o medidas de seguridad agrega complejidad al proceso del establecimiento de llamadas en H.323. Esta complejidad es superior en la incompatibilidad de H.323 con los firewalls y NATs [10].

2.2.Amenazas de seguridad de un sistema VoIP.

La definición de amenaza según la norma ISO 27001 es “una causa potencial de un incidente indeseado, que puede dar lugar a daños a un sistema o a una organización”. Las amenazas a la seguridad son incidentes que provocan que al menos un concepto de seguridad sea puesto en riesgo.

En un sistema VoIP podemos mencionar diferentes tipos de amenazas de seguridad como: denegación de servicio (DoS), Spam over Internet Telephony (SPIT), fraudes telefónicos, accesos no autorizados, ataques de ingeniería social (Vishing), interceptación de llamadas, entre otros [5].

2.2.1. Denegación de servicio (DoS)

La denegación de servicio son ataques maliciosos que degradan el sistema hasta inhabilitar el funcionamiento, afectando la disponibilidad del mismo. Este ataque puede ser logrado mediante la inyección de gran cantidad de paquetes cuidadosamente creados para explotar debilidades de software.

El objetivo de los ataques de denegación de servicio en una red VoIP es colapsar los dispositivos de red mediante la inundación de llamadas falsas que generan tráfico excesivo. De esta manera, las llamadas legítimas se interrumpen o no pueden conectarse [5].

2.2.2. Accesos no autorizados

Los accesos no autorizados son ataques dirigidos a los sistemas de control de llamadas, facturación, administración, y cualquier otra función telefónica donde se requiera de autenticación. Cada una de estas funciones pueden contener datos, que al ser comprometidos pueden perjudicar al usuario de alguna forma.

2.2.3. Fraude Telefónico (Toll fraud)

Los ataques de fraude telefónico son frecuentes especialmente en los sistemas telefónicos tradicionales. Son ataques que tienen como objetivo recaudar dinero a través del servicio telefónico, mediante robos de minutos de llamadas o realizando llamadas de larga distancia.

2.2.4. Interceptación (Eavesdropping)

El ataque de interceptación de llamadas es también conocido con el término de Eavesdropping. Este ataque consiste en la captura de las conversaciones telefónicas e interceptación de los mensajes utilizados en el sistema. por parte de intrusos ajenos a la conversación.

A diferencia de la interceptación de llamadas en redes tradicionales, en VoIP la interceptación puede darse en dos partes: los paquetes de voz y la señalización. Mediante la interceptación de paquetes de voz se accede contenido del mensaje de una conversación telefónica. La interceptación de la señalización revela la infraestructura y configuración de la red o la localización de los dispositivos.

2.2.5. SPIT (Spam over Internet Telephony)

El Spam over Internet Telephony (SPIT) es el SPAM de la telefonía VoIP. Es un ataque que consiste en el envío de mensajes SMS o mensajes de voz a los buzones de los usuarios.

A pesar que el SPIT en la actualidad no es un ataque demasiado extendido en comparación con el SPAM, sin embargo, las redes VoIP son muy vulnerables al envío

de mensajes de voz no deseados. Esto hace que sea una amenaza que afectaría gravemente al correcto funcionamiento de las redes VoIP, por la limitada cantidad de memoria que posee un servidor de buzón de voz.

Este ataque es cada vez más común de acuerdo a la expansión de la comunicación VoIP, como sucedió con los correos electrónicos, ya que los interesados en telemarketing han visto en las redes VoIP, una plataforma muy importante para poder llegar a millones de usuarios alrededor del mundo.

2.2.6. Vishing

Vishing es el término usado para referirse a la ingeniería social en telefonía IP. Es un ataque con las mismas características que el phishing pero adaptado a todas las posibilidades que puede ofrecer una red VoIP. Los ataques de phishing representan un gran problema para el usuario.

Los ataques de robo de información confidencial por medio de vishing son muy comunes en las comunicaciones IP y se utilizan las mismas técnicas del phishing.

La telefonía IP permite a un atacante realizar una llamada desde cualquier lugar del mundo, y utilizado técnicas de ingeniería social como mostrar una identidad falsa o la identidad de una persona conocida por la víctima, pueden obtener información confidencial como números de cuenta, datos personales o cualquier otro tipo de información.

2.3.Medidas de seguridad

El procedimiento a seguir para garantizar la seguridad a una red VoIP consiste de tres etapas: identificación de protocolos, identificación de tecnologías y establecimiento de medidas de seguridad. El cumplimento de este procedimiento depende de la tecnología, protocolos y dispositivos utilizados.
Cada una de estas etapas se describen a continuación [5].

1. Identificación de protocolos. Es necesario identificar los protocolos usados en la red VoIP.

2. Identificación de tecnologías. Consiste en identificar los dispositivos que conforman la red VoIP. Implica la identificación del modelo (hardware) o versión (software).

3. Establecimiento de medidas de seguridad. Una vez determinado el protocolo y la tecnología utilizada se puede definir las medidas de seguridad a implementarse. El establecimiento de estas medidas la se realizará por cada capa del modelo OSI.

2.3.1. Recomendaciones UIT-T X.805

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial. La recomendación UIT-T X.805 fue aprobada el 29 de octubre de 2003 por la Comisión de Estudio 17 (2001-2004) del UIT-T por el procedimiento de la Recomendación UIT-T A.8., en esta Recomendación se define el marco para la Arquitectura de Seguridad para Sistemas de Comunicación de Extremo a Extremo, y las dimensiones que garantizan la seguridad extremo a extremo de aplicaciones distribuidas.

(UIT-T, 2003). X.805 se basa en algunos conceptos de X.800 y en los marcos de seguridad (X.810-X.816). Las dimensiones de seguridad de las comunicaciones, disponibilidad y privacidad de X.805 ofrecen nuevos tipos de protección para la red.

Estas siete dimensiones de seguridad se exponen a continuación [11]:

1. Privacidad y confidencialidad de datos
2. Autenticación
3. Integridad de datos
4. No repudio
5. Control de Acceso
6. Comunicación
7. Disponibilidad

Entre las recomendaciones específicas para VoIP se encuentran [11]:

1. Garantizar la seguridad de operaciones, administración, mantenimiento y configuración (OAM&P) de los servicios de red.
2. Proteger la información de control o señalización que se utiliza en el servicio de red. Por ejemplo, proteger el protocolo SIP que se utiliza para iniciar y mantener las sesiones de VoIP.
3. Proteger los datos y la voz cuando el usuario utiliza el servicio de red. Por ejemplo, proteger la confidencialidad de la conversación de un usuario en un servicio VoIP.

2.3.2. Recomendaciones de seguridad de NIST

La National Institute of Standards and Technology (NIST) tiene como misión promover la innovación y la competitividad industrial mediante el avance ciencia de la medición, normas, y la tecnología de forma que mejoren la seguridad económica. El mismo que propone varias recomendaciones prácticas para la implementación segura de una red VoIP, entre las más importantes, podemos citar [11]:

1. Desarrollar la arquitectura de red apropiada.
2. Asegurar que la organización ha examinado y puede manejar y mitigar los riesgos relacionados con el manejo de la información, sistemas operativos y la continuidad de sus operaciones esenciales después de implementar el sistema de VoIP.
3. Desarrollar controles físicos apropiados en la red VoIP a menos que se encuentre cifrada.
4. Usar los sistemas de emergencia de energía requeridos para asegurar la operación continua durante apagones o fallas del fluido eléctrico.
5. Utilizar los mecanismos de protección apropiados y firewalls especializados en VoIP.

2.3.3. Recomendaciones de seguridad de ISO/IEC 27002

Las normas ISO/IEC 27000, son un conjunto de estándares desarrollados, por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información que pueden ser utilizados por cualquier tipo de organización privada o pública de cualquier tamaño.

La norma ISO/IEC 27002, proporciona recomendaciones de buenas prácticas en el campo de seguridad de la información, la cual puede servir como base para la implementación de medidas de seguridad para la prevención de riesgos dentro de una organización.

Entre las recomendaciones ISO/IEC 27002 enfocadas a las comunicaciones de Voz sobre IP están [11]:

1. Controlar los accesos a servicios internos y externos conectados en red.
2. Proteger tráfico de VoIP
3. Cifrar
4. Aplicar mecanismos de autenticación adecuados se aplican a los usuarios y equipos
5. Llevar un rígido manejo de llaves.
6. Segregar el tráfico de datos y de voz
7. Hacer uso de servidores proxy delante de firewalls
8. Resguardar los IP-PBX's.
9. Usar controles de seguridad perimetrales Firewall o SBC

Implementar herramientas de seguridad de red como IDS/IPS (detección y prevención de intrusiones), gestión de vulnerabilidades, entre otros

3. Revisión sistemática de literatura

El termino revisión sistemática se utiliza para referirse a una metodología específica de investigación, desarrollada para obtener y evaluar la evidencia disponible sobre un tema central [12].

3.1. Metodología de Bárbara Kitchenham

La metodología propuesta por Barbara Kitchenham para revisiones sistemáticas se basa en pautas desarrolladas para la investigación médica [13], que pueden ser utilizados en otros campos de estudio.

3.1.1. Fases de la revisión sistemática

Kitchenham propone un método para realizar revisiones sistemáticas que se basa en pautas desarrolladas para la investigación médica y estas han sido adaptadas para ser usadas en el ámbito de la ingeniería de software [13].

Una revisión sistemática se define como una manera de evaluar e interpretar toda la investigación disponible relevante respecto de una interrogante de investigación particular, en un área temática o fenómeno de interés. Los estudios individuales que contribuyen a una revisión sistemática se denominan estudios primarios, una revisión sistemática se considera un estudio secundario. En particular este método propone tres etapas fundamentales que son: (i) planificación de la revisión, (ii) desarrollo de la revisión y (iii) publicación de los resultados de la revisión, las que a su vez se encuentran divididas en otras etapas que detallan la forma en que se deben desarrollar [13].

3.1.1.1. Planificación de la revisión

La primera fase de investigación se inicia a partir de los conceptos, que representan de manera explícita y formalmente el tema en cuestión [12]. Esta etapa tiene como propósito específico definir los parámetros más importantes para llevar a cabo la revisión [13].

3.1.1.1.1. Identificación de la necesidad de la revisión.

Antes de emprender una revisión sistemática, el investigador debe asegurarse de que ésta es necesaria. En particular, es recomendable identificar y analizar cualquier revisión sistemática existente acerca del fenómeno de interés con un criterio de evaluación apropiado [13]. Se sugiere contestar las siguientes:

¿Cuáles son los objetivos de la revisión?
¿Qué fuentes fueron buscadas para identificar estudios primarios?
¿Qué criterios se incluyeron o excluyeron y cómo fueron aplicados?
¿Qué criterios fueron usados para evaluar la calidad de los estudios primarios y cómo fueron aplicados?
¿Cómo se diferencian los estudios investigados?

¿Cómo fueron combinados los datos?
¿Era razonable combinar los estudios?

Junto con lo anterior, también se deben identificar claramente los recursos con que inicialmente se cuenta para llevar a cabo la revisión.

3.1.1.1.2. Definición de un protocolo de búsqueda.

En esta sub-etapa se deben definir las normas que seguirá la investigación respecto del proceso de búsqueda en las fuentes de información definidas en la sub-etapa anterior. Deben ser definidos los términos que se buscarán, las combinaciones de éstos, la estrategia de búsqueda empleada según cada fuente y la manera en que se registrarán los resultados. Respecto de la estrategia de búsqueda, es importante establecer la manera en que se va a proceder respecto de cada fuente empleada. Respecto al Internet, que nos facilita la accesibilidad de la literatura científica, pero también es necesario hacer un filtrado adecuado que permita acceder sólo a aquella información que sea realmente útil. Es importante tener en cuenta que el proceso de búsqueda es perfectible, por lo que el protocolo puede y debe ser mejorado durante el desarrollo de la búsqueda, por ejemplo, se pueden incorporar otros términos de búsqueda o realizar otras combinaciones de los términos usados

3.1.1.1.3. Definición de un protocolo de revisión.

El protocolo de revisión especifica los métodos que serán usados para emprender la revisión sistemática. El disponer de un protocolo predefinido contribuye a evitar los prejuicios del investigador. La idea es impedir, en la medida de lo posible, que la selección de los estudios individuales pueda estar guiada por las expectativas del investigador [13].

Durante esta etapa se realiza la revisión de cada uno de los estudios encontrados y que potencialmente pueden ser incluidos en la revisión. Se deben definir las normas de revisión a seguir, los criterios de exclusión e inclusión que serán empleados, la estrategia de extracción de datos y finalmente la estrategia de síntesis [13].

Dado que los estudios que son revisados se encuentran en formato de artículo científico, y dada la necesidad de detallar un procedimiento de revisión, en [13] se considera la siguiente estructura que se indica en la Figura 6.

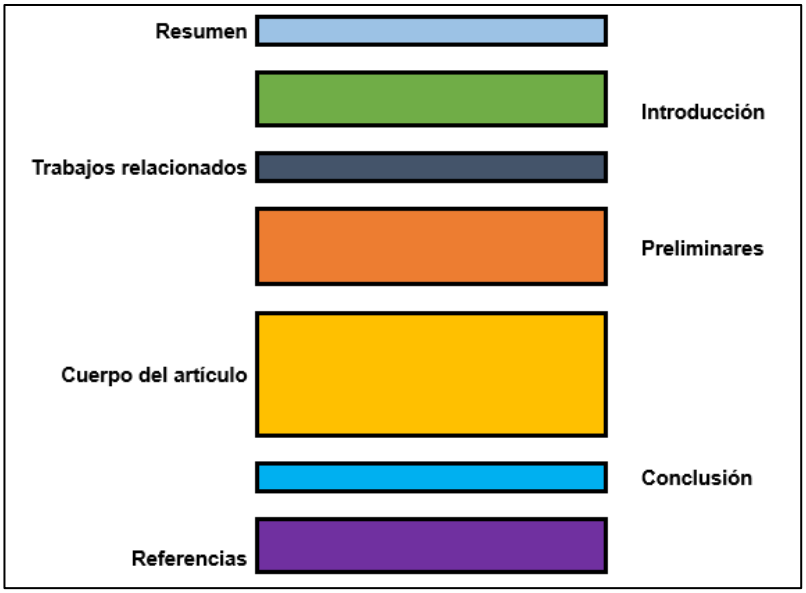


Figura 6. Definición del protocolo de revisión propuesto por B. Kitchenham [13].

3.1.1.1.4. Evaluación de la planificación.

Esta etapa consiste en hacer una valoración objetiva de la planificación. Ya que esta propuesta se enmarca en el contexto de proyectos de fin de carrera la evaluación de la planificación tendrá que hacerla el tutor o guía del proyecto [13].

3.1.1.2. Desarrollo de la revisión

En esta etapa se lleva a cabo la revisión propiamente tal. Su desarrollo está guiado por la planificación de la revisión. Sin embargo, y ya que es un proceso flexible, es posible incluir cambios que mejoren su desempeño [13].

3.1.1.2.1. Búsqueda de estudios primarios

La búsqueda de estudios primarios se debe realizar en base al protocolo de búsqueda que fue definido para ello y que se encontrará en un formato como el sugerido en la etapa anterior. Los estudios que se consideren potencialmente útiles se deberán dejar

accesibles para la siguiente etapa, ya sea en formato electrónico y/o impreso, o bien dejar registrado dónde ubicarlos una vez que se proceda a la selección [13].

3.1.1.2.2. Selección de estudios primarios

La selección de los estudios debe hacerse en base al protocolo de revisión definido. Este proceso será guiado por los criterios de inclusión y exclusión, dependiendo de los intereses del proyecto es recomendable registrar los motivos de exclusión [13].

3.1.1.2.3. Extracción y gestión de datos

En esta subetapa se extrae la información de interés en los estudios, ya sean resúmenes, ideas o partes de los documentos. Esta extracción se debe realizar en base al protocolo de revisión definido. Además, se debe registrar la información necesaria para gestión, como la relativa a la bibliografía, ubicación física del documento u otra información que los investigadores consideren pertinente [13].

Se recomienda usar herramientas, como por ejemplo EndNote, para mantener los datos más relevantes de cada estudio revisado. Este tipo de herramientas, junto con el registro de la información de los documentos, permite realizar búsquedas, ordenamientos, en general, hacer una adecuada gestión de la información [13].

3.1.1.2.4. Síntesis de datos

En esta subetapa, al igual que en las anteriores, se debe aplicar el protocolo definido en la revisión, y consiste en registrar la información extraída de los estudios primarios siguiendo alguna estrategia. Los datos pueden ser sintetizados considerando, por ejemplo, el enfoque que se le desea dar a la presentación del estado del arte o la identificación del o los fenómenos de interés [13].

3.1.1.3. Publicación de Resultados.

Esta etapa corresponde a la utilización de los resultados una vez que disponemos de ellos. Es muy importante la difusión de los resultados obtenidos producto de una revisión

sistemática. Las formas más convenientes de comunicar los resultados son: a través de la participación en conferencias, publicación de un artículo o de un informe técnico [13].

e. Materiales y Métodos

1. Materiales

Los materiales y equipos utilizados en el desarrollo del presente trabajo son los siguientes:

1.1. Materiales y equipos de oficina

Entre los materiales de oficina utilizados constan: hojas de papel, lápices, borradores, bolígrafos, grapadora, memoria flash, computadora, impresora, entre otros.

1.2. Software

El software utilizado en el desarrollo del presente trabajo es: gestor bibliográfico Mendeley Desktop, procesador de texto y navegador web.

1.3. Fuentes bibliográficas

Las fuentes de búsqueda utilizados en la recopilación de información primaria para el análisis sistemático, son bibliotecas digitales del área de tecnologías de la información y la comunicación, como son: Google académico, IEEE Xplore, Springer y ScienceDirect.

2. Métodos

Los métodos utilizados en el desarrollo del presente trabajo investigativo son el método analítico y el método sintético.

2.1. Método Analítico.

Este método permitió analizar los datos obtenidos de la recopilación de fuentes bibliográficas; es decir, las revistas científicas relacionadas con la seguridad en las

comunicaciones VoIP, necesarias para el desarrollo del presente trabajo. Permitiendo realizar un estudio comparativo de la documentación bibliográfica seleccionada.

2.2. Método Sintético

Este método se utilizó para analizar las conclusiones y sintetizar la información recopilada de las revistas científicas acerca de la seguridad en los sistemas de voz sobre IP.

3. Metodología de trabajo utilizada

El presente trabajo se desarrolló tomando como base la metodología propuesta por Bárbara Kitchenham y perfeccionada para trabajos de fin de carrera promovida y desarrolla por el Grupo Alarcos de la Escuela Superior de Informática de la Universidad Castilla-La Mancha, España. En donde se agregan dos actividades en la etapa de planificación, como son la definición de protocolo de búsqueda y la evaluación de la planificación como se puede apreciar en Figura 7.

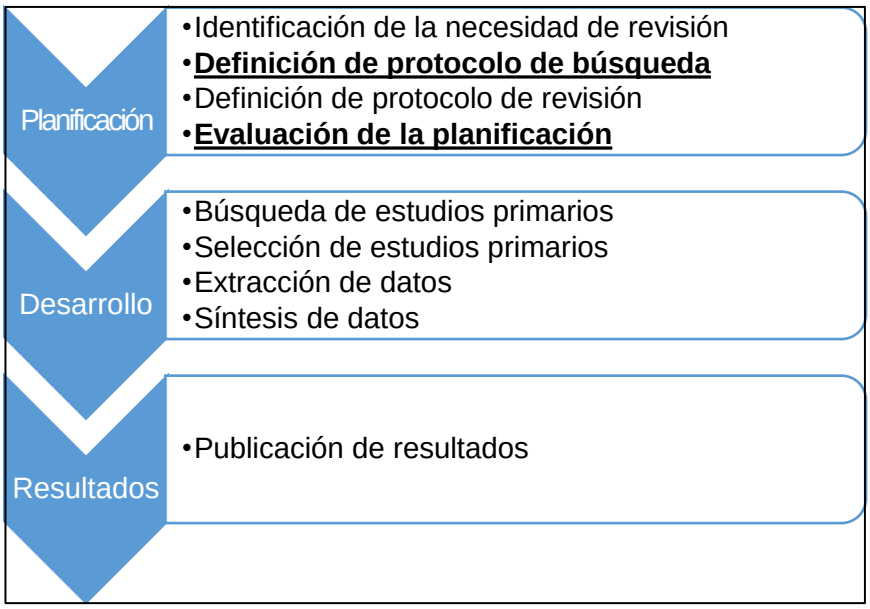


Figura 7. Etapas propuestas por la metodología para la revisión sistemática.

Esta metodología indica las directrices y los pasos a seguir desde la planificación de la revisión hasta la publicación de los resultados.

f. Resultados

En esta sección se detalla el procedimiento completo establecido para completar la revisión bibliográfica, esto se ha desarrollado en tres fases en donde se cumple cada uno de los objetivos propuestos.

Fase I: Seleccionar documentación bibliográfica de la seguridad en los sistemas VoIP más utilizados en la actualidad.

Esta fase comprende la planificación y definición de reglas de búsqueda, la búsqueda y obtención de la información bibliográfica necesaria para el análisis, la misma que abarca varias tareas que a continuación se describen.

1. Planificación de la revisión

En esta etapa se define los parámetros más importantes que son tomados en cuenta durante el desarrollo de la revisión. Se establecen las razones de la investigación, se definen los criterios de búsqueda de estudios primarios y los criterios de inclusión y excusión de la documentación bibliográfica sobre seguridad en los sistemas de comunicación VoIP.

1.1. Identificación de la necesidad de revisión

Conociendo que en la actualidad las comunicaciones VoIP están bastante extendidas y la mayor preocupación de los usuarios es la seguridad que ofrece esta tecnología, por tal razón, esta revisión sistemática busca hacer una recopilación de los estudios y análisis relacionados con la seguridad en las comunicaciones basadas en el protocolo IP, a fin de conocer la situación actual de este campo de estudio.

1.1.1. Objetivo de la revisión

De acuerdo con la problemática planteada, el objetivo del presente trabajo de revisión sistemática es: Analizar la seguridad de las comunicaciones VoIP.

1.1.2. Pregunta de investigación

La pregunta planteada y que será contestada durante la presente investigación es: ¿Son seguras las comunicaciones basadas en VoIP?

1.1.3. Recursos y fuentes de búsqueda.

Para la presente revisión sistemática de literatura se cuenta con documentación relacionada a la seguridad de las comunicaciones VoIP, disponibles en bases de datos científicas especializadas y otros repositorios académicos de acceso libre en Internet.

1.2. Definición del protocolo de búsqueda

En esta etapa se definen todos los parámetros y criterios de búsqueda de la información bibliográfica, consta de varias etapas que se detallan a continuación:

1.2.1. Definir las palabras claves para la búsqueda de documentación bibliográfica.

El presente trabajo tiene como finalidad hacer un análisis sistemático de literatura del tema “Seguridad Informática en los sistemas VoIP”, por lo tanto, las palabras claves tanto en idioma inglés como en español que se han considerado para la búsqueda de información son: **Security (Seguridad), VoIP, IP PBX, IP telephony.**

1.2.2. Definición de las cadenas de búsqueda

Para realizar la búsqueda se han utilizado las palabras claves concatenadas con algunos operadores booleanos, tomando en cuenta que VoIP, IP PBX e IP Telephony, se refieren a la misma tecnología, en la definición de la cadena de búsqueda se utilizó el operador OR(O) para concatenar las tres palabras(sinónimas) y el operador AND(Y) para concatenar la palabra seguridad, ya que se necesita buscar información relacionada con la seguridad de éstas tres palabras.

Las cadenas de búsqueda en inglés y español quedan estructuradas de la siguiente manera:

(seguridad) Y (voip O ip telephony O IP PBX)
(security) AND (voip OR ip telephony OR IP PBX)

1.2.3. Definir las fuentes de búsqueda.

Las fuentes de búsqueda que se han tomado en cuenta son Bibliotecas digitales especializadas de ciencia y tecnología y artículos publicados en Internet, siempre y cuando sean de fuentes debidamente verificadas como:

- Google académico
- IEEE Xplore
- Springer
- Sciencedirect

1.2.4. Registro de resultados

Se define el formato para el registro de los resultados de las búsquedas del tema "seguridad de los sistemas VoIP".

Para la presente revisión sistemática se ha estimado conveniente registrar en tablas, indicando el número total de artículos encontrados, los incluidos y excluidos, por cada fuente de búsqueda.

1.3. Definición del protocolo de revisión

A diferencia del protocolo de búsqueda, la definición de un protocolo de revisión, provee de reglas preestablecidas para la revisión de cada uno de los artículos seleccionados.

El protocolo de revisión definido para el presente trabajo, es el propuesto por la metodología (de Bárbara Kitchenham) utilizada para esta revisión sistemática, el flujo se puede apreciar en la Figura 8.

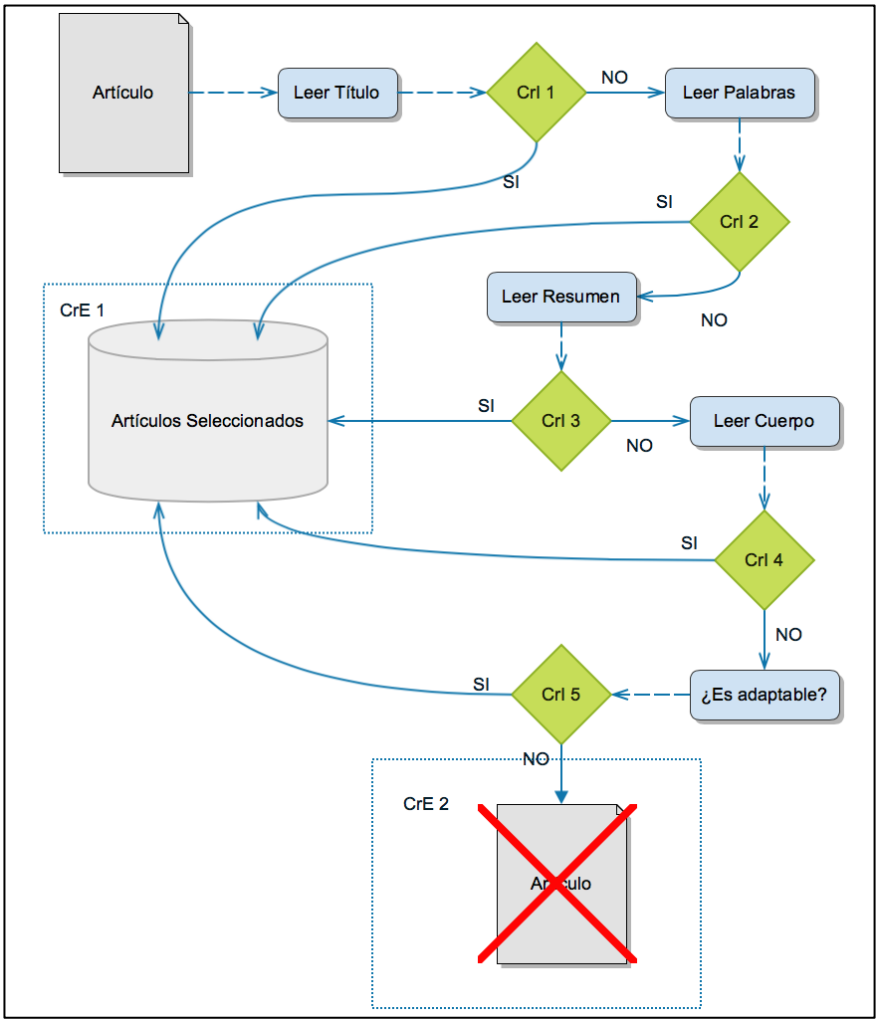


Figura 8. Protocolo para la revisión de artículos [12].

1.3.1. Definir los criterios de inclusión y exclusión de la documentación

Para filtrar la información más relevante para este estudio se han considerado algunos criterios de inclusión y exclusión detallados a continuación.

1.3.1.1. Criterios de inclusión

Toda la bibliografía que se tomará en cuenta para el análisis debe cumplir con los siguientes criterios:

- Deben estar escritos entre el año 2015 a 2019.
- La búsqueda será en el área de ciencias de la computación.

- Se tomarán en cuenta solamente artículos científicos.
- Se incluirán solamente documentos en idioma español e inglés.

1.3.1.2. Criterios de exclusión

Se excluirán los documentos de acuerdo a los criterios descritos en la siguiente lista:

- Los artículos escritos antes del año 2015 o sin fecha de publicación.
- Documentación con información no acorde al tema de investigación.
- Documentos que no indiquen el autor o bibliografía.

1.4. Búsqueda de estudios primarios

Una vez definido las cadenas y convenciones de búsqueda, así como los criterios de inclusión y exclusión se realizó la búsqueda de documentación bibliográfica en cada uno los repositorios anteriormente señalados. Además, se ha redefinido las cadenas de búsqueda de acuerdo a los operadores y términos que soporta cada buscador. Los resultados obtenidos de la búsqueda se muestran en la siguiente tabla.

TABLA I. RESULTADO DE BÚSQUEDA DE ESTUDIOS PRIMARIOS.

Biblioteca	Cadena de búsqueda	Resultados
Springer	(IP telephony OR ip pbx OR voip) security	29
ScienceDirect	(ip OR telephony OR pbx OR voip) and security	6
IEEE Xplore	(security AND (voip OR ip telephony OR ip pbx OR sip))	38
Google académico	allintitle: seguridad VoIP OR PBX OR IP OR telefonía	10
Google académico	allintitle: security VoIP OR PBX OR IP OR telephony	15
TOTAL		98

2. Desarrollo de la revisión

Una vez realizada la planificación, definiendo los parámetros y reglas a seguir durante el proceso de revisión sistemática, se continúa a una siguiente etapa que empieza con la selección de estudios primarios sobre la seguridad de las comunicaciones basadas en el protocolo IP.

2.1. Seleccionar los estudios primarios

En esta etapa se realiza un filtrado y selección de los artículos más relevantes referentes a la seguridad VoIP, de acuerdo a los criterios de inclusión y exclusión definidos en la atapa de planificación, estos artículos servirán como estudios primarios para su posterior análisis. Para obtener un resultado representativo de estos, el número mínimo recomendado de fuentes bibliográficas es de 25 artículos.

TABLA II. RESULTADO DE ARTÍCULOS EXCLUIDOS Y SELECCIONADOS

Biblioteca	Total	Excluidos	Selecionados
Springer	29	23	6
ScienceDirect	6	3	3
IEEE Xplore	38	23	15
Google académico	10	9	1
Google académico	15	13	2
TOTAL	98	70	27

Del total de las búsquedas, donde se han encontrado 98 coincidencias, se han analizado minuciosamente cada uno de ellos con la finalidad de escoger los artículos que aportan al tema en estudio, descartando los documentos repetidos. Finalmente se han seleccionado 27 artículos referentes al tema de estudio que se detallan en la siguiente tabla (Tabla III). Se ha asignado un código a cada uno de ellos para facilitar las referencias dentro de este trabajo.

TABLA III. LISTA DE ARTÍCULOS SELECCIONADOS

CÓD	TÍTULO	AUTOR	BIBLIOTECA
A001	Seguridad de la Telefonía IP en Ecuador: Análisis en Internet	Estrada, José Calva, Mayra Rodríguez, Ana Tipantuña, Christian	Google académico
A002	Audit Analysis Models, Security Frameworks and Their Relevance for VoIP	Gavilanez, Oscar Gavilanez, Franklin Rodriguez, Glen	Google académico
A003	Security Analysis of VoIP Networks Through Penetration Testing.	Ochang, Paschal A. Irving, Philip	Google académico
A004	Analysis of the IP telephony security issues using automatic neural network classifier	Rezac, Filip Rozhon, Jan Safarik, Jakub Voznak, Miroslav Bajakova, Zuzana	IEEE Explorer
A005	Comparative analysis on security techniques in VoIP environment	Shivankar, Simantini J. Tembhurkar, Manish P.	IEEE Explorer
A006	Performance analysis of intrusion prevention system on cyber security for voice over Internet protocol (VoIP)	Pomsathit, A.	IEEE Explorer
A007	ASIC design and implementation for VoIP intrusion prevention system	Chen, Ming-Jen Wen, Chih-Chao Lin, Hsin-Chen	IEEE Explorer

		Chu, Yuan-Sun	
A008	Application of Visual Analysis to Detect and Analyze Patterns in VoIP Attack Traffic	Volodina, Ekaterina Aziz, Adnan Rathgeb, Erwin P. Hossfeld, Tobias	IEEE Explorer
A009	SIP amplification attack analysis and detection in VoLTE service network	Ko, Author Eunhye Park, Seongmin Kim, Sekwon Son, Kyungho Kim, Hwankuk	IEEE Explorer
A010	Capture and Analysis of Malicious Traffic in VoIP Environments Using a Low Interaction Honeypot	da Silva Vargas, Ivan Riboldi Jordao Kleinschmidt, Joao Henrique	IEEE Explorer
A011	Securing SIP infrastructures with PKI — The análisis	Segec, P. Moravcik, M. Hrabovsky, J. Papan, J. Uramova, J.	IEEE Explorer
A012	An efficient and easily deployable method for dealing with DoS in SIP services	Tsiatsikas, Zisis Geneiatakis, Dimitris Kambourakis, Georgios Keromytis, Angelos D.	Science Direct
A013	An energy efficient authenticated key agreement protocol for SIP-based green VoIP networks	Zhang, Liping Tang, Shanyu Zhu, Shaohui	Science Direct
A014	Systems and methods for SPIT detection in VoIP: Survey and future directions	Ajmal Azad, Muhammad Morla, Ricardo Salah, Khaled	Science Direct
A015	VoIP-aware network attack detection based on statistics and behavior of SIP traffic.	Lee, Jonghan Cho, Kyumin Lee, Chang Yong Kim, Seungjoo	Springer
A016	Performance evaluation of framework of VoIP/SIP server under virtualization environment along with the most common security threats.	Kolhar, Manjur Alameen, Abdalla Gulam, Mujthaba	Springer
A017	Single round-trip SIP authentication scheme with provable security for Voice over Internet Protocol using smart card	Kumari, Saru Wu, Fan Li, Xiong Farash, Mohammad Sabzinejad Jiang, Qi Khan, Muhammad Khurram Das, Ashok Kumar	Springer
A018	Security analysis and improvement of two authentication and key agreement schemes for session initiation protocol	Arshad, Hamed Nikooghadam, Morteza	Springer
A019	Secure VOIP LTE network for secure transmission using PLRT (Packet Level Restraining Technique) under DDOS Attack	Shoket, Humma Aulakh, Jagdeep Singh	IEEE Explorer
A020	Comparison of signaling and media approaches to detect VoIP SPIT attack	Gad, Ahmed Fawzy	IEEE Explorer
A021	Comparative study on DOS attacks Detection Techniques in SIP-based VOIP networks	Safoine, Rababe Mounir, Soufyane Farchi, Abdelmajid	IEEE Explorer
A022	Coping with denial-of-service attacks on the IP telephony system	Cadet, Frantz Fokum, Daniel T.	IEEE Explorer
A023	An Empirical Study of Denial of Service (DoS) against VoIP	Yu, James	IEEE Explorer
A024	Mitigation of Flooding Based Denial of Service Attack against Session Initiation Protocol Based VoIP System	Shoket, Humma Aulakh, Jagdeep Singh	IEEE Explorer

A025	An empirical study of security of VoIP system	Ghafarian, Ahmad Seno, Seyed Amin Hosseini Dehghani, Maria	IEEE Explorer
A026	Development of a Distributed VoIP Honeypot System with Advanced Malicious Traffic Detection	Behan, Ladislav Sevcik, Lukas Voznak, Miroslav	Springer
A027	Aspects of Voice Communications Fraud	Helenport, Alexandre Tait, Bobby L.	Springer

Fase II: Realizar un estudio comparativo de la documentación bibliográfica seleccionada.

En esta fase se realiza el análisis del contenido de cada uno de los artículos, para hacer la extracción de información y conclusiones más relevantes de cada uno de ellos.

2.2. Evaluación de la calidad de los estudios

Para la evaluación de la calidad de cada una de las fuentes bibliográficas se han tomado en cuenta algunos parámetros que se detallan en la Tabla IV.

TABLA IV. EVALUACIÓN DE LOS ARTÍCULOS POR CRITERIOS DEFINIDOS

CÓD	Año de publicación	No de citaciones	Lugar de publicación.	DOI	BIBLIOTECA
A001	2016	0	Enfoque UTE	10.29019/enfoqueute.v7n2.93	Google académico
A002	2017	1	Computer Science (Cornell University)	http://arxiv.org/abs/1704.0244	Google académico
A003	2017	3	International Conference on Information and Software Technologies	10.1007/978-3-319-67642-5_50	Google académico
A004	2016	1	2016 24th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)	10.1109/SOFTCOM.2016.7772119	IEEE Explorer
A005	2015	4	2015 2nd International Conference on Electronics and Communication Systems (ICECS)	10.1109/ECS.2015.7124770	IEEE Explorer
A006	2015	1	11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015)	10.1049/cp.2015.0752	IEEE Explorer
A007	2016	1	2016 International Conference on Applied System Innovation (ICASI)	10.1109/ICASI.2016.7539941	IEEE Explorer
A008	2018	0	2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And	10.1109/TrustCom/BigDataSE.2018.00048	IEEE Explorer

			Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)		
A009	2016	2	2016 International Conference on Information Networking (ICOIN)	10.1109/ICOIN.2016.7427126	IEEE Explorer
A010	2015	9	IEEE Latin America Transactions	10.1109/TLA.2015.7069104	IEEE Explorer
A011	2017		2017 15th International Conference on Emerging eLearning Technologies and Applications (ICETA)	10.1109/ICETA.2017.8102525	IEEE Explorer
A012	2015	12	Computer Communications	10.1016/j.comcom.2014.11.002	Science Direct
A013	2016	11	Journal of Network and Computer Applications	10.1016/J.JNCA.2015.06.022	Science Direct
A014	2018	2	Computers & Security	10.1016/j.cose.2018.03.005	Science Direct
A015	2015	4	Peer-to-Peer Networking and Applications	10.1007/s12083-014-0289-8	Springer
A016	2018	0	Neural Computing and Applications	10.1007/s00521-017-2886-y	Springer
A017	2016	1	Multimedia Tools and Applications	10.1007/s11042-015-2988-4	Springer
A018	2015	17	The Journal of Supercomputing	10.1007/s11227-015-1434-8	Springer
A019	2018	0	2018 5th International Conference on Signal Processing and Integrated Networks (SPIN)	10.1109/SPIN.2018.8474211	IEEE Explorer
A020	2018	0	2018 International Conference on Innovative Trends in Computer Engineering (ITCE)	10.1109/ITCE.2018.8316600	IEEE Explorer
A021	2018	0	2018 6th International Conference on Multimedia Computing and Systems (ICMCS)	10.1109/ICMCS.2018.8525878	IEEE Explorer
A022	2016	8	SoutheastCon 2016	10.1109/SECON.2016.7506691	IEEE Explorer
A023	2016	2	2016 SAI Computing Conference (SAI)	10.1109/SAI.2016.7556105	IEEE Explorer
A024	2015	8	2015 IEEE International Conference on Computational Intelligence & Communication Technology	10.1109/CICT.2015.66	IEEE Explorer
A025	2016	2	2016 SAI Computing Conference (SAI)	10.1109/SAI.2016.7556105	IEEE Explorer
A026	2019	0	International Conference on Advanced Engineering Theory and Applications	10.1007/978-3-030-14907-9_40	Springer
A027	2016	0	International Conference on Global Security, Safety, and Sustainability	10.1007/978-3-319-51064-4_6	Springer

Como se puede apreciar en la tabla anterior, todos los artículos seleccionados sobre la seguridad VoIP tienen validez científica, ya sea porque están indexados con su respectivo identificador de objeto digital (DOI) de importantes revistas de ciencia y tecnología, publicados en los últimos cinco años; además, por un importante número de citaciones que reciben algunos, especialmente los más antiguos.

2.3. Extracción de los datos más relevantes.

Consiste en analizar cada uno de los artículos seleccionados y extraer la información más relevante que responda a la pregunta y el objetivo de la investigación. Los datos de cada artículo se encuentran sintetizadas en las siguientes tablas (Tabla V a Tabla XXXI).

TABLA V. RESULTADOS DEL ARTÍCULO A001

Artículo	**Seguridad de la Telefonía IP en Ecuador: Análisis en Internet**
Conclusiones relevantes [14]	Las marcas que han sufrido mayor afectación son: Elastix, Cisco y Avaya. Muchos de estos sistemas tienen ejecutando software desactualizado en sus servidores y por ello, son más vulnerables. La mayoría de IP-PBX funcionan con aplicaciones basadas en Asterisk como FreePBX y Elastix. Las implementaciones basadas en Asterisk están revelando demasiada información a través de Internet, debido a la "facilidad" que ofrecen las soluciones open source para su implementación. Se descubrieron graves amenazas a plataformas de telefonía IP basadas en Asterisk (Elastix) cuando éstas se conectan directamente a Internet sin adecuados mecanismos de protección. El uso de una u otra solución de telefonía no implica necesariamente una implementación vulnerable. Sin embargo, el empleo de versiones desactualizadas de software, la configuración incorrecta del plan de marcado, la innecesaria conexión a redes externas, y, en general, la falta de dominio técnico de la solución telefónica que se implementa (parámetros por defecto), frecuentemente derivan en fraude y un importante perjuicio económico para la víctima.

TABLA VI. RESULTADOS DEL ARTÍCULO A002

Titulo	**Audit Analysis Models, Security Frameworks and Their Relevance for VoIP**
Conclusiones relevantes [16]	Los ataques de ingeniería social no pueden prevenirse con las herramientas y el software actuales de seguridad. Los ataques de ingeniería social tienen poca importancia para los profesionales de VoIP, y los escritores e investigadores dedican su tiempo exclusivamente a temas de seguridad técnica. La ingeniería social sigue siendo quizás la amenaza más peligrosa para la seguridad de la información para cualquier empresa; en consecuencia, la ingeniería social sigue siendo un problema que debe ser abordado.

TABLA VII. RESULTADOS DEL ARTÍCULO A003

Titulo	**Security Analysis of VoIP Networks Through Penetration Testing.**
Conclusiones relevantes [17]	La convergencia de voz y datos proporciona preocupaciones de seguridad principalmente como resultado de la arquitectura VoIP y la arquitectura IP subyacente. Las vulnerabilidades existentes en las arquitecturas VoIP hacen surgir la necesidad de implementar procedimientos y metodologías estándar como las pruebas de penetración para identificar vulnerabilidades explotables que a su vez ayudarán a proporcionar mejoras de seguridad.

TABLA VIII. RESULTADOS DEL ARTÍCULO A004

Titulo	**Analysis of the IP telephony security issues using automatic neural network classifier**
Conclusiones relevantes [18]	De la mano con la tecnología VoIP, el riesgo de problemas de seguridad también aumenta. Los servidores de comunicaciones con frecuencia se eligen como objetivos de ataques para obtener acceso a las cuentas de usuario y causar un daño financiero al propietario. La mayoría de las soluciones VoIP comerciales y de código abierto actuales utilizan el Protocolo de inicio de sesión (SIP) para crear, administrar o terminar llamadas. SIP está basado en texto y, desafortunadamente, al igual que el protocolo HTTP no implementa ninguna medida de seguridad. Por lo tanto, una parte sustancial de todos los ataques a la infraestructura de VoIP se dirige precisamente a las debilidades en SIP. Al igual que otros servicios de Internet, también la telefonía IP es vulnerable a los ataques DoS / DDoS, donde el protocolo SIP sirve como una herramienta para enviar grandes cantidades de paquetes y agotar los parámetros de rendimiento de las soluciones SIP seleccionadas.

TABLA IX. RESULTADOS DEL ARTÍCULO A005

Titulo	**Comparative analysis on security techniques in VoIP environment**
Conclusiones relevantes [19]	Voip debido a su popularidad, se convierte en uno de los principales objetivos de los cyber-atacantes. Hay muchas amenazas posibles en VoIP tales como interrupciones o denegación de servicio (DoS), interceptación de llamadas y los ataques de autenticación. De toda la revisión bibliográfica de las técnicas de seguridad de VoIP, podemos decir que las técnicas de seguridad no son precisas y eficientes.

TABLA X. RESULTADOS DEL ARTÍCULO A006

Titulo	Performance analysis of intrusion prevention system on cyber security for voice over Internet protocol (VoIP)
Conclusiones relevantes [20]	Algunos ataques solamente son para sustraer datos sin afectar a la integridad del sistema, mientras que la Denegación de Servicio (DoS) apunta a destruir severamente el host que está sirviendo a los usuarios.

TABLA XI. RESULTADOS DEL ARTÍCULO A007

Titulo	ASIC design and implementation for VoIP intrusion prevention system
Conclusiones relevantes [21]	La tecnología VoIP sigue siendo muy progresiva, pero las estrategias de defensa se están quedando muy atrás. Por lo tanto, el ataque a sistemas VoIP es un problema muy serio. De acuerdo al monitoreo de organismos gubernamentales se ha revelado muchas de las vulnerabilidades de la seguridad VoIP. La organización especializada de investigación de seguridad VoIP VOIPSA (Voice over IP Alliance) presenta una lista de ataques VOIP, que se pueden dividir principalmente en Solicitud de inundación, mensaje con formato incorrecto, mensajes falsos e intercepción de llamadas.

TABLA XII. RESULTADOS DEL ARTÍCULO A008

Titulo	Application of Visual Analysis to Detect and Analyze Patterns in VoIP Attack Traffic
Conclusiones relevantes [22]	La telefonía IP se está convirtiendo en "simplemente otra" aplicación de Internet que es vulnerable a múltiples escenarios de ataques. VoIP está sujeta a esquemas de fraude conocidos, que atacan a los servicios de telefonía tradicionales, así como a las aplicaciones de Internet de hoy en día, ya que VoIP combina estas tecnologías, además, VoIP abre nuevas oportunidades para el mal uso y el fraude. Los servidores SIP, particularmente permiten el acceso desde redes externas, y están sujetos a intentos de registro fraudulentos (Registration Hijacking).

TABLA XIII. RESULTADOS DEL ARTÍCULO A009

Titulo	SIP amplification attack analysis and detection in VoLTE service network
Conclusiones relevantes [23]	El ataque de amplificación SIP ha surgido con el desarrollo de la tecnología de comunicación inalámbrica y la comercialización del servicio VoLTE. Para proporcionar el servicio de voz sobre la red LTE se utilizan el protocolo SIP, que es vulnerable al ataque de amplificación SIP y otras amenazas.

TABLA XIV. RESULTADOS DEL ARTÍCULO A010

Titulo	Capture and Analysis of Malicious Traffic in VoIP Environments Using a Low Interaction Honeypot
Conclusiones relevantes [24]	Una de las principales dificultades de VoIP son las relacionadas con la seguridad, con nuevos ataques que comprometen el entorno de producción. Un sistema que antes sufría, en su gran mayoría ataques a la infraestructura física, pasa ahora a ser vulnerable a todas las amenazas dirigidas a la pila de protocolo TCP/IP. También surgen ataques específicos dirigidos a los protocolos de voz, como SIP (Session Initiation Protocol), IAX (Intra-Asterisk Exchange) y RTP (Real-time Transport Protocol), entre otros. Es posible observar una serie de ataques destinados a la infraestructura VoIP, desde ataques iniciales, como el rastreo en busca de dispositivos SIP a ataques que comprometen la seguridad de la infraestructura.

TABLA XV. RESULTADOS DEL ARTÍCULO A011

Titulo	Securing SIP infrastructures with PKI — The analysis
Conclusiones relevantes [25]	Se identifica un conjunto de amenazas y ataques a la seguridad en el protocolo SIP, que puede provocar la interrupción de su entorno de comunicación. Los más comunes y más fáciles de encontrar son los ataques a la denegación de servicio (DoS). DoS se enfoca en la sobrecarga de recursos de víctimas o servicios al generar una gran cantidad de mensajes. También existen otros tipos de ataques SIP, como escuchas ilegales, robo o manipulación de la identidad, fraudes, correo no deseado, entre otros. Los ataques pueden ser dirigidos no solo desde el entorno externo, sino también desde el entorno interno, por lo tanto, la vulnerabilidad de cualquiera de los protocolos usados de la pila también compromete indirectamente la señalización SIP.

TABLA XVI. RESULTADOS DEL ARTÍCULO A012

Titulo	An efficient and easily deployable method for dealing with DoS in SIP services
Conclusiones relevantes [26]	La arquitectura y los servicios de voz sobre IP (VoIP) pueden ser susceptibles a una gran cantidad de ataques, entre ellos, la denegación de servicio (DoS) es quizás la más poderosa, ya que apunta a sobrecargar los recursos subyacentes de un servicio y hacer que sea inaccesible para los usuarios legítimos. Los ataques de bajo volumen de denegación de servicio (DoS), últimamente están en aumento y, sin duda, siguen siendo difíciles de detectar y repeler. SIP debe enfrentar varios problemas de seguridad principalmente debido a su naturaleza abierta y orientada al texto.

TABLA XVII. RESULTADOS DEL ARTÍCULO A013

Titulo	An energy efficient authenticated key agreement protocol for SIP-based green VoIP networks
Conclusiones relevantes [27]	Los paquetes de voz transmitidos a través de Internet no están protegidos en la mayoría de los entornos VoIP, la información del usuario podría verse fácilmente comprometida por varios ataques maliciosos. Dado que los datos de voz transmitidos a través de los entornos VoIP no están protegidos, la privacidad y la información de valor de los usuarios podrían verse comprometidas fácilmente por ataques inactivos o activos. En comparación con otros protocolos de señalización como H.323, SIP es más ligero y flexible. Sin embargo, la autenticación de SIP se hereda directamente de la autenticación HTTP, que es vulnerable a varios ataques, tales como ataques de suplantación de identidad, ataques de suplantación de contraseñas, ataques de suplantación de servidores, entre otros. Dado que las contraseñas del usuario se almacenan en la base de datos del servidor SIP, el adversario podría lanzar ataques de robo de contraseñas de los usuarios. Además, una persona privilegiada del servidor SIP podría robar fácilmente la tabla de identidad y verificación de contraseñas del servidor SIP y luego usar estas contraseñas para hacerse pasar por un usuario legal y acceder a otros servidores.

TABLA XVIII. RESULTADOS DEL ARTÍCULO A014

Titulo	Systems and methods for SPIT detection in VoIP: Survey and future directions
Conclusiones relevantes [28]	Se generó un aumento proporcional en el spam de VoIP y el SPam over Internet Telephony (SPIT), que son formas de abuso y fraude que pueden tener graves consecuencias y pérdidas financieras tanto para los proveedores de servicios como para los suscriptores. Las tarifas asequibles de llamadas de VoIP, su fácil integración con las redes IP y los servicios de valor agregado también han creado una oportunidad lucrativa para que los emisores de spam y los vendedores por teléfono inicien llamadas masivas y no solicitadas a través de VoIP. Las estadísticas recientes sobre el spam de telefonía han revelado que responder a una llamada de spam daría como resultado una pérdida estimada de alrededor de $ 475 millones anuales en los Estados Unidos. Además, la USFTC (US Federal Trade Communication) ha estimado que la pérdida anual atribuida a las actividades de estafas y correo no deseado alcanzó los $ 8,6 mil millones en ese país.

TABLA XIX. RESULTADOS DEL ARTÍCULO A015

Titulo	**VoIP-aware network attack detection based on statistics and behavior of SIP traffic.**
Conclusiones relevantes [29]	El servicio VoIP es vulnerable a varias amenazas de seguridad potenciales. Además, las soluciones de seguridad basadas en IP existentes no pueden proteger la información de las llamadas. El servicio VoIP tiene muchas vulnerabilidades de seguridad como DoS (Denegación de Servicio), SPIT y escuchas ilegales. Hereda todas las amenazas de la red IP e incluye nuevas amenazas de sus protocolos, incluyendo SIP (Session Initiation Protocol) y H.323. La red IP está abierta a cualquier usuario de Internet. En consecuencia, es más fácil acceder a sistemas VoIP, como servidores proxy, IP-PBX (Private Branch Exchange) y teléfonos IP. Los ataques DoS ya son comunes en otros servicios IP. Los ataques de VoIP-DoS son difíciles de detectar y mitigar con las soluciones de seguridad basadas en IP existentes, tales como firewalls e IPS (Sistema de prevención de intrusiones). El segundo método de ataque es el SPAM de VoIP.

TABLA XX. RESULTADOS DEL ARTÍCULO A016

Titulo	**Performance evaluation of framework of VoIP/SIP server under virtualization environment along with the most common security threats.**
Conclusiones relevantes [30]	El phishing o vishing se utilizan de forma generalizada y amplia en una llamada VoIP. Un Softphone requiere Internet para hacer llamadas; en consecuencia, estos dispositivos están considerablemente expuestos a las amenazas de virus y malware. El SPIT es común para los usuarios VoIP. Un remitente de correo no deseado utiliza la dirección IP, que está asociada con cada teléfono VoIP, para enviar correo basura al buzón de correo de voz. La manipulación de llamadas VoIP es otra forma de espionaje. Las amenazas para VoIP están básicamente asociadas con la infraestructura de red y no con los puntos finales, ya que estos puntos finales pueden utilizar las herramientas de protección contra virus y malware o el sistema de detección de intrusos (IDS) existentes en la red. Amenazas como las escuchas ilegales, el man-in-the-midle y SPIT necesitan la intervención de un servidor para proteger a la red de daños adicionales. La amenaza vishing puede ser protegida personalmente porque requiere la persona y no el antivirus, IDS o malware.

TABLA XXI. RESULTADOS DEL ARTÍCULO A017

Titulo	**Single round-trip SIP authentication scheme with provable security for Voice over Internet Protocol using smart card.**
Conclusiones relevantes [31]	Para varias aplicaciones IP, incluyendo VoIP, el tema del Protocolo de inicio de sesión (SIP) ha atraído mayor preocupación a los investigadores. SIP utiliza protocolos de autenticación como el Protocolo simple de transporte de correo (SMTP) y el Protocolo de transporte de hipertexto (HTTP). Al ser un protocolo basado en canales inseguros, un protocolo de autenticación SIP es susceptible a amenazas, por lo tanto, la seguridad es una gran preocupación en los mecanismos de autenticación SIP.

TABLA XXII. RESULTADOS DEL ARTÍCULO A018

Titulo	**Security analysis and improvement of two authentication and key agreement schemes for session initiation protocol**
Conclusiones relevantes [32]	El método de autenticación convencional para SIP es la autenticación HTTP, que es insegura contra varios ataques de seguridad. Los sistemas de telefonía basados en IP son propensos a varios ataques de seguridad. Por ejemplo, un adversario puede hacerse pasar por un usuario legal y recibir llamadas dirigidas al usuario víctima. El adversario también podría hacer llamadas de larga distancia gratuitas en nombre del usuario víctima. Además, el adversario puede escuchar el canal de comunicación y modificar la información que se transmite entre las partes. Un mecanismo seguro para la autenticación y la negociación de claves es capaz de proporcionar varios aspectos de seguridad para los sistemas de telefonía basados en IP.

TABLA XXIII. RESULTADOS DEL ARTÍCULO A019

Titulo	**Secure VOIP LTE network for secure transmission using PLRT (Packet Level Restraining Technique) under DDOS Attack**
Conclusiones relevantes [33]	La red VOIP está amenazada de ataques maliciosos. Primero, la denegación de servicio (DOS) que puede causar el mal funcionamiento de algunos recursos de la red o caída del sistema en general al generar paquetes maliciosos. Segundo, los piratas informáticos son capaces de bloquear los paquetes con propósitos maliciosos. Tercero, el servicio de gestión de perfil de usuario puede tener acceso no autorizado. Finalmente, el SPIT se puede enviar a los usuarios en Internet.

TABLA XXIV. RESULTADOS DEL ARTÍCULO A020

Titulo	**Comparison of signaling and media approaches to detect VoIP SPIT attack**
Conclusiones relevantes [34]	Los atacantes pueden usar el protocolo SIP para crear amenazas de seguridad de redes VoIP.

	Uno de los ataques recientes en las redes VoIP se llama Spam sobre telefonía por Internet (SPIT). Este ataque crea llamadas de spam que se envían a los usuarios conectados a Internet. Debido a que todas las llamadas se establecen mediante SIP, SPIT hace uso de sus mensajes y campos para crear los mensajes más probables.

TABLA XXV. RESULTADOS DEL ARTÍCULO A021

Titulo	**Comparative study on DOS attacks Detection Techniques in SIP-based VOIP networks**
Conclusiones relevantes [35]	Al ser un protocolo basado en texto e implementado en un entorno abierto, SIP está expuesto a varias amenazas de seguridad, incluida la inundación. Uno de los ataques más conocidos es la denegación de servicio. Dado esto, se diseñaron numerosas técnicas de detección de inundaciones. VoIP tiene sus propios inconvenientes, y la seguridad es uno de ellos, especialmente cuando el atacante usa las redes VoIP para poner en peligro la confidencialidad de la información del usuario. Además, a medida que aumenta el número de suscriptores de VoIP, las formas en que los atacantes lideran actividades maliciosas también se expanden. Entre los ataques más destacados están la denegación de servicio o Inundaciones y ataques provenientes de intrusiones que obstruyen las comunicaciones privadas no protegidas. En los últimos años, una gran cantidad de investigaciones se centraron en mejorar la seguridad de VoIP mediante la fusión de diferentes mecanismos como la autenticación y el cifrado, así como las pautas de seguridad para proteger las infraestructuras VoIP, mientras que los riesgos de seguridad en estas comunicaciones han aumentado. Los ataques de inundación se consideran uno de los ataques más comunes en diferentes tipos de mensajes SIP.

TABLA XXVI. RESULTADOS DEL ARTÍCULO A022

Titulo	**Coping with denial-of-service attacks on the IP telephony system**
Conclusiones relevantes [36]	VoIP a menudo se implementa en un entorno abierto; por lo tanto, está sujeto a las mismas amenazas, por ejemplo, ataques de denegación de servicio (DoS). Como VoIP se ejecuta en la red IP, es vulnerable a las fallas de las redes de datos subyacentes. El tráfico de voz, al igual que el tráfico de datos, está expuesto a las mismas amenazas de seguridad de Internet. VoIP también hereda las vulnerabilidades existentes de las aplicaciones, sistemas operativos y protocolos de los que depende. Los ataques DoS son un problema serio que enfrentan los sistemas VoIP. El impacto de estos ataques en la telefonía IP puede variar. El impacto abarca desde consumidores molestos al interrumpir la

	disponibilidad y la disminución de la calidad de servicio (QoS); a graves pérdidas financieras para los operadores de VoIP. Hacer que la infraestructura VoIP sea tan segura como el sistema telefónico tradicional es un desafío para los investigadores de seguridad. Los ataques DoS y DDoS hacen que los componentes específicos, como los servidores VoIP y los teléfonos IP, del sistema de telefonía se vuelvan inutilizables. La mayoría de estos ataques se llevan a cabo contra la capa de aplicación de la infraestructura. Es relativamente fácil lanzar ataques DoS en dispositivos basados en SIP inundándolos con un gran número de solicitudes de llamada o mensajes SIP no válidos. Debido a la flexibilidad de la telefonía IP, hay varios tipos posibles de ataques DoS que pueden lograrse de varias maneras.

TABLA XXVII. RESULTADOS DEL ARTÍCULO A023

Titulo	**An Empirical Study of Denial of Service (DoS) against VoIP**
Conclusiones relevantes [37]	Además del ataque de inundación de REGISTRO, también identificamos el ataque de inundación INVITE que son capaces de provocar un ataque de denegación de servicio (DoS). Hay un aumento en los ataques de seguridad contra IP-PBX. Sus hallazgos muestran que el servidor Asterisk es más vulnerable que OpenSIPS para los ataques de inundación. También reconocemos que los servidores Asterisk son más vulnerables a los ataques DoS que otros servidores basados en SIP como se informa en otros estudios. Esto destaca la gravedad del problema y requiere un esfuerzo proactivo continuo por parte de los profesionales de la red.

TABLA XXVIII. RESULTADOS DEL ARTÍCULO A024

Titulo	**Mitigation of Flooding Based Denial of Service Attack against Session Initiation Protocol Based VoIP System**
Conclusiones relevantes [38]	La naturaleza basada en texto de los mensajes SIP ofrece más oportunidades para que los atacantes realicen ataques contra la integridad, confidencialidad y disponibilidad. Algunos ataques relacionados con la propiedad intelectual, como rastreo, suplantación de identidad, denegación de servicio, ataques de repetición y ataques de hombre en el medio son posibles en SIP. También son posibles muchos ataques específicos de SIP como terminaciones falsas y registros falsos. Los dispositivos SIP son bastante vulnerables a ataques DoS basados en inundaciones. El bombardeo excesivo del mensaje INVITE bloquea el servidor SIP.

TABLA XXIX. RESULTADOS DEL ARTÍCULO A025

Titulo	An empirical study of security of VoIP system
Conclusiones relevantes [39]	A medida que los servicios VoIP (voz sobre IP) son cada vez más populares, aumentan los distintos tipos de ataques contra ellos. SIP está sujeto a varios tipos de ataques, incluido el ataque de denegación de servicio (DoS). SIP, que forma la base de VoIP, se basa en los estándares de código abierto de Asterisk en los que los mensajes se transmiten en texto claro sin cifrar, por lo tanto, está sujeto a varios tipos de ataques. Los ataques comunes contra SIP incluyen escuchas ilegales, secuestro de conexiones, fraude de llamadas y ataques DoS. Existen tres tipos de ataques DoS que pueden lanzarse contra la infraestructura VoIP, la explotación de fallas de implementación, la explotación de vulnerabilidades sintácticas a nivel de la aplicación y la inundación del servidor SIP. Para mitigar los ataques DoS contra SIP, la implementación de IDS (Sistema de Detección de Intrusos) basada en la red es una práctica común.

TABLA XXX. RESULTADOS DEL ARTÍCULO A026

Artículo	Development of a Distributed VoIP Honeypot System with Advanced Malicious Traffic Detection
Conclusiones relevantes [40]	El creciente interés en los servicios VoIP atrae cada vez más atención en los círculos de piratería. Si bien continuamente se descubren nuevos mecanismos de defensa y se trata de mejorar los sistemas de seguridad para proteger la infraestructura de VoIP con regularidad, el error es mantener el ritmo de los atacantes que en su mayoría están un paso adelante para descubrir las debilidades del sistema. Los ataques de inundación representan ataques típicos que pueden agotar las fuentes disponibles de servidores VoIP y también pueden afectar la calidad del habla o el rendimiento general de la infraestructura. El SPIT pertenece a una de las amenazas importantes en la infraestructura VOIP, representa la mayor parte de las llamadas no solicitadas enviadas a través de redes VoIP. El ataque más común es la inundación de REGISTRO, que los atacantes usaron en el 79% de todos los ataques. En el 45% de los casos, los atacantes suan inundación de mensajes INVITE. Mientras que el ataque de inundación con mensajes OPTIONS se presentan solamente en el 5% de los casos.

TABLA XXXI. RESULTADOS DEL ARTÍCULO A027

Artículo	Aspects of Voice Communications Fraud
Conclusiones relevantes [41]	La reciente evolución de la telefonía VoIP ha creado nuevos vectores de explotación. Más allá de esos nuevos vectores de explotación, también ha aumentado en gran medida la cantidad de sistemas

	telefónicos que están expuestos, directa o indirectamente, a redes de datos públicas y privadas expuestas al fraude. Las encuestas han demostrado que, en los últimos diez años, la pérdida global por fraude en las comunicaciones de voz oscila entre $40 mil millones y $60 mil millones, lo que representa entre el 10 y el 15% del costo total de delitos cibernéticos. Este número no representa las pérdidas relacionadas con ataques de denegación de servicio (DoS). El fraude de comunicaciones de voz se puede dividir en cuatro categorías principales: Fraude telefónico, violación de la privacidad, suplantación de identidad y denegación de servicio. Los datos adquiridos ilegítimamente a través de las comunicaciones de voz también se utilizan como un medio para facilitar otros delitos cibernéticos en otras áreas.

Todos los estudios analizados han sido filtrados de acuerdo a los criterios de selección e inclusión establecidas, y extraídas de fuentes revisadas científicamente, por lo tanto, esta información es útil y válida para esta investigación.

2.4. Análisis de estudios seleccionados

En Tabla XXXII se puede visualizar los aspectos de seguridad relacionados a los sistemas VoIP abordados en cada uno de los artículos seleccionados.

TABLA XXXII. COMPARATIVA DE SEGURIDAD VOIP

CÓD	VoIP considerado inseguro	Poca importancia Ing. Social	Seguridad no ha desarrollado	Vulnerabilidades				Amenazas			
				Software desactualizado	Configuración deficiente	Vulnerabilidades de SIP	Heredadas de IP	DoS	Ingeniería social	Intercepción de llamada	SPIT
A001				X	X						
A002		X							X		
A003						X	X				
A004							X	X			
A005	X		X					X		X	
A006								X			
A007	X		X							X	
A008	X					X	X				
A009						X					
A010						X	X				
A011								X			
A012						X		X			
A013						X	X				
A014							X		X		X
A015							X	X			
A016									X		X

A017						X					
A018						X					
A019								X			
A020						X					X
A021	X					X		X			
A022							X	X			
A023								X			
A024						X		X			
A025			X			X					
A026			X								X
A027			X								

En las figuras 9 y 10, se han realizado una representación gráfica tanto de las causas más comunes que provocan la inseguridad, así como las amenazas más frecuentes en las redes VoIP.

La Figura 9 indica que una de las causas más comunes que influyen en la seguridad de las redes VoIP es la vulnerabilidad del protocolo SIP, esto representa un 55% de los artículos revisados; en segundo lugar, están las vulnerabilidades que hereda del protocolo TCP/IP (36%), mientras que otras causas menos frecuentes son el uso de software desactualizado y configuración deficiente que representan el 4% y 5% respectivamente.

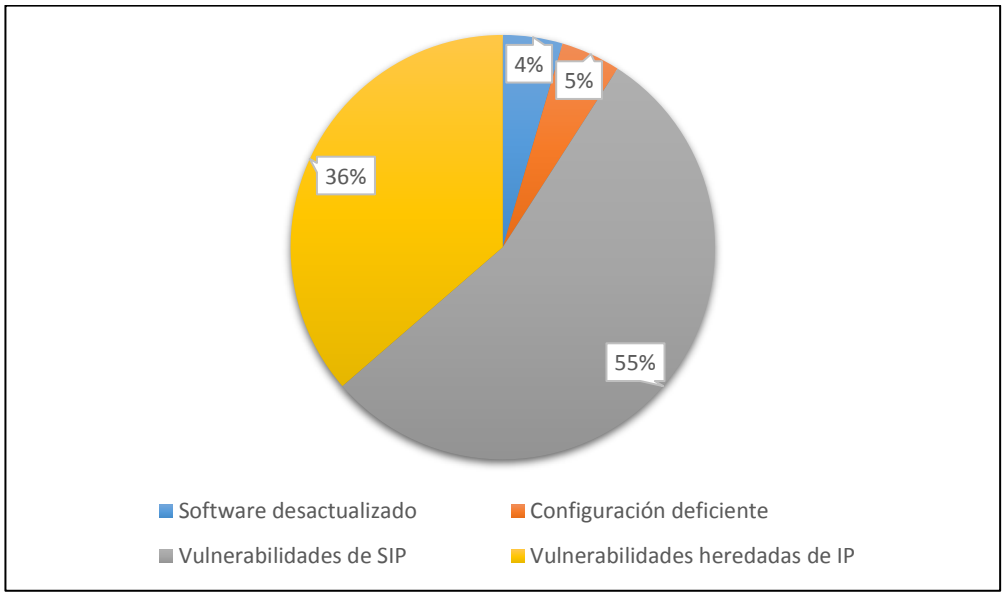


Figura 9. Causas más frecuentes que afectan la seguridad en sistemas VoIP

Analizados los artículos seleccionaos se deduce que una de las amenazas más comunes en las redes VoIP es la denegación de servicios (DoS), ya que el 55% de los artículos revisados consideran como la más frecuente, un 20% de las amenazas son

producidos por SPIT, mientras que la ingeniería social (Vishing) representa un 15% de las amenazas, finalmente la interceptación de llamadas representa un 10% (Figura 10).

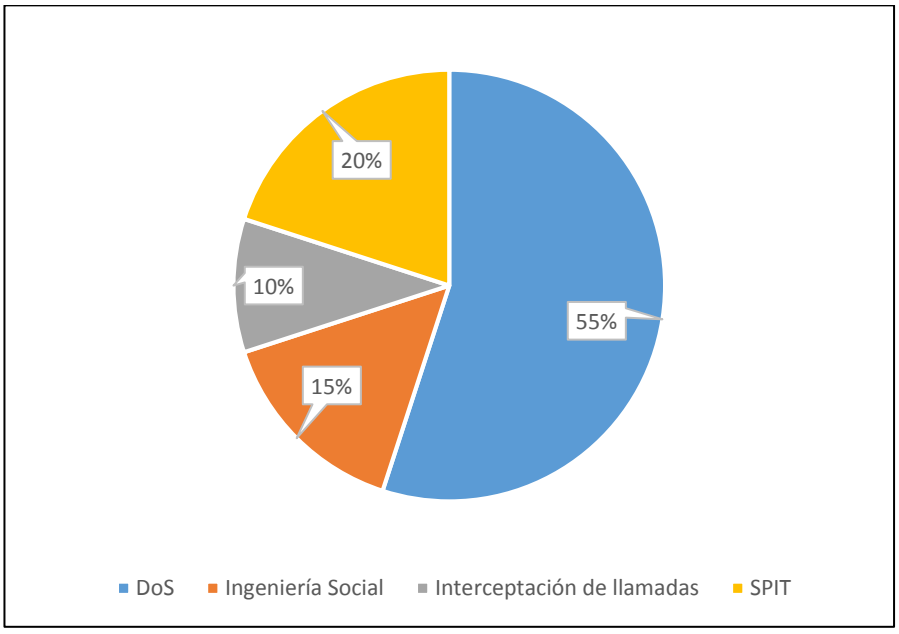


Figura 10. Amenazas más comunes en las redes VoIP

Fase III: Analizar la información relevante de la documentación bibliográfica.

Esta etapa comprende el análisis de la información obtenida de las fuentes primarias y la presentación de resultados.

3. Resultados obtenidos a partir de los estudios seleccionados.

La seguridad de las comunicaciones VoIP es un tema muy importante a ser debatido con la finalidad de garantizar un mejor servicio a los usuarios de esta tecnología, ya que con la expansión de este servicio esto ha sido el objetivo de los piratas informáticos y personas inescrupulosas.

TABLA XXXIII. ANÁLISIS Y RESULTADOS OBTENIDOS SOBRE SEGURIDAD VOIP

Aspectos de seguridad de las redes VoIP	Artículos Relacionados
Los sistemas VoIP son altamente vulnerables e inseguros frente a los ataques maliciosos.	A005, A007, A008 y A021

La ingeniería social es un problema muy serio en las comunicaciones, pero que sin embargo se ha dado mayor importancia a la seguridad de carácter técnico (DoS, hombre en el medio, Interceptación de llamadas, SPIT, entre otros).	A002, A014 y A016
La seguridad de las comunicaciones basadas en IP no ha avanzado a la par con el desarrollo de esta tecnología, por lo que estos sistemas tienden a ser cada vez más vulnerables.	A005, A007, A025, A026, A027
Si bien podemos deducir que los sistemas de software libre son más vulnerables a estos ataques, no porque son arquitectónicamente más susceptibles, sino por la facilidad de configuración, las configuraciones por defecto y a las versiones desactualizadas que manejan en sus servidores.	A001
El protocolo más utilizado es el SIP, sin embargo, es un protocolo ligero y basado en texto plano, por lo cual es mucho más vulnerables frente a ataques maliciosos que afectarían la integridad del sistema.	A004, A008, A009, A010, A012, A013, A017, A018, A020, A021, A024 y A025
Indican que la tecnología VoIP ha heredado las mismas vulnerabilidades del protocolo TCP/IP, tales como DoS y manipulación de señal.	A003, A004, A008, A010, A013, A014, A015 y A022
Los ataques DoS son más comunes en los sistemas de comunicación VoIP de acuerdo a los artículos estudiados, donde se menciona y se enfatiza como la principal amenaza a la seguridad.	A004, A005, A006, A011, A012, A015, A019, A021, A022, A023 y A024
El SPIT ocupa también un lugar muy importante dentro de las amenas de seguridad a los sistemas VoIP. Las redes VoIP en los últimos años ha sufrido un aumento proporcional de SPAM y SPIT, generando graves pérdidas económicas a los proveedores y abonados. Solamente en Estados Unidos se estima que las pérdidas relacionadas a actividades de estafas atribuidas a SPIT alcanzan los 8,6 mil millones anuales.	A014, A016, A020 Y A026
Otra de las amenazas como la intercepción de llamadas, no ha sido considerada como frecuente en la mayoría de los artículos revisados, ya que solamente dos artículos han considerado como amenaza principal.	A005 y A016

g. Discusión

1. Desarrollo de la propuesta alternativa

Se ha propuesto el presente trabajo de investigación con la finalidad de hacer una revisión de bibliografía referente a temas de seguridad en las comunicaciones VoIP, debido a la importancia que tienen estas comunicaciones en la actualidad, y por lo tanto la seguridad debe ser un tema a ser analizado profundamente a fin de ofrecer a los usuarios un servicio eficiente y seguro.

1.1. Seleccionar documentación bibliográfica de la seguridad en los sistemas VoIP más utilizados en la actualidad.

La selección de documentación se ha realizado basando en los parámetros establecidos durante la etapa de planificación (Planificación de la revisión, página 31), tales como: año de publicación comprendido dentro de los últimos cinco años, fuentes de búsqueda, formato del documento y la pertinencia al tema en estudio. En base a los parámetros establecidos se ha seleccionado un total de 27 artículos de alto contenido científico sobre la seguridad de las comunicaciones VoIP (ver Tabla III), los mismos que están publicados en bases de datos especializados.

Considerando que los artículos seleccionados cumplen con los parámetros establecidos, son elegios como estudios primarios válidos para la revisión sistemática de literatura propuesta.

1.2. Realizar un estudio comparativo de la documentación bibliográfica seleccionada.

Una vez seleccionado los estudios primarios, en esta etapa se ha verificado la calidad científica de la documentación, asegurando que todos estos artículos son aptos para la revisión sistemática de literatura propuesta. Como se puede apreciar en la Tabla IV, toda la bibliografía está indexada y publicada en revistas científicas.

La extracción de los resultados de cada uno de los artículos se ha realizado mediante tablas (Tabla V - Tabla XXXI), donde se encuentra resumida la información más relevante que cada uno de los artículos aporta al tema de investigación, que es la seguridad de las redes VoIP.

En todos los estudios se han encontrado información importante que ha contribuido a la síntesis del tema en estudio y la obtención de conclusiones. Si bien muchos artículos tienen diferentes criterios, la gran mayoría coincide en que el principal objetivo es promover la seguridad en los sistemas de comunicación VoIP.

En la Tabla XXXII se puede apreciar los aspectos más importantes sobre la seguridad en los sistemas VoIP, obtenidos de cada uno de los artículos seleccionados para esta etapa de revisión.

1.3.Analizar la información relevante de la documentación bibliográfica.

Las vulnerabilidades de los sistemas VoIP se ha representado en la Figura 9, donde se puede apreciar que las debilidades del protocolo SIP y la pila TCP/IP son las causas más importantes para los ataques a una red VoIP.

En cuanto a las amenazas, a las que mayor hacen mención en los artículos revisados y consideran más frecuentes es la denegación de servicios (DoS) y otros como interceptación de llamadas (Figura 10). Mientras que, la mayoría de los autores y sobre todo especialistas en seguridad VoIP se centran solamente en desarrollar mecanismos para la protección de la infraestructura, también hay otras amenazas que son muy importantes como la ingeniería social, que pueden causar perjuicios económicos a los usuarios, sin embargo, se ha dado poca importancia a este tema.

Muchos autores hacen referencia a que la seguridad de sistemas de comunicación basadas en VoIP es un área que ha quedado muy atrás de los avances de esta tecnología.

Los resultados obtenidos se han resumido en una tabla (Tabla XXXIII), donde se puede evidenciar la información relevante que ha aportado cada uno de los artículos en estudio.

2. Valoración técnica, económica y social

El presente trabajo de titulación ha contribuido en diferentes aspectos como son:

2.1. Valoración técnica

Este trabajo contribuye a los investigadores en las áreas afines a la seguridad en redes VoIP a conocer las actuales vulnerabilidades y amenazas más frecuentes a las que cotidianamente son expuestas.

2.2. Valoración económica

El trabajo realizado no ha excedido de los límites presupuestados, ya que se han utilizado herramientas de software libre; para la consulta bibliográfica, se ha hecho uso de bibliografía de acceso libre. Además, la Universidad Nacional de Loja ha contribuido con sus instalaciones y personal de apoyo durante el desarrollo del presente trabajo.

2.3. Valoración social

Los resultados del presente trabajo aporta con información sintetizada sobre la seguridad de las comunicaciones basadas en VoIP, que permitirá a los lectores conocer sobre la realidad actual de la seguridad que ofrece esta tecnología.

h. Conclusiones

- La telefonía IP en la actualidad es un servicio generalizado a nivel mundial, sin embargo, esta expansión trae consigo problemas de seguridad, ya que una red VoIP está conectado directamente a Internet y esto hace que sea mundialmente accesible. Si bien se han implementado mecanismos para mitigar estas amenazas (DoS, SPIT, Vishing), la seguridad es un tema que no se ha desarrollado a la par de las comunicaciones VoIP, por consiguiente, basándose en el análisis realizado se concluye que las redes VoIP son altamente vulnerables e inseguras.

- Para garantizar que la información obtenida sea válida para la investigación propuesta, uno de los parámetros principales es que los artículos científicos se encuentren publicados dentro de los últimos cinco años, encontrando en los repositorios seleccionados información y bibliografía suficiente referentes al tema de seguridad en las comunicaciones VoIP, que cumplen con los parámetros o filtros establecidos para la presente investigación.

- Mediante el análisis comparativo realizado entre todos los artículos que han superado los filtros establecidos como: año de publicación, pertinencia al tema, formato del documento e idioma; se ha podido concluir que toda la documentación seleccionada está relacionada a un mismo tema como es un enfoque a la seguridad de las comunicaciones en la actualidad, las amenazas más comunes y las causas que lo originan.

- La mayoría de los estudios analizados concuerdan en que los problemas de seguridad de las comunicaciones basadas en voz sobre IP están relacionadas a la vulnerabilidad del protocolo SIP y otros derivados de TCP/IP. Así mismo hacen referencia al ataque de denegación de servicios como el problema más común.

i. Recomendaciones

Concluida la investigación, se recomienda lo siguiente:

- Definir correctamente la cadena de búsqueda utilizando los operadores admitidos por el buscador de cada una de las bases de datos científicas, con la finalidad de obtener mayor éxito en la búsqueda de fuentes primarias, para lograr resultados óptimos y acordes a la temática propuesta.

- Delimitar la búsqueda de manera que las palabras clave coincidan solamente en títulos y metadatos de los artículos, mas no en todo el cuerpo del documento. De esta manera el buscador devuelve solamente resultados relacionados a la temática propuesta excluyendo los artículos que no aportan al tema de estudio.

- Dar mayor importancia a la prevención de otros tipos de amenazas en las comunicaciones VoIP como la ingeniería social, que, si bien no es generado por una vulnerabilidad en la infraestructura de la red, también ha generado muchos perjuicios a los usuarios de la telefonía IP.

- En vista de que el protocolo SIP es considerado muy vulnerable a los ataques informáticos por estar basado en texto plano, una posibilidad es la utilización de protocolos alternativos como IAX2 o H.323, ya que estos protocolos permiten el cifrado de las comunicaciones.

j. Bibliografía

[1] P. G. Maldonado Mendieta, «Esquema de seguridad para una central VoIP, en software libre en su implementación Elastix,» 2016. [En línea]. Available: http://repositorio.puce.edu.ec/handle/22000/11292.

[2] K. Watkins, «Las vulnerabilidades de VoIP,» McAfee, S.A., Madrid.

[3] G. d. R. Veloz Remache, «Análisis de vulnerabilidades a nivel de capa de aplicación en la transmisión de VoIP aplicado en una intranet,» *Maskana,* vol. 5, nº Ed. Espeial, 2016.

[4] B. Hartpence, Packet Guide to Voice over IP, USA: O'Reilly Media, Inc., 2013.

[5] M. J. Liberona Campos, «Seguridad en voz sobre IP,» Universidad Técnica Federico Santa María, Valparaiso, 2010.

[6] Asterisk project, «Asterisk,» [En línea]. Available: https://www.asterisk.org. [Último acceso: 21 octubre 2018].

[7] R. Soria Vargas, M. A. Acevedo Mosqueda, J. Hernández Castillo y M. Sánchez Meraz, «Sistema de video llamadas seguras empleando una PBX-Asterisk,» *Red de Revistas Científicas de América Latina y el Caribe, España y Portugal,* vol. 2, nº 19, pp. 47-51, 2015.

[8] Elastix.org, «Elastix. Freedom to communicate,» [En línea]. Available: https://www.elastix.org. [Último acceso: 23 octubre 2018].

[9] Issabel Project, «Issabel.org,» [En línea]. Available: https://www.issabel.org/. [Último acceso: 23 octubre 2018].

[10] A. Santana Vázquez, Consideraciones sobre la Seguridad en las redes de Telecomunicaciones soportes de voz sobre IP (VoIP) en Cuba, Cuba: UNIVERSIDAD CENTRAL "MARTA ABREU" DE LAS VILLAS., 2007.

[11] J. K. Arellano Aucancela, MODELO DE SEGURIDAD CONTRA ATAQUES DE DENEGACIÓN DE SERVICIO (DoS) DE TRÁFICO SIP EN SERVICIOS VOIP PARA REDES LAN CORPORATIVAS., Riobamba: Escuela Superior Politécnica de Chimborazo, 2017.

[12] N. Dawson Díaz y V. Vega Zepeda, «Ejecución de una revisión sitemática en gestión de requerimientos de software para pequeños entornos.,» de *ResearchGate*, Chile, 2015.

[13] E. Fernández Medina, M. Piattini, C. Calero, C. Gutiérrez y A. María, «Análisis y revisión de la literatura en el contexto de proyectos de fin de carrera: Una propuesta,» *ResearchGate,* 2005.

[14] E. José, M. Calva, A. Rodríguez y C. Tipantuña, «Seguridad de la Telefonía IP en Ecuador: Análisis en Internet,» *Enfoque UTE,* vol. 7, nº 2, pp. 25-40, 2017.

[15] O. Gavilanez, F. Gavilanez y G. Rodriguez, «Audit Analysis Models, Security Frameworks and Their Relevance for VoIP,» 2017.

[16] P. A. Ochang y P. Irving, «Security Analysis of VoIP Networks Through Penetration Testing,» pp. 601-610, 2017.

[17] F. Rezac, J. Rozhon, J. Safarik, M. Voznak y Z. Bajakova, «Analysis of the IP telephony security issues using automatic neural network classifier,» *2016 24th International Conference on Software, Telecommunications and Computer Networks (SoftCOM),* pp. 1-5, 2016.

[18] S. J. Shivankar y M. P. Tembhurkar, «Comparative analysis on security techniques in VoIP environment,» *2015 2nd International Conference on Electronics and Communication Systems (ICECS),* pp. 1176-1180, 2015.

[19] A. Pomsathit, «Performance analysis of intrusion prevention system on cyber security for voice over Internet protocol (VoIP),» *11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015),* pp. 1-5, 2015.

[20] M.-J. Chen, C.-C. Wen, H.-C. Lin y Y.-S. Chu, «ASIC design and implementation for VoIP intrusion prevention system,» *2016 International Conference on Applied System Innovation (ICASI),* pp. 1-4, 2016.

[21] E. Volodina, A. Aziz, E. P. Rathgeb y T. Hossfeld, «Application of Visual Analysis to Detect and Analyze Patterns in VoIP Attack Traffic,» *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE),* pp. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018.

[22] A. E. Ko, S. Park, S. Kim, K. Son y H. Kim, «SIP amplification attack analysis and detection in VoLTE service network,» *2016 International Conference on Information Networking (ICOIN),* pp. 334-336, 2016.

[23] I. R. J. da Silva Vargas y J. H. Kleinschmidt, «Capture and Analysis of Malicious Traffic in VoIP Environments Using a Low Interaction Honeypot,» *IEEE Latin America Transactions,* vol. 13, nº 3, pp. 777-783, 2015.

[24] P. Segec, M. Moravcik, J. Hrabovsky, J. Papan y J. Uramova, «Securing SIP infrastructures with PKI — The analysis,» *2017 15th International Conference on Emerging eLearning Technologies and Applications (ICETA),* pp. 1-8, 2017.

[25] Z. Tsiatsikas, D. Geneiatakis, G. Kambourakis y A. D. Keromytis, «An efficient and easily deployable method for dealing with DoS in SIP services,» *Computer Communications,* vol. 57, pp. 50-63, 2015.

[26] L. Zhang, S. Tang y S. Zhu, «An energy efficient authenticated key agreement protocol for SIP-based green VoIP networks,» *Journal of Network and Computer Applications,* vol. 59, pp. 126-133, 2016.

[27] M. Ajmal Azad, R. Morla y K. Salah, «Systems and methods for SPIT detection in VoIP: Survey and future directions,» *Computers & Security,* vol. 77, pp. 1-20, 2018.

[28] J. Lee, K. Cho, C. Y. Lee y S. Kim, «VoIP-aware network attack detection based on statistics and behavior of SIP traffic.,» *Peer-to-Peer Networking and Applications,* vol. 8, nº 5, pp. 872-880, 2015.

[29] M. Kolhar, A. Alameen y M. Gulam, «Performance evaluation of framework of VoIP/SIP server under virtualization environment along with the most common security threats.,» *Neural Computing and Applications,* vol. 30, nº 9, pp. 2873-2881, 2018.

[30] S. Kumari, F. Wu, X. Li, M. S. Farash, Q. Jiang, M. K. Khan y A. K. Das, «Single round-trip SIP authentication scheme with provable security for Voice over Internet Protocol using smart card.,» *Multimedia Tools and Applications,* vol. 75, nº 24, pp. 17215-17245, 2016.

[31] H. Arshad y M. Nikooghadam, «Security analysis and improvement of two authentication and key agreement schemes for session initiation protocol,» *The Journal of Supercomputing,* vol. 71, nº 8, pp. 3163-3180, 2015.

[32] H. Shoket y J. S. Aulakh, «Secure VOIP LTE network for secure transmission using PLRT (Packet Level Restraining Technique) under DDOS Attack,» *2018 5th International Conference on Signal Processing and Integrated Networks (SPIN),* pp. 878-882, 2018.

[33] A. F. Gad, «Comparison of signaling and media approaches to detect VoIP SPIT attack,» *2018 International Conference on Innovative Trends in Computer Engineering (ITCE),* pp. 56-62, 2018.

[34] R. Safoine, S. Mounir y A. Farchi, «Comparative study on DOS attacks Detection Techniques in SIP-based VOIP networks,» *2018 6th International Conference on Multimedia Computing and Systems (ICMCS),* pp. 1-5, 2018.

[35] F. Cadet y D. T. Fokum, «Coping with denial-of-service attacks on the IP telephony system,» *SoutheastCon 2016,* pp. 1-7, 2017.

[36] A. Ghafarian, S. A. H. Seno y M. Dehghani, «An Empirical Study of Denial of Service (DoS) against VoIP,» *2016 SAI Computing Conference (SAI),* pp. 1031-1036, 2016.

[37] H. Shoket y J. S. Aulakh, «Mitigation of Flooding Based Denial of Service Attack against Session Initiation Protocol Based VoIP System,» *2015 IEEE International Conference on Computational Intelligence & Communication Technology,* pp. 391-396, 2015.

[38] A. Ghafarian, S. A. H. Seno y M. Dehghani, «An empirical study of security of VoIP system,» *2016 SAI Computing Conference (SAI),* pp. 1031-1036, 2016.

[39] L. Behan, L. Sevcik y M. Voznak, «Development of a Distributed VoIP Honeypot System with Advanced Malicious Traffic Detection,» pp. 409-419, 2019.

[40] A. Helenport y B. L. Tait, «Aspects of Voice Communications Fraud,» *Springer,* pp. 69-81, 2016.

[41] M. A. Calva Martínez, «Análisis de Vulnerabilidades, Investigación Forense y Política de Seguridad para Sistemas de Telefonía IP Basados en Asterisk,» 2016.

k. Anexos

Anexo 1. Licencia