UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

“MODELO DE SEGURIDAD SOBRE LA TELEFONÍA IP/ OPEN SOURCE EN BASE A LA METODOLOGÍA PTES EN LA EMPRESA SINFOTECNIA’’

AUTORA: LUCÍA ISABEL GUERRÓN SUBÍA

DIRECTOR: MSc. EDGAR ALBERTO MAYA OLALLA

IBARRA- ECUADOR

2021

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA.

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo de Titulación a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1003440698		
APELLIDOS Y NOMBRES:	Guerrón Subía Lucía Isabel		
DIRECCIÓN:	Secundino Peñafiel 3-86 y Tobías Mena		
EMAIL:	isabelgx91@gmail.com		
TELÉFONO FIJO:	2585814	**TELÉFONO MÓVIL:**	0984823412

DATOS DE LA OBRA		
TÍTULO:	"MODELO DE SEGURIDAD SOBRE LA TELEFONÍA IP/ OPEN SOURCE EN BASE A LA METODOLOGÍA PTES EN LA EMPRESA SINFOTECNIA.''	
AUTOR:	Guerrón Subía Lucía Isabel	
FECHA:DD/MM/AA	12/10/2021	
SOLO PARA TRABAJO DE GRADO		
PROGRAMA:	■ **PREGRADO**	☐ **POSGRADO**
TÍTULO POR EL QUE OPTA:	Ingeniera en Electrónica y Redes de Comunicación.	
ASESOR/DIRECTOR:	Ing. Edgar Alberto Maya Olalla. MSc.	

Firma: .....

Nombre: Guerrón Subía Lucía Isabel

2. CONSTANCIA.

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

En la ciudad de Ibarra, a los 12 días del mes de octubre del 2021

EL AUTOR:

Lucía Isabel Guerrón Subía

CI: 1003440698

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

MAGISTER EDGAR MAYA OLALLA, DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN CERTIFICA:

Que, el presente trabajo de titulación "MODELO DE SEGURIDAD SOBRE LA TELEFONÍA IP/ OPEN SOURCE EN BASE A LA METODOLOGÍA PTES EN LA EMPRESA SINFOTECNIA'', fue realizado en su totalidad por el Srta. Lucía Isabel Guerrón Subía, portador de la cedula de identidad: 1003440698, bajo mi supervisión.

Es todo en cuanto puedo certificar en honor a la verdad.

.....

Ing. Edgar Maya Olalla, MSc

CI: 1002702197

DIRECTOR DEL PROYECTO

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DEDICATORIA

Este trabajo está dedicado a mi familia ya que sin su apoyo, paciencia, compresión y amor no podría haber alcanzado este propósito.

A mis padres **Wilson** y **Amparito** que, con su ejemplo de superación y constancia, me enseñaron a ser fuerte ante las adversidades que se presentan en la vida.

A mis **abuelitos(as)** por su cariño, su ejemplo y su orientación en especial a mi abuelita **Isabel** que me ha cuidado y ayudado siempre en todo lo que está a su alcance.

A mi hermana por ser mi amiga, mi cómplice, mi compañera y alegrarme en momentos difíciles y por demostrarme que nunca hay que dejarse vencer tan fácilmente y a una persona muy especial que me brindó su cariño y comprensión durante esta etapa.

Lucía Isabel

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

AGRADECIMIENTO

Agradezco a **Dios** y a mi **Virgencita de Guadalupe** por todas las bendiciones hasta este momento de mi vida, por ser mis guías en cada una de las dificultades que se me presentaron en el camino porque gracias a eso sembraron en mí las ganas de seguir adelante, la sabiduría, el conocimiento y sobre todo la fe para que pueda culminar esta etapa de mi carrera universitaria.

A mis **padres,** por su esfuerzo y sacrificio a lo largo de todos estos años, gracias por su comprensión, amor sincero y por inculcarme la educación, principios y valores que forman lo que soy hasta ahora, un Dios les pague realmente es poco ya que siempre su apoyo ha sido incondicional.

A la **Universidad Técnica del Norte** y a mis docentes por mi formación profesional en cada uno de los campos académicos que comprendían el perfil de la carrera de Ingeniería en Electrónica y Redes.

A la Empresa de Soluciones Integrales **Sinfotecnia** por permite realizar este proyecto en sus instalaciones, en especial al Ing. Esteban Vallejos por toda la colaboración prestada en la realización del mismo.

Lucía Isabel

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

En el presente trabajo de titulación se desarrolla un modelo de Seguridad sobre la Telefonía IP en la Empresa Sinfotecnia, considerando las vulnerabilidades registradas en la confidencialidad e integridad de la información de la red de VoIP, para de esta forma plantear las soluciones de VoIP que sean más correctas y necesarias.

El estándar seleccionado desarrolla las etapas de la metodología PTES la cual es establecida en el hacking ético para detectar el nivel de acceso externo e interno, sobre las plataformas de voz sobre IP; así como el estado de riesgo de su infraestructura usando herramientas que posteriormente contribuyan al análisis de la seguridad.

En los escenarios simulados los riesgos que predominan, en los activos de comunicación son: firewall SIP desactivado, desactualización de sistemas, falta de parches de seguridad, denegación de servicios e interpretación de la comunicación, se los definió como elevados porque todo el personal que se encuentra laborando en la empresa, realiza intercomunicaciones con el fin de agilizar sus tareas.

Los resultados de las pruebas realizadas quedarán descritos en los reportes en donde además se especificará el riesgo y la clasificación de las vulnerabilidades y se formulará las configuraciones de seguridad a nivel físico y lógico que se deseen ejecutar para de esta manera evitar amenazas en las llamadas y proteger la información en las comunicaciones.

ABSTRACT

This research is based on a Security model on Telephony IP in the Sinfotecnia Company, considering the vulnerabilities registered in the confidentiality and integrity of the VoIP network information, in order to propose the most correct and necessary VoIP solutions.

The selected standard develops the stages of the PTES methodology, which is established in ethical hacking to detect the level of external and internal access to voice over IP platforms; as well as the risk status of your infrastructure using tools that subsequently contribute to security analysis.

In the simulated scenarios, the risks that predominate in the communication assets are: deactivated firewall SIP, outdated systems, lack of security patches, denial of services and eavesdropping, which were defined as high because all the personnel working in the company carry out intercommunications in order to speed up their tasks.

The results of the tests performed will be described in the reports, which will also specify the risk and classification of the vulnerabilities and will formulate the security configurations at the physical and logical level to be implemented in order to avoid threats in the calls and protect the information in the communications.

1. CAPÍTULO I. Antecedentes

Este primer capítulo aborda la problemática, en la cual se da a conocer los motivos que originaron el desarrollo de este proyecto de investigación, a continuación se define los objetivos tanto general como específicos y el alcance y justificación que sostiene la finalidad de esta investigación.

1.1. Tema.

Modelo de Seguridad sobre la telefonía IP/Open Source en base a la metodología PTES en la empresa Sinfotecnia.

1.2. Problema

La Telefonía IP siendo un sistema basado en Internet da apertura a cierta cantidad de vulnerabilidades que pueden afectar la confidencialidad e integridad de la información en pequeñas, medianas y grandes empresas; por esta razón la empresa de Soluciones Integrales SINFOTECNIA cuya matriz se encuentra ubicada en la ciudad de Ibarra, tiene la necesidad de mejorar la seguridad de sus comunicaciones entre sus distintas oficinas y sucursales de manera que se pueda mitigar los ataques e infiltraciones(escaneo, obtención de acceso) que se registraron en el presente año, lo que podría desencadenar en incidentes de poca o gran magnitud tanto para los clientes como para la empresa en general.

Al momento la empresa para brindar conectividad y comunicación a sus dependencias tiene implementado un servidor Asterisk con sistema operativo basado en Linux, el cual tiene configurado dieciséis extensiones telefónicas distribuidas entre las oficinas de Ibarra y Ambato respectivamente, esto también involucraría la implementación de políticas de seguridad al momento de establecer comunicación por voz y datos que evite el riesgo de pérdida de información en tiempo real y que garantice

beneficios y competitividad en el mercado de las empresas de telecomunicaciones en el norte del país.

Se propone el desarrollo de un modelo de seguridad basado en la metodología PTES aplicando las fases de ejecución de una prueba de penetración con el fin de detectar las vulnerabilidades, el nivel de acceso , el grado de seguridad externo e interno y adoptar medidas preventivas que garantice una mayor protección de la información ante amenazas existentes en el servicio de telefonía IP, documentando los procesos, las herramientas y las recomendaciones que se debe seguir en cada etapa; para de esta manera optimizar los tiempos de respuesta ante eventos y delitos ejecutados por terceros malintencionados (hackers).

1.3. Objetivos

1.3.1. Objetivo General.

Establecer un modelo de seguridad en la red de telefonía IP de la Empresa Sinfotecnia, basado en la metodología PTES, utilizando las fases de un pentest para mitigar los posibles ataques que se puedan presentar en los servicios de VoIP protegiendo así la información y los recursos de esta mediana empresa.

1.3.2. Objetivos Específicos.

Analizar el estado actual de la red de telefonía IP de la empresa Sinfotecnia para conocer los dispositivos de red, servidores, protocolos utilizados y así detectar las vulnerabilidades de los mismos.

Investigar herramientas de seguridad para software libre que permitan realizar ataques y evaluar cuales son los puntos débiles en la telefonía IP a nivel de plataforma e infraestructura que comprometen la integridad, disponibilidad y confidencialidad de la información.

Ejecutar el modelo de seguridad basado en la metodología PTES y simular entornos virtuales en el servicio de VoIP para de esta manera adoptar los mecanismos más idóneos de seguridad que definan los parámetros requeridos en la empresa Sinfotecnia.

Elaborar las políticas de seguridad en base a los resultados obtenidos en las simulaciones para ayudar a la prevención de amenazas que puedan comprometer en un futuro la información de la empresa.

1.4. Alcance

Este proyecto de titulación tiene como fase preliminar la recopilación de información relacionada con la seguridad informática en sistemas de telefonía IP para analizar detalladamente los métodos de ataques existentes que los intrusos emplean en este tipo de red aplicándola tanto a nivel de capa seguridad de protocolos de VoIP, protocolos de señalización H.323 y SIP[1], protocolos de direccionamiento UDP[2], protocolos de transmisión RTP[3] así como a dispositivos terminales y gestores de llamadas.

Se procederá a realizar el levantamiento de la información de la red IP actual y a ejecutar un análisis de riesgo basado en controles CIS para determinar las deficiencias y requerimientos que garanticen la integridad, confidencialidad y disponibilidad de la información.

El modelo de seguridad se basará en la metodología de hacking ético PTES, la cual permitirá determinar el estado y el impacto de los ataques a los que es vulnerable la central de VoIP Asterisk entre las cuales se analizará 7 fases:

---

[1] SIP: Protocolo de inicio de sesiones (Session Inition Protocol).
[2] UDP: Protocolo de datagrama de usuario. (User Datagram Protocol).
[3] RTP: Protocolo de transporte de tiempo real. (Real-Time Protocol Transport Protocol).

La primera etapa consistirá en la **interacción preacuerdo** con los directivos de la Empresa Sinfotecnia en la que se establecerá el enfoque, los objetivos, el alcance, los aspectos a explorarse antes de que comiencen las pruebas de penetración.

La segunda etapa se basa en la **recopilación inteligente de información** sobre el sistema, identificación interna y externa de servicios, mapeo, análisis de perfiles tanto de empleados como corporativos, información de negocios, presencia en medios sociales, entre otros.

La tercera etapa de **modelación de amenazas** se fundamentará en los datos obtenidos anteriormente para el análisis de las amenazas de los procesos y las tecnologías clave utilizadas por los atacantes y de esta manera identificar el método más eficaz de ataque en la telefonía IP.

La cuarta etapa de **análisis de vulnerabilidad** se enfocará a identificar vulnerabilidades, parches faltantes, testeo, servicios abiertos, contraseñas por defecto, errores de configuración, fugas de información, entre otros.

En la quinta etapa de **explotación** se tratará de la revisión real de los fallos del sistema de telefonía IP y especialmente se centra en el establecimiento de acceso al sistema al definir las herramientas y las restricciones de seguridad para este.

La sexta etapa de **post explotación** es para la recopilación de evidencias, la protección y valoración del sistema comprometido con el fin de mantener un control permanentemente y en la última etapa de **reportes** se detallará los resultados de las pruebas realizadas además se especificará el riesgo y la clasificación de las vulnerabilidades. (Pérez, 2012).

Se planteará escenarios de simulación para determinar soluciones en la capa de seguridad de protocolos de VoIP. En este apartado es necesario realizar un estudio de las herramientas en entornos libres detallando los parámetros más eficientes que posea

cada uno de estos softwares de manera que permitan efectuar ataques a la red de VoIP de la empresa Sinfotecnia.

El desarrollo de mecanismos de seguridad debe estar basada en estándares internacionales, por tal motivo se propone generar las políticas de seguridad apoyadas en el estándar ISO/ICE 27002, capitulo 5 para protección de la información en una red integrada de voz y datos.

1.5. Justificación

A través de la investigación del problema planteado toda empresa privada o pública está expuesta a distintos tipos de inseguridades que pueden poner en riesgo intereses económicos, tecnológicos, sociales y legales cuando se maneja información compartida en conversaciones telefónicas confidenciales, como es el caso del servicio de telefonía IP. Por tal razón este proyecto pretende descubrir y detectar los principales ataques que asechan este servicio en la Empresa Sinfotecnia de tal manera que se garantice la seguridad de la información y privacidad de los datos según lo estipulado en los artículos 76 y 78 de la Ley Orgánica de Telecomunicaciones 2015 y el COIP del Ecuador, artículos 230, 232, 234 referentes a los delitos informáticos y ataque a la integridad de sistemas informáticos.

Además la finalidad de la propuesta de este modelo de seguridad de telefonía IP es implementar y adoptar las herramientas de software libre cumpliendo así con el decreto ejecutivo No.1014 cuyos instrumentos contribuyen a diagnosticar las vulnerabilidades que posee actualmente la red IP, por esta razón la metodología escogida debido a que ofrece una guía técnica para realizar pruebas de penetración es la PEST de Hacking Ético la misma que fue propuesta por una organización de profesionales en seguridad de la información que lleva el mismo nombre que la

metodología, buscando de esta forma determinar el nivel de acceso y el grado de seguridad externo e interno de la plataforma Asterisk.

Con las medidas de seguridad adoptadas se pretende que la empresa mejore sus comunicaciones institucionales creando conciencia en sus usuarios de lo importante que es el manejo de la información, evitando la proliferación y el fácil acceso en redes basadas en Internet.

2. CAPÍTULO II. Fundamentación Teórica

Este capítulo trata de la introducción a la telefonía IP, seguridad informática, describiendo los principales riesgos y tipos de ataques que se puedan presentar tanto en la arquitectura, protocolos de voz y señalización como en los dispositivos terminales de la red de VoIP.

2.1. Introducción a VoIP a través de Asterisk

La evolución tecnológica ha permitido que las redes telefónicas empleen infraestructuras digitales; este es el caso de la tecnología **VoIP** que se basa en el concepto de la digitalización de las comunicaciones por voz utilizando el protocolo IP sin requerimiento de los circuitos conmutados PSTN[4] de la telefonía tradicional. En un principio el protocolo IP fue diseñado para redes de transmisión de datos, pero debido a su gran desarrollo fue adoptado a las redes de voz mediante el encapsulamiento de la información y la transmisión de la misma como paquetes de datos IP.

En este contexto cabe diferenciar de la **Telefonía IP** que es un servicio telefónico que depende y utiliza la VoIP para establecer comunicaciones pero que se refiere a la infraestructura adecuada para instalar un entorno de comunicaciones IP, en el que se pueda ofrecer funcionalidades más avanzadas como PBX-IP[5], etc.

De esta manera varias empresas han visto en la tecnología VoIP un ahorro sustancial en sus costos ya que para realizar las llamadas emplean soluciones Open Source como es la plataforma Asterisk que no tiene restricción de licencias a diferencia de un sistema de comunicación propietario.

---

[4] PSTN: Red Telefónica Pública Conmutada (Public Switched Telephone Network).
[5] PBX-IP: Central Telefónica Virtual (Private Branch Exchange)

2.2. Tecnología VoIP

La voz sobre IP (Voice over Internet Protocol) es el conjunto de recursos, protocolos de comunicación, metodologías y técnicas de transmisión que hace posible transportar la señal de voz en forma digital a través de Internet, cuya señal debe ser procesada y encapsulada en paquetes para que pueda ser enviada sobre una red de datos (Rico, 2013).

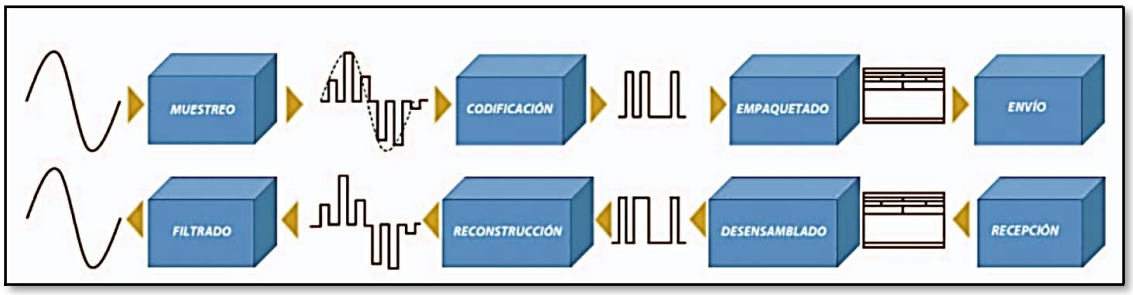
De tal manera la voz sobre IP no constituye un servicio sino una tecnología basada:

- Múltiples protocolos tanto para el nivel de control (señalización) como para el nivel de usuario.
- Múltiples topologías de red.
- Múltiples dispositivos como códecs, terminales, entre otros.

Para brindar VoIP, esta tecnología primeramente debe convertir una señal analógica en digital, para ello realiza un proceso llamado muestreo de la señal, después procede a realizar la conversión analógico digital (A/D) utilizando codificadores códecs para de esta manera obtener una señal digital como se muestra en la Figura 1:

Figura 1.

Digitalización de la voz en VoIP



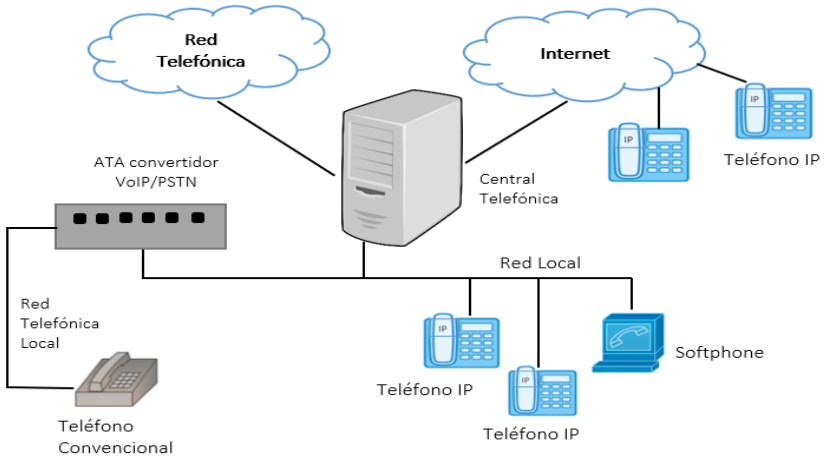
Nota. Obtenido de (Management Solutions, 2006)

2.3. Estructura básica de VoIP.

En la tecnología de VoIP influyen tres elementos principales como indica la central telefónica de la Figura 2.

Figura 2.

Esquema de los componentes de una red de VoIP



Nota. Adaptado de (Emilse, 2014)

- **Terminales:** Son los dispositivos que usarán los usuarios para iniciar y recibir llamadas; estos pueden ser teléfonos IP (hardware) o softphones[6] (software)que realizan las funciones de teléfonos convencionales.
- **Gateways**: También conocido como dispositivo ATA (Adaptador Telefónico Analógico) y son los encargados de brindar un puente de comunicación entre los usuarios, es decir proveen interfaces para conectar redes de VoIP con las redes convencionales PSTN. Es transparente para el usuario.

[6] Softphones: Herramienta de VoIP basada en software que permite a un computador o teléfono inteligente realizar o recibir llamadas VoIP.

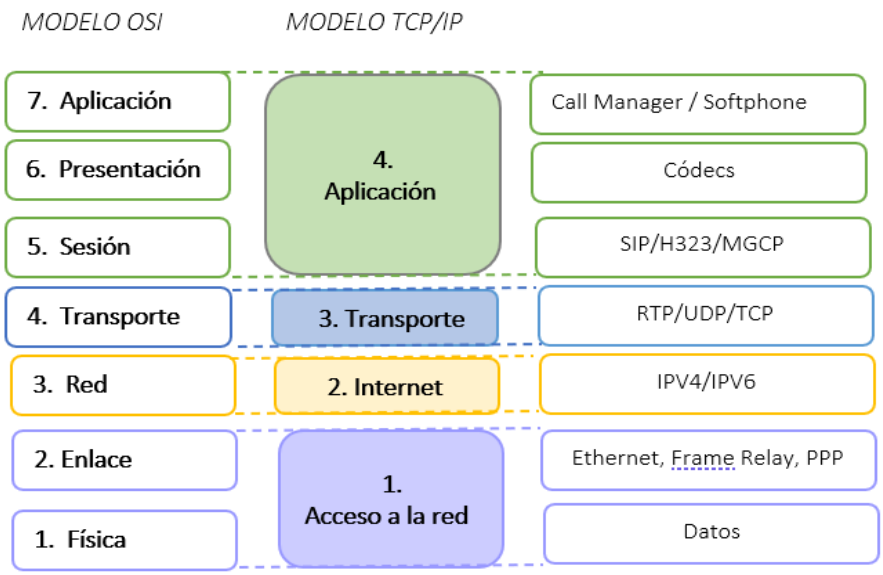
- **Servidor**: Es el encargado de proporcionar funcionalidades de una central telefónica PBX (Rico, 2013). Es decir, es el responsable de autenticación, admisión, enrutamiento, control e interacción entre los usuarios de una red. Este servidor puede adoptar distintos nombres según el tipo de protocolo de señalización que esté utilizando; para el protocolo SIP opta por el nombre de servidor SIP, si trabaja sobre el protocolo H.323 tiene el nombre de Gatekeeper[7].

2.4. Protocolos y estándares VoIP

El objetivo de VoIP es dividir en paquetes los flujos de audio para transportarlos sobre redes basadas en IP es por esto se toma de referencia a los modelos de protocolos de Internet tanto OSI, así como TCP/IP distinguiendo en cada una de sus capas los distintos protocolos usados en las comunicaciones de VoIP, ver Figura 3.

Figura 3.

Protocolos usados en VoIP según modelo OSI, TCP/IP



Nota. Adaptado de *(Management Solutions, 2006)*

[7] Gatekeeper: Software de telefonía IP multiplataforma.

Según Suárez & Quispe (2011) afirman que “estos protocolos de VoIP poseen un mecanismo de conexión que incluye una serie de transacciones de señalización entre terminales, que establecen flujos de audio para cada dirección de la conversación”.

2.4.1. Protocolos de transporte

Son las normas que definen la comunicación que se forma entre los extremos de un canal de comunicaciones previamente establecido. Este transporte no solo incluye el trasladar los paquetes de un extremo al otro, sino que tendrá que fragmentar y reensamblar los paquetes además de proporcionar los mecanismos adecuados para reducir el retardo, jitter, etc. Los protocolos de transporte más empleados son RTP y RTCP.

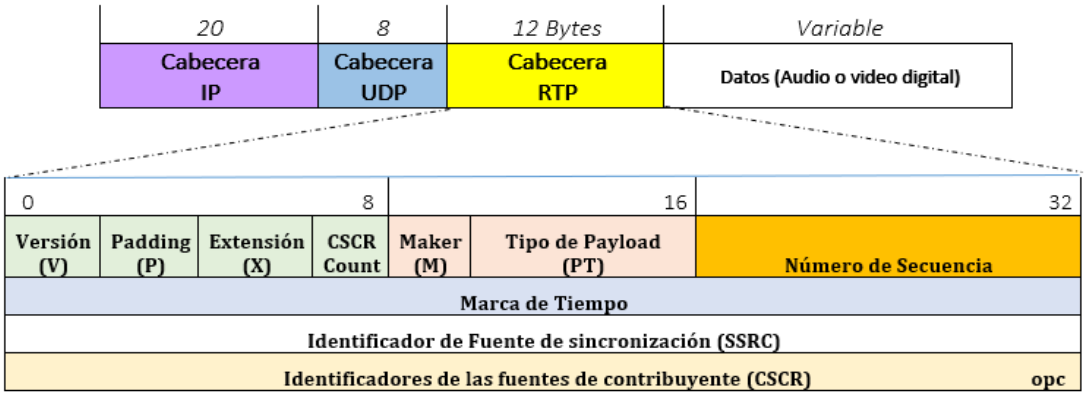
2.4.1.1. Protocolo de Transporte en Tiempo Real (RTP)

El protocolo RTP (Real Time Transport Protocol) define el estándar para la transmisión de tráfico (audio y video) sensible a los retardos a través de redes IP. Ofrece servicios como: la identificación del tipo de carga, numeración de secuencia, sincronización de medios, marcas de orden, marcas temporales etc.

RTP trabaja bajo el protocolo de comunicación UDP (puertos 10000-20000) y hace su mayor esfuerzo para la entrega de paquetes al destino, sin embargo, no garantiza su entrega. En la Figura 4 se puede ver como los paquetes RTP están divididos en dos bloques; por un lado, se encuentra la cabecera que contiene la información necesaria para reconstruir el flujo de bits generado por el códec del emisor y por el otro, la carga útil. (José & Roldán, 2006)

Figura 4.

Encabezado del paquete RTP



Nota. Adaptado de *(López, 2009)*

2.4.1.2. Protocolo de Control en Tiempo Real (RTCP)

El protocolo RTCP (Real Time Control Protocol) es complementario a RTP y se encarga de monitorizar el flujo de paquetes RTP ya que obtiene estadísticas sobre el jitter, latencia[8], perdida de paquetes etc. Con RTCP, los usuarios de VoIP pueden intercambiar información sobre la calidad de la señal transmitida, es decir RTCP permite control de congestión, monitoreo y registro de rendimiento en la llamada entre usuarios.

En una sesión RTCP los usuarios retrasmiten periódicamente paquetes de control al resto de participante, consiguiendo que cada paquete RTCP tenga informes sobre el emisor y receptor; además RTCP administra el CNAME[9] el cual es el único identificador para un participante a lo largo de una sesión.

Tipos de paquetes.

Los tipos de paquetes que tiene el protocolo RTCP se identifican en la tabla 1.

[8] Latencia: Es el tiempo que tarda en transmitirse un paquete dentro de la red.

[9] CNAME: Nombre canónico del punto final de la comunicación.

Tabla 1.

Paquetes RTCP

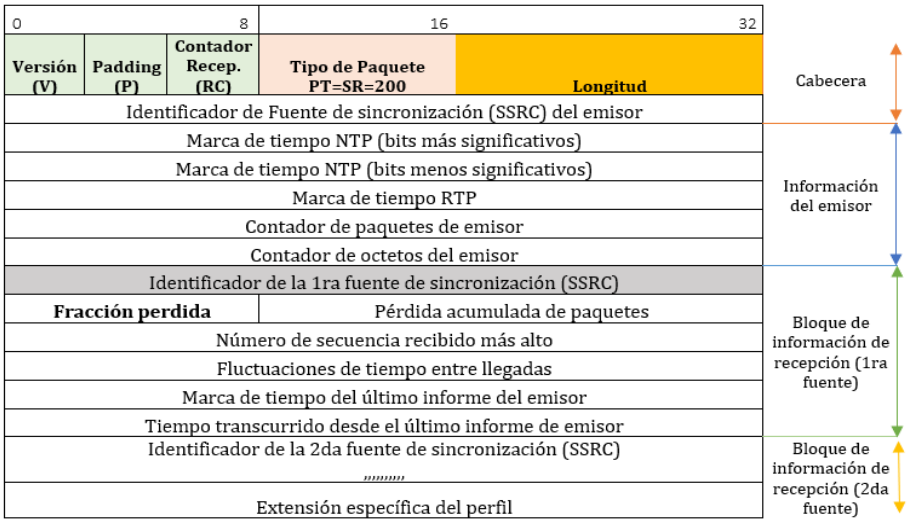
#	Tipo	Paquete	Descripción
200	SR	Informe de emisor	Conjunto de estadísticas de transmisión y recepción de emisores.
201	RR	Informe de receptor	Conjunto de estadísticas que provienen de receptores.
202	SDES	Descripción de Fuente	Identifica a la fuente incluyendo su (CNAME).
203	BYE	Mensaje de Fin	Termina la sesión de una fuente en una comunicación.
---	APP	Aplicación	Paquetes específicos de una aplicación

Nota. Adaptado de (Muñoz, 2008)

Los informes de emisor y receptor se envían periódicamente cada intervalo de tiempo y se estructuran en bloques asi cada cual aporta información estadística sobre los datos recibidos de una fuente específica. La diferencia entre los dos informes es que los del emisor incluyen sección adicional que emplean los participantes (ver Figura 5,6).

Figura 5.

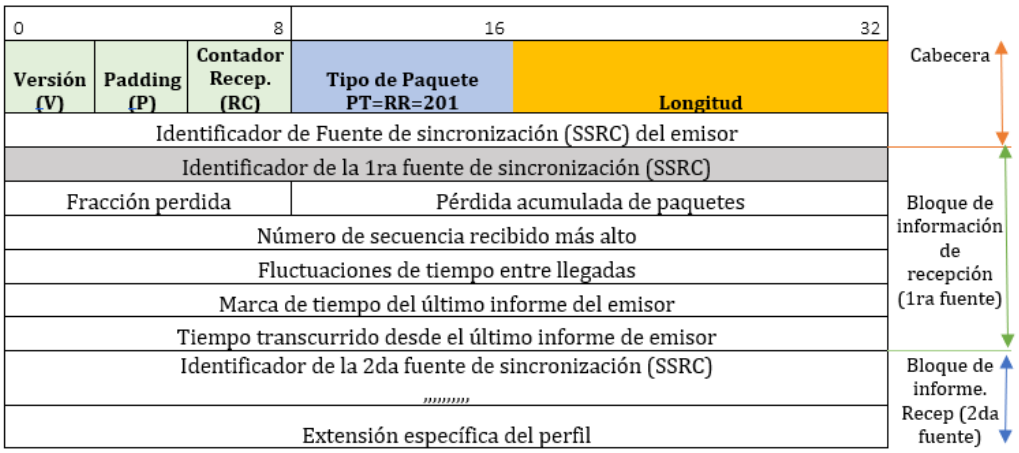
Informe de emisor en una sesión RTCP



Nota. Modificado de (España, 2003)

Figura 6.

Informe de receptor en una sesión RTCP



Nota. Modificado de (España, 2003).

2.4.2. Protocolo de señalización.

El objetivo de estos protocolos de capa aplicación es establecer una canal de comunicación a través del cual fluya la información del usuario y liberar el canal cuando finalice la comunicación (José & Roldán, 2006). Es necesario que exista un dialogo entre los componentes de la red y los terminales de los usuarios respectivamente.

2.4.2.1. Protocolo de Inicio de Sesión (SIP)

El protocolo SIP (Session Initiation Protocol) fue creado por el IETF y es el encargado de establecer, modificar o terminar una sesión multimedia entre dos o más extremos definiendo sockets, tipos de archivo y formatos.

SIP trabaja en el puerto 5060 para UDP y TCP y debido a su sencillez y escalabilidad para integrarse con otros protocolos utiliza RTP/RTCP y SDP para la realizar las sesiones de comunicación; es decir al protocolo RTP lo usa para transportar

los datos de voz en tiempo real, mientras que el protocolo SDP (Protocolo de descripción de sesión) se usa para la negociación de los participantes, tipo de codificación, etc.

- **Arquitectura del protocolo SIP**

La arquitectura de SIP está compuesta por dos elementos principales: Agentes de Usuario (UA) y servidores:

A. **Agentes de usuario (UA):** manejan la señalización y pueden ser de 2 tipos:
   - *Agentes de usuario clientes (UAC):* que son los elementos que inician las peticiones de llamada.
   - *Agentes de usuario servidor (UAS):* que son los elementos encargados de recibir las peticiones UAC.

B. **Servidores:** que pueden ser de 4 tipos:
   1. *Servidor Proxy SIP:* realiza las funciones de intermediario entre los agentes de usuarios y servidores puesto que cuando le llega una petición de inicio de llamada de un cliente decide a que servidor debería ser enviada y entonces retransmite la petición hasta llegar a su destino.
   2. *Servidor de Redirección:* es un servidor que genera respuestas de redirección a las peticiones que recibe, además reencamina las peticiones hacia el próximo servidor (Gutiérrez, 2015).
   3. *Servidor de Registro:* es un servidor que acepta peticiones de registro de los usuarios y guarda la información de estas peticiones para proporcionar una traducción de direcciones (Gutiérrez, 2015).
   4. *Servidor de Localización:* Facilita información al Proxy sobre la ubicación del destinatario de una llamada (Gutiérrez, 2015).

- **Mensajes SIP**

El dialogo entre clientes y los servidores SIP se basa en el intercambio de mensajes de texto. La estructura genérica de un mensaje SIP ya sea de petición o respuesta es la siguiente: línea de comienzo, cabeceras (una o más), línea vacía que indica final de las cabeceras y el cuerpo del mensaje que es opcional (José & Roldán, 2006). A continuación, en las Tabla 2 se observa los tipos de peticiones SIP.

Tabla 2.

Peticiones SIP

Petición SIP	Descripción
INVITE	Mensaje inicial de invitación envidado por el extremo llamante.
ACK	Confirma el establecimiento de una sesión.
BYE	Indica la finalización de una sesión por parte de uno de sus participantes.
CANCEL	Cancela una petición pendiente.
REGISTER	Registra al User Agent.
OPTIONS	Solicita información sobre capacidades de un servidor.
INFO	Contiene información fuera de banda.

Nota. Adaptado de Tecnología VoIP y Telefonía IP (José & Roldán, 2006)

En las Tabla 3 se aprecia los tipos de respuestas SIP, luego de recibir una petición.

Tabla 3.

Respuestas SIP

Respuesta SIP	Descripción
1xx	Mensajes provisionales.
2xx	Respuesta de éxito.
3xx	Mensajes de desvió.
4xx	Error de petición.
5xx	Error de servidor.
6xx	Error general.

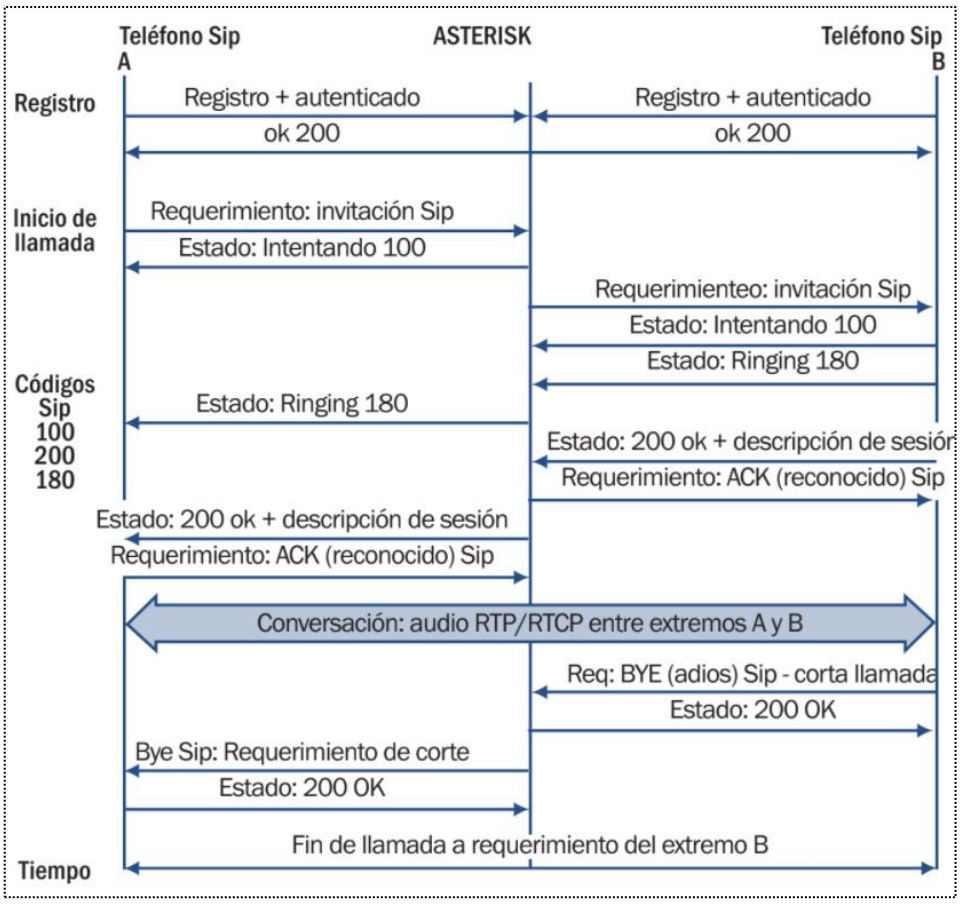
Nota. Adaptado de Tecnología VoIP y Telefonía IP (José & Roldán, 2006)

- **Sesiones SIP**

Antes de iniciarse el proceso de comunicación como se observa en la Figura 7 los dos usuarios A y B, deben registrarse en el servidor de registro; cuando el usuario A quiere contactar con el usuario B se realiza una petición INVITE hacia el Proxy Server que será el encargado de enrutar el mensaje. Este Proxy Server reenvía la petición al destinatario B, previamente consultando en el Servidor de localización la dirección del usuario B y así cuando B descuelga se retransmite un mensaje 200 OK al emisor de la llamada, y cuando ya se hayan enviado los mensajes ACK la llamada queda establecida.

Figura 7.

Establecimiento de llamada entre dos terminales.



Nota. Obtenido de *(Arias & Arias, 2013)*

Entonces según (José & Roldán, 2006) los pasos para el establecimiento de sesiones SIP serían los siguientes:

- Registro, instalación y localización del usuario.
- Descripción de la sesión multimedia que se pretende establecer.
- Aceptación de la petición de conexión del otro extremo.
- Establecimiento de la llamada.
- Comunicación
- Finalización de la llamada.

2.4.2.2. Protocolo H.323.

El protocolo H.323 es una recomendación ITU que define los componentes y los medios de interacción para la trasmisión de voz, videos y datos multimedia a través de redes basadas en conmutación de paquetes en las que no se ofrecen un grado de calidad de servicio. H.323 presta control de llamada, gestión de información y ancho de banda para una comunicación punto a punto y multipunto, así como define interfaces entre una red interna y una red externa. (Gómez & Gil, 2008)

La principal ventaja de la señalización H.323 es su rapidez en comparación con SIP, debido a que el formato de los mensajes H.323 es binario facilitando la tarea de interoperabilidad.

Arquitectura de H.323 Las redes basadas en H.323 consta de los siguientes elementos:

A. *Terminales multimedia de usuario:* equipos utilizados por los usuarios finales que proveen interacción en tiempo real bidireccional como teléfonos IP, softphones (Gómez & Gil, 2008).

B. *Pasarelas (gateways):* hardware que posee las interfaces necesarias para interconectar distintos tipos de tecnologías. (PSTN, ISDN, etc.)

C. *Porteros (gatekeeper):* es el punto central de una red H.323 que proporciona servicios a los terminales de usuario registrados como control de llamadas, gestión de ancho de banda y traducción de direcciones (Gómez & Gil, 2008).

D. *Unidad de control multipunto (MCU):* provee la capacidad para que varios terminales y gateways puedan participar en una conferencia multipunto.

Pila de protocolos asociados a H.323.

- **H.225 Señalización RAS:** es el protocolo encargado de proveer las resoluciones de direcciones y los servicios de admisión a la red VoIP.
- **H.225 Señalización de control de llamada:** es el encargado del proceso de conexión de las llamadas entre los agentes H.323 (terminales de usuario).
- **H.245 Medio de control y transporte:** maneja los mensajes de control de extremo a extremo entre entidades H.323. Los procedimientos H.245 establecen canales lógicos para la transmisión de audio, video y datos y controlan la información del canal (CISCO, 2014).

Proceso de llamadas.

En la figura 8 se observa las 3 fases que se llevan a cabo en el flujo de llamadas H.323.

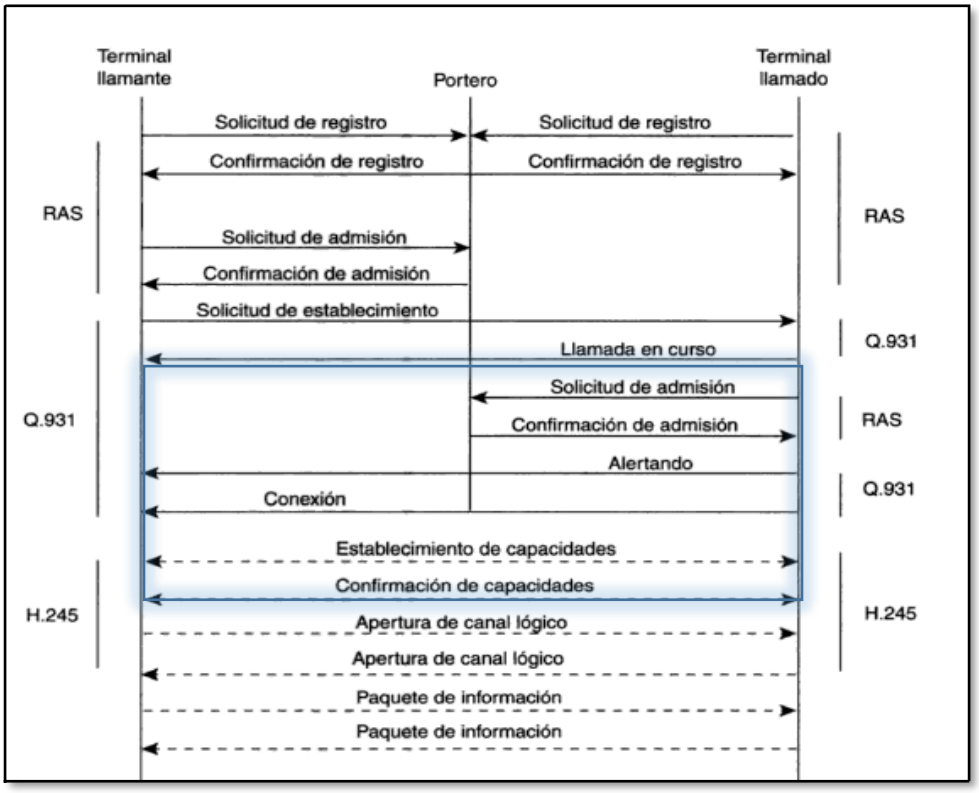
Fase RAS: establece un canal para las comunicaciones entre los terminales y su Gatekeeper.

Fase Q.931: sirve para establecer la primera conexión entre dos terminales.

Fase H.245: Intercambio de capacidades, mensajes de control de flujo, apertura y cierre de canales lógicos.

Figura 8.

Proceso de llamada (Conexión)



Nota. Obtenido de (España, 2003)

2.4.2.3. Protocolo IAX

El protocolo Inter-Asterisk Exchange Protocol (IAX) también puede ser referido como IAX2 si se contempla la segunda versión del mismo, es utilizado para manejar conexiones VoIP entre servidores Asterisk y clientes que también utilizan este protocolo. IAX2 cuenta con un puerto UDP único (4569) para las comunicaciones entre los terminales finales y este puerto es compartido tanto por la señalización como por los datos.

El principal objetivo de IAX es minimizar el ancho de banda requerido en la transmisión de voz y video a través de la red IP, la señalización y los datos son multiplexados en el mismo puerto UDP entre los sistemas y además los mensajes son binarios.

Tipos de Tramas.

- **Frames M o mini tramas:** son tramas que contienen la menor información en la cabecera para reducir el uso en el ancho de banda, por lo que no tienen que ser respondidas.
- **Frames F o full trama:** son tramas completas que incluyen información de sincronización, que a diferencia de las anteriores deben ser respondidas explícitamente (3CX, 2010).

Funcionamiento de IAX.

La llamada IAX o IAX2 tiene las siguientes fases como indica en la Figura 9.

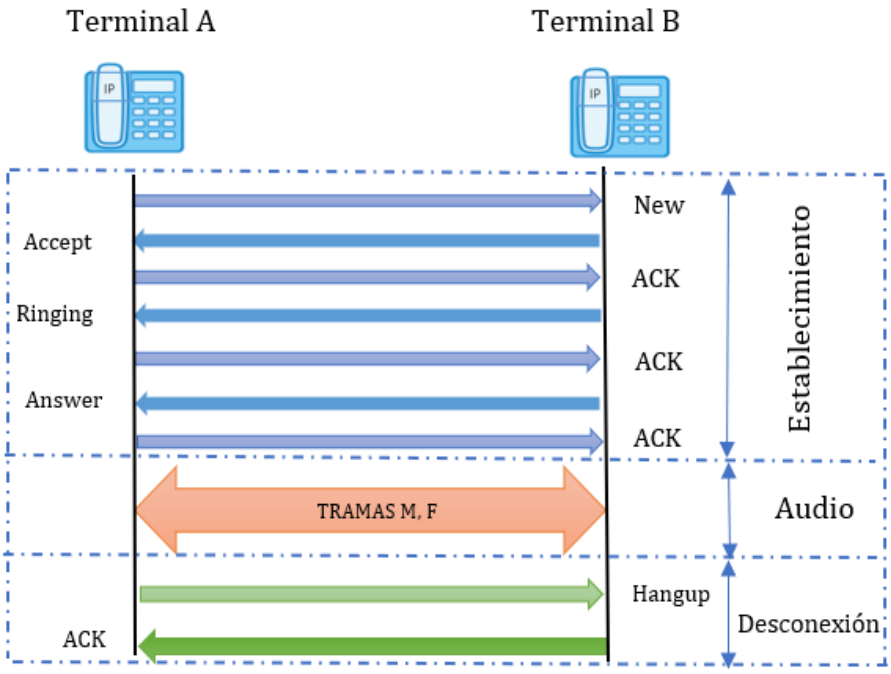
Fase 1. Establecimiento de la llamada: El terminal llamante inicia una conexión y manda un mensaje NEW mientras el terminal llamado responde con un ACCEPT y el llamante le responde con un ACK; enseguida el terminal llamado da las señales de "ringing" y la llamante contesta con un ACK para confirmar la recepción del mensaje. De esta manera el llamado acepta la llamada con un ANSWER y el llamante confirma ese mensaje (3CX, 2010).

Fase 2. *Flujo de datos o flujo de audio:* Se mandan los frames M y F en ambos sentidos con la información de voz.

Fase3. *Liberación de la llamada o desconexión*: un mensaje de HANGUP y se confirmar dicho mensaje (3CX, 2010).

Figura 9.

Establecimiento de una llamada IAX



Nota. Adaptado de (3CX, 2010)

2.5. Códecs.

Los códecs son los encargados de realizar la digitalización, codificación y compresión del audio antes de su transmisión y luego su decodificación, descompresión en la recepción, para que de esta manera se pueda establecer una comunicación y se tenga como resultado una señal audible y clara entre los usuarios que realizan y reciben llamadas telefónicas sobre IP (Suárez & Quispe, 2011).

En la tabla 4 según el códec empleado en la transmisión, se utilizará más o menos ancho de banda y entre los principales los más usados en telefonía se tiene:

Tabla 4.

Tipos de Códecs en Telefonía IP.

Códec	Ancho de banda (kHz)	Características	Aplicación
G. 711 *Estándar de la UIT-T*	64	Basado en muestras y no utiliza un algoritmo de compresión.	Telefonía
G.723.1 *Estándar de la UIT-T*	6,3 / 5,3	Bajo requerimiento de ancho de banda.	Telefonía
G.726 *Estándar de la UIT-T*	16/24/32/40	Utiliza un algoritmo que reduce el ancho de banda.	Telefonía
G.728 *Estándar de la UIT-T*	16	Se basa en una decodificación de procesamiento en la pérdida de paquetes.	Telefonía por satélite. Videoconferencia.
G.729 *Estándar de la UIT-T*	11,8 / 8 / 6,4	Bajo requerimiento de consumo de ancho de banda y una óptima calidad de audio. Se necesita licencia para su uso.	Aplicaciones de VoIP.
GSM *Estándar de ETSI*	13	Utiliza la información de muestras anteriores para predecir la muestra actual.	Telefonía móvil
iLBC *Libre*	15,2 / 13,33	Mantiene una buena relación de ancho de banda y calidad de voz.	Comunicaciones de voz robustas sobre IP.

Nota. Adaptado de (Suárez & Quispe, 2011)

2.6. Centrales IP

En el mercado existen numerosas alternativas para implementar telefonía IP, entre tecnologías propietarias o sistemas abiertos, sin embargo, las dos son vulnerables a la inseguridad presentada en redes de VoIP. En este caso se analizará la plataforma Asterisk.

2.6.1. Asterisk

Es un framework de código abierto, para la construcción de aplicaciones de comunicaciones, convierte un hardware en una plataforma de comunicaciones. Asterisk potencia sistemas IP PBX, puertas de enlace VoIP, servidores de conferencias y otras soluciones personalizadas.

Asterisk permite la construcción de aplicaciones multiprotocolo de comunicación en tiempo real. Escrito en C bajo la plataforma Linux conecta diferentes protocolos de telefonía soportando VoIP (principalmente a través de SIP).

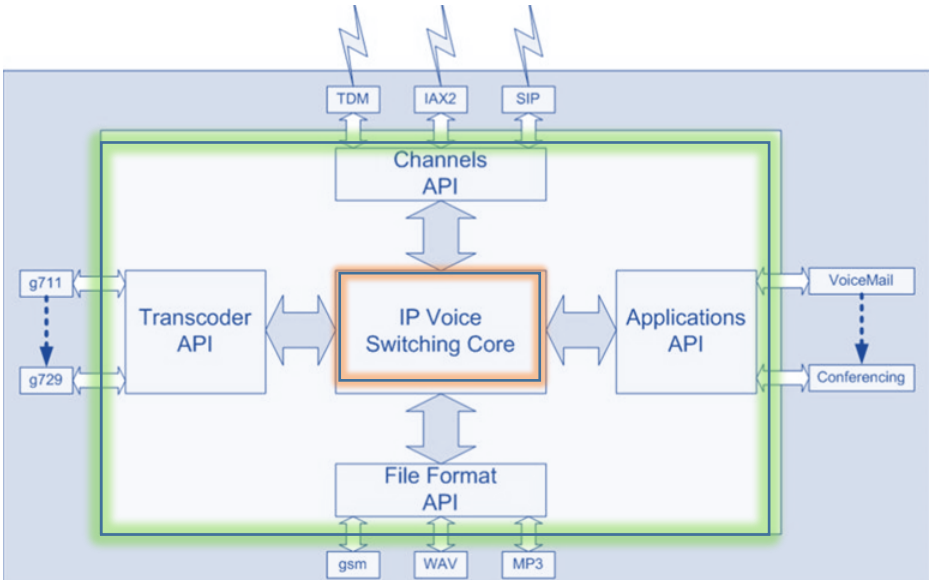
2.6.1.1. Arquitectura Asterisk

La arquitectura de Asterisk está formada principalmente por 4 APIs como se visualiza en la Figura 10 donde un API es el conjunto de funciones y procedimientos que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción (Barbéran, Javier, 2011).

1. API de canales: maneja y extrae la información como protocolos, interfaces y códecs según el tipo de conexión.
2. API de aplicaciones: Permite a varios módulos de tareas cumplir varias funciones, multiconferencias, lista de directorios, buzones de voz, aplicaciones personalizadas, etc. (Barbéran, Javier, 2011).
3. API de traducción de códecs: Carga módulos usados para la compresión codificación de la señal tales como G.711, G.729, GSM, etc.
4. API de formato de ficheros: Maneja la lectura y escritura de varios formatos de archivos para el almacenaje de datos en el sistema de archivos (Barbéran, Javier, 2011).

Figura 10.

Arquitectura Asterisk.



Nota. Obtenido de (Atelis PLC, 2015)

2.6.2. Free PBX

FreePBX es una interfaz gráfica de usuario (GUI) que controla y gestiona Asterisk, creada bajo la licencia GPL. Poseer una interfaz fácil de usar y funcional para el software de sistema de telefonía.

2.6.3. Ventajas y desventajas de la VoIP

Las principales ventajas de la VoIP son las siguientes:

- Facilidad: permite desarrollar una red homogénea en la que se combina información como voz, video o datos, por una sola línea ofreciendo mayores beneficios y gestión de servicios.
- Ahorro: Con este servicio se economiza gastos tanto de infraestructura como de mantenimiento, ya que el costo más relevante sería solo el pago de servicio de internet o ISP.

- Conferencia: Se puede transmitir más de una llamada entre varias personas en tiempo real sobre una línea telefónica, debido a que los paquetes son comprimidos durante la transmisión.
- Hardware y software más barato: Reduce la cantidad de dispositivos que se necesita para voz y datos.

Las principales desventajas de la VoIP son las siguientes:

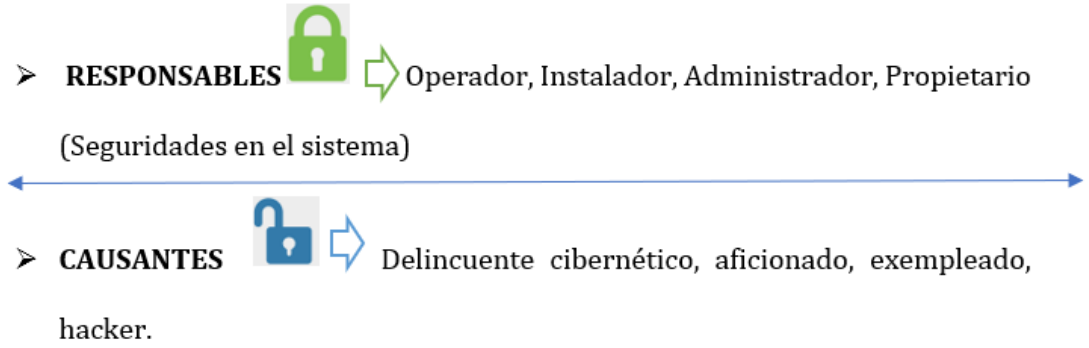
- Calidad de audio: este parámetro depende del ancho de banda, hardware y servicios, la calidad y confiabilidad de las conexiones VoIP si no es así; los posibles problemas que resultarían en las llamadas están las demoras, ruido y eco (Yunk, 2019).
- Dependencia del ancho de banda: VoIP depende de la conexión a Internet, si el ancho de banda es insuficiente posiblemente causará problemas de calidad con el servicio.
- Seguridad: Las posibles amenazas que pueden presentar las redes de VoIP incluyen robo de identidad y servicios, phishing, virus y malware, spam por telefonía por Internet y ataques de denegación de servicio (Yunk, 2019).

2.7. Seguridad en Redes de VoIP.

La seguridad de un sistema es un conjunto de capas que no solo depende de ciertos dispositivos de la red, de ciertas políticas y procedimientos, ni de la infraestructura de la empresa, es un conjunto que involucra no solo la arquitectura del sistema, sino también el recurso humano, y la buena utilización del sistema (Gutiérrez, 2015). Los involucrados se enumera en la Figura 11:

Figura 11.

Esquema de los responsables y causantes en la seguridad de la red



Nota. Autoría propia

2.7.1. Vulnerabilidades en VoIP

Existen vulnerabilidades de diferentes tipos: físicas, naturales, de hardware, software, medios de almacenamiento, comunicación y humanas que se pueden presentar por intrusión, por configuración o pueden ser propias del sistema.

Tabla 5.

Tipos de Ataques en los distintos niveles

VULNERABILIDADES Y ATAQUES		
• **Nivel Físico**	• **Nivel de protocolos**	• **Nivel de aplicación**
Acceso físico a la red, servidores y dispositivos.	*Escuchas Ilegales o interceptación.*	*Servicios Web de teléfonos IP.*
Reinicio de Máquinas.	*Secuestro de sesiones.*	*SPAM VoIP.*
	Denegación de servicio.	*VoIP phishing (Vishing)*
	Manipulación de señales y transmisiones multimedia.	*Fraude Telefónico.*
	Inundaciones SYN.	

• **En base al Sistema Operativo.**	• En base de Políticas	• Nivel de Servicios
Malas configuraciones.	*Contraseñas predeterminadas y débiles.*	*Negación en DHCP.*
Gusanos y virus	*Accesos a los datos sin restricciones.*	*Ataques DoS.*
Desbordamiento en Buffers.	*Malas políticas de privilegios.*	*Inyecciones SQL.*

Nota. Adaptado de (Gutiérrez, 2015)

2.7.2. Ataque-Definición

Según el NIST (National Institute of Standars and Technology), se define ataque como: "Intento de pasar los controles de seguridad en un equipo. El ataque puede alterar, dar a conocer o denegar información. Será efectivo dependiendo de la vulnerabilidad del sistema y de la efectividad de los planes de contramedidas. Un ataque activo es resultado de la alteración de información y uno pasivo en dar a conocer alguna información. El grado de éxito de un ataque depende de la vulnerabilidad del sistema y la efectividad de las contramedidas existentes".

I. Fases de un ataque

- Reconocimiento: Se recolecta información del sistema de forma activa o pasiva.
- Escaneo: probar activamente las vulnerabilidades que puede explotarse.
- Obtener acceso: explotar una vulnerabilidad para acceder al sistema.
- Mantener el acceso: se mantiene en el sistema para lograr el objetivo del ataque.

- Cubrir las huellas: el atacante trata de borrar las evidencias del ataque. (Gómez J. , 2015)

2.8. Hacking Ético

Rama de la seguridad informática que permite evaluar el nivel de vulnerabilidad y el riesgo en el que se encuentran los sistemas informáticos o los activos de una organización de forma legal y autorizada (Gutiérrez, 2015).

I. Conceptos básicos

- **Cracker**: Un cracker es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que, a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño a su objetivo. (Pignanelli, 2012)
- **Hacker ético**: profesionales de la seguridad que aplican sus conocimientos de hacking con fines defensivos y legales.

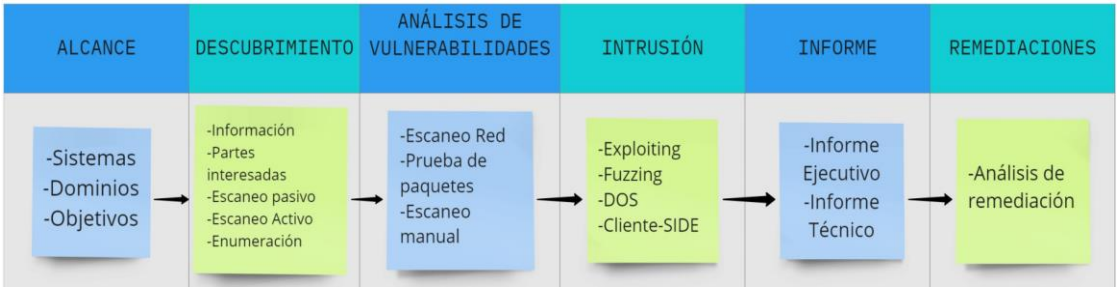
II. Etapas del Hacking Ético

En la Figura 12 se especifica que el hacking ético consta de las siguientes etapas.

- Contrato con el cliente de las pruebas a realizar incluido un acuerdo de no revelar información.
- Crear un equipo de hacking y planificar las pruebas.
- Realizar los test.
- Analizar los resultados y realizar un informe.
- Entrega del informe al cliente.

Figura 12.

Pasos que se siguen en el hacking



Nota. Adaptado de (Pedraza, 2014)

2.9. Metodología PTES

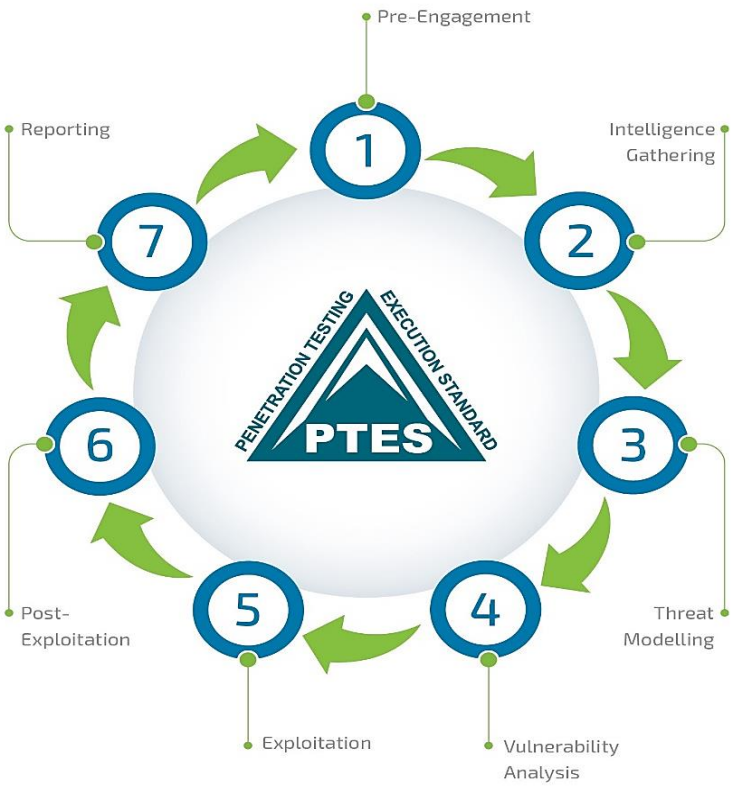
PTES (PENETRATION TESTING EXECUTION STANDARD) es un estándar que cubre todo lo relacionado con una prueba de penetración mediante una serie de pautas técnicas, relacionadas con los diferentes entornos que puede encontrar un evaluador, así como una serie de directrices, herramientas y sugerencias aplicables en pequeñas y grandes empresas (Pentest Standard, 2012) . PTES divide la ejecución de un test de intrusión en 7 fases como se muestra en la Figura 13.

1. *Interacciones previas al compromiso*: Se refiere al acuerdo durante el cual se definirán los términos, condiciones y la profundidad a evaluar, las fechas de la evaluación, así como las herramientas que podrían medir la efectividad e impacto de un posible ataque.
2. *Reunión de Inteligencia*: Es aquella en la que el auditor se dedicará a obtener y recopilar toda la información posible sobre el objetivo desde fuentes abiertas.
3. *Modelado de amenazas*: Se analiza el equipo técnico, las instalaciones tanto redes, hardware y software, es decir agentes de amenazas internas y externas que tenga la organización.

4. *Análisis de Vulnerabilidad*: Con los datos recogidos en la fase anterior se buscan las posibles vías y métodos de ataque más efectivos.
5. *Explotación*: En esta etapa se pone en ejecución las herramientas para así atacar a las vulnerabilidades detectadas y obtener acceso a los sistemas.
6. *Post Explotación*: Se puede seguir escalando el proceso de explotación con la información de las vulnerabilidades encontradas en los sistemas examinados.
7. *Informes*: Con las pruebas recogidas y los test realizados, se procede a analizar los resultados para dar una solución al estado de la seguridad de la organización.

Figura 13.

Metodología PTES



Nota. Obtenido de (Infopulse, 2019)

2.9.1. Selección y comparativa de las metodologías para pruebas de penetración.

Actualmente existen diversas guías o metodologías para llevar a cabo un pentesting sin embargo es importante analizar los parámetros que cada una de ellas ofrece por esta razón en la Tabla 6 se realiza la comparación entre 4 metodologías para de esta manera elegir la metodología más efectiva desde la perspectiva de la seguridad de tecnologías de VoIP, que es el principal enfoque de esta investigación.

Entre las metodologías más utilizadas por auditores de red se encuentran las siguientes:

- ISSAF: Marco de Evaluación de Seguridad de Sistemas de Información.
- OSSTMM: Manual de Metodología Abierta de Evaluación de Seguridad.
- PTES: Estándar de Ejecución de Pruebas de Penetración
- NIST SP: Guía Técnica para Evaluaciones y Pruebas de Seguridad de la Información.

Tabla 6.

Comparación entre metodologías de pruebas de penetración

CONCEPTOS	ISSAF	OSSTMM	PTES	NIST SP 800-53
Facilidad de Ejecución	Se requiere conocimientos medios	Se requiere conocimientos avanzados debido a uso de su terminología y procedimientos	Se requiere conocimientos medios.	Se requiere conocimientos previos.
Metodología/ Complejidad	Descripción de test de intrusión básico.	Es una metodología muy minuciosa y es la más conocida.	Existe un análisis en todas sus etapas.	Descripción de procesos demasiado general.

Etapas	*Consta de 3 fases:* 1. Planificación y preparación. 2. Evaluación. 3. Reportes y Limpieza.	*Consta de 4 fases:* 1. Inducción. 2. Interacción. 3. Requerimientos 4. Intervención. Y además consta de 6 secciones adicionales de seguridad.	*Consta de 7 fases:* 1. Preacuerdo 2. Recopilación de inteligencia. 3. Modelado de amenazas 4. Análisis vulnerabilidades. 5. Explotación 6. Post explotación 7. Reporte.	*Consta de 4 fases:* 1. Planificación. 2. Descubrimiento 3. Ejecución 4. Documentación y Reporte
Entornos de aplicación.	Organizaciones pequeñas.	Organizaciones grandes de todo tipo	Organizaciones pequeñas y grandes	Organizaciones medianas.
Herramientas	No define un uso específico de herramientas.	Define el uso de herramientas open Source pero no las especifica.	Define el uso de herramientas open Source en cada etapa.	No especifica las herramientas a utilizarse.
Tecnología VoIP	No menciona contenidos de redes sobre VoIP.	Hay una sección orientada a PBX	Posee un apartado dirigido a redes de VoIP.	Menciona la tecnología, pero no la describe.

Nota. Elaboración propia

En base a las características analizadas anteriormente las metodologías más enfocadas a mitigar las brechas de inseguridad en tecnologías de voz sobre IP son las guías metodológicas OSSTMM y PTES, sin embargo, se seleccionó el estándar PTES porque tiene instrucciones muy detalladas de cómo ir ejecutando las herramientas de penetración en cada etapa; además se puede adaptarlo dependiendo de las pruebas que se vayan a efectuar en cada escenario que se proponga.

3. CAPÍTULO III. Análisis de la situación actual de la Empresa Sinfotecnia.

En este capítulo se recolecta la información de la red actual de la Empresa Sinfotecnia, considerando las vulnerabilidades registradas en la confidencialidad e integridad de la información de la red de VoIP, para de esta forma plantear las soluciones de VoIP más correctas e idóneas.

3.1. Generalidades

SINFOTECNIA, es una empresa de Soluciones Integrales en el ámbito de las Telecomunicaciones, que surgió como una pequeña empresa en el año 2004 y que a través de estos años se ha ido consolidando como una empresa reconocida tanto en la provincia de Imbabura como en el norte del país y entre los principales productos y servicios que ofrece a empresas públicas y/o privadas se encuentran los siguientes: cableado estructurado, equipos de networking, desarrollo e implementación de redes informática, redes eléctricas, redes de comunicación, redes de seguridad, mantenimiento y asesoría técnica. En la Figura 14 se muestra su imagen corporativa.

Figura 14.

Logo de la Empresa

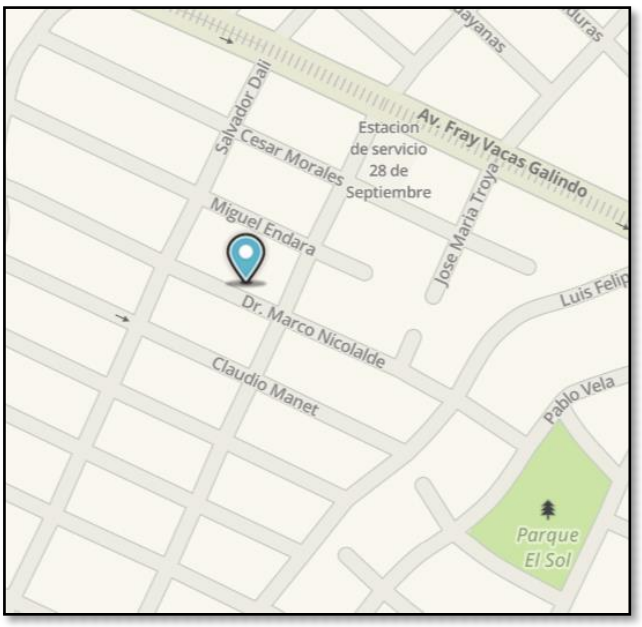
Nota. Obtenido de Empresa Sinfotecnia.

3.2. Situación actual de la Empresa Sinfotecnia.

En la actualidad SINFOTECNIA tiene su oficina matriz en la cuidad de Ibarra, entre las calles Dr. Marco Nicolalde 4-22 y Aurelio Gómez Jurado, como se muestra en la Figura 15; así como una sucursal ubicada en la ciudad Ambato entre la Av. Los Shyris 2239 y Luis Cordero, visualizada en la Figura 16.

Figura 15.

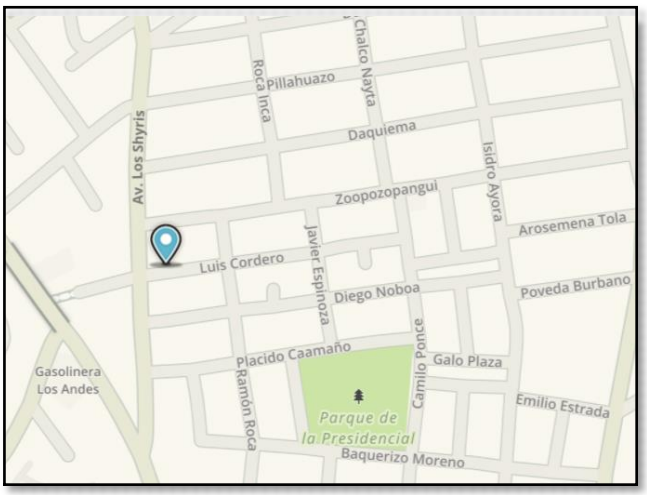
Ubicación de la oficina matriz de la Empresa Sinfotecnia



Nota. Captura obtenida de aplicación WAZE.

Figura 16.

Ubicación de la sucursal Ambato.



Nota. Captura obtenida de aplicación WAZE.

3.2.1. Misión de Sinfotecnia.

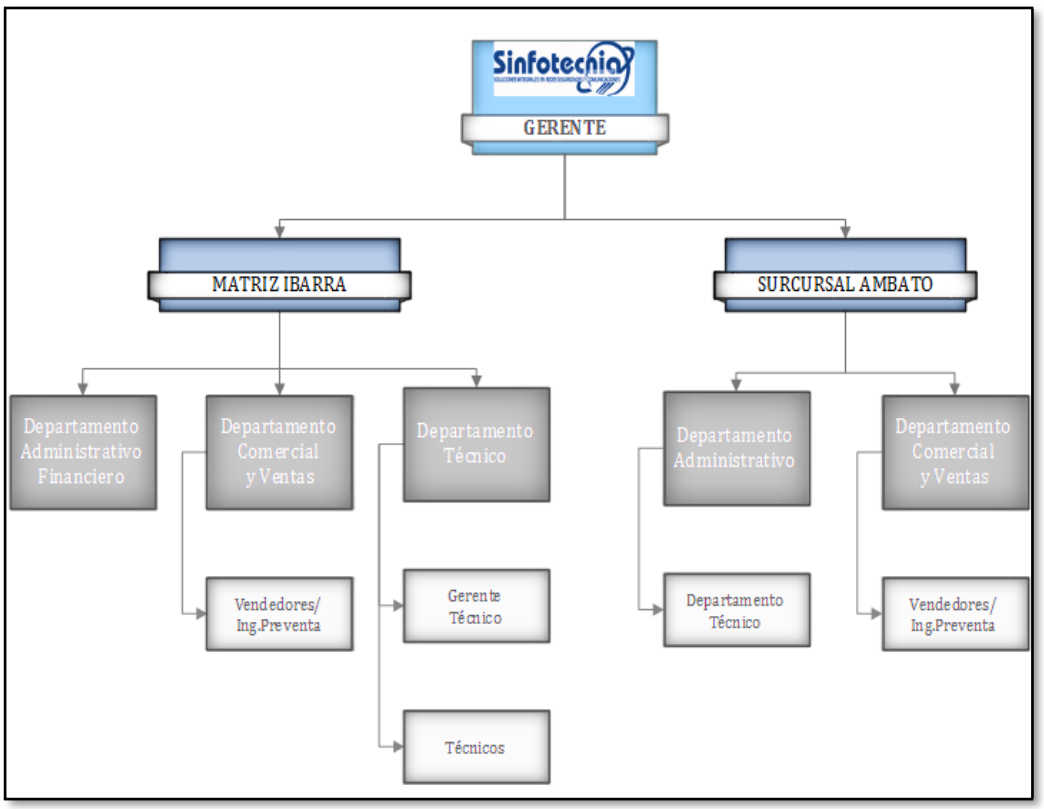
Sinfotecnia es una empresa que ofrece productos y servicios de calidad, con un personal altamente calificado y capacitado brindando día a día las mejore soluciones integrales en redes, seguridades y comunicaciones con los debidos certificados y garantías para satisfacer a las instituciones públicas y privadas que forman parte de nuestro distinguido grupo de clientes en el norte del país.

3.2.2. Organigrama estructural de Sinfotecnia.

La empresa cuenta con una nómina de 11 trabajadores distribuidos en el área administrativa y técnica, como se muestra en la Figura 17 teniendo las siguientes dependencias según el organigrama.

Figura 17.

Esquema estructural de la Empresa



Nota. Adaptado de la Empresa Sinfotecnia.

3.3.Análisis de la infraestructura tecnológica de Sinfotecnia.

En esta sección se describe la estructura interna de la empresa, los departamentos, el cableado estructurado, el cuarto de equipos, así como el área de trabajo definidos con su respetivo direccionamiento.

3.3.1. Estructura Física de la Empresa.

Sinfotecnia funciona en un edificio de 2 plantas, la Figura 18 muestra la distribución de las instalaciones físicas en cada planta.

Figura 18.

Distribución física de instalaciones

Nota. Adaptado de la Empresa Sinfotecnia.

3.3.2. Estructura de la red de datos de Sinfotecnia.

Sinfotecnia tiene implementada en su matriz una red de datos de topología *tipo estrella*, teniendo como nodo central un Router Cisco 800 el cual maneja un direccionamiento IP clase C 192.168.X.X con una máscara de subred /24 para la red LAN interna, y para enlaces externos emplea las siguientes direcciones:

- IP pública ➔ 201.183.X.X
- Máscara➔ /24
- Gateway➔201.183.X.X
- DNS➔200.124.X.X, 200.124.X.X

3.3.3. Cableado horizontal.

La empresa posee un rack de telecomunicaciones ubicado en la planta baja en el que se tiene instalado cableado estructurado *categoría 6e* para comunicar las distintas dependencias que tiene la empresa a través de los equipos de conmutación. Igualmente, cada oficina cuenta con puntos de voz y de datos teniendo un total de 40 puntos respectivamente certificados.

- Planta Alta ➔ 5 puntos de red.
- 2do Piso ➔ 16 puntos de red.
- 1er Piso ➔ 19 puntos de red.

3.3.4. Cableado vertical.

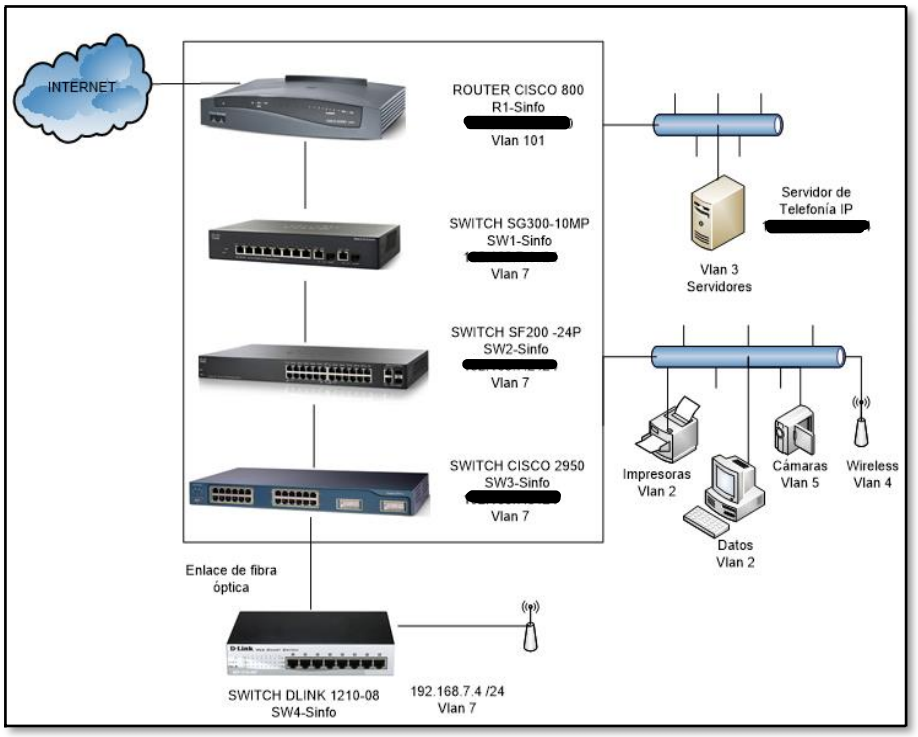
El tendido del cable 6e entre los distintos pisos se encuentra realizado a través de canaletas sobre las paredes del edificio cumpliendo la norma de cableado estructurado TIA/ANSI 586 B, todos los cables de cobre están centralizados en el patch panel del gabinete principal de 48u.

3.3.5. Esquema de red.

El esquema de red con el que cuenta la empresa en la cuidad de Ibarra y en la sucursal de Ambato se muestra en la figura 19 y 20 respectivamente.

Figura 19.

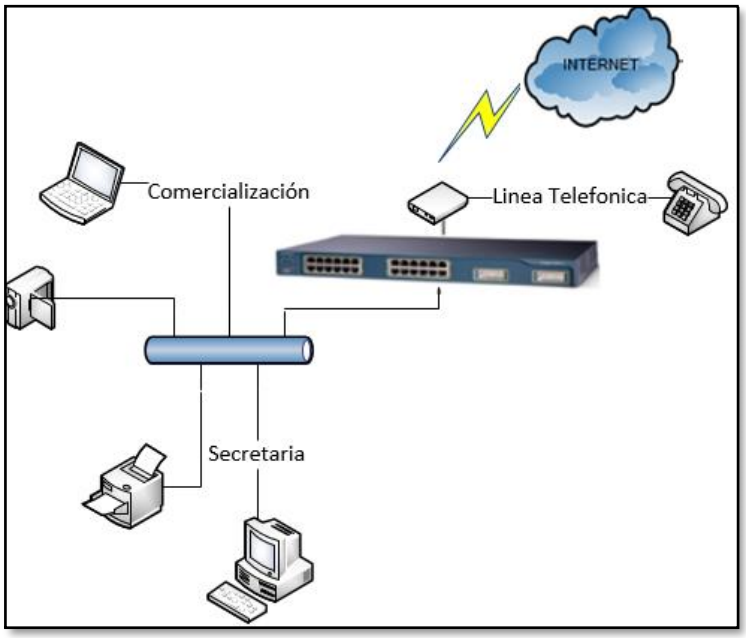
Topología de red de la Empresa oficinas Ibarra



Nota. Obtenido de Empresa Sinfotecnia

Figura 20.

Topología de red de la Empresa oficina Ambato



Nota. Obtenido de Empresa Sinfotecnia.

3.3.6. Direccionamiento y segmentación de la red.

La red se encuentra segmentada en VLANs, lo cual ayuda a disminuir la transmisión de tráfico en la red ya que agrupa a los usuarios con requerimientos similares de red en una misma VLAN, teniendo la tabla 7 con el direccionamiento asignado.

Tabla 7.

Direccionamiento de las VLANs

VLAN	ID VLAN	Subredes	Máscara
Red de datos	2	192.168.X.X	/24
Telefonía ip	3	192.168.X.X	/24
Wireless	4	192.168.X.X	/24
Cámara de vigilancia	5	192.168.X.X	/24
Red de pruebas	6	192.168.X.X	/24
Nativa y administración de equipos	7	192.168.X.X	/24
Enlace Internet	101	192.168.X.X	/30

Nota. Obtenido de Empresa Sinfotecnia

Entre las VLANs más importantes están:

- Red de Datos (VLAN 2): Esta red virtual permitirá la conexión de los computadores hacia el servidor que asignará DHCP a los equipos de los clientes.
- Red de VoIP (VLAN 3): Esta red virtual permitirá la conexión de los teléfonos IP hacia el servidor de VoIP.
- Red de Servidores (VLAN 4): Esta red pertenece exclusivamente a equipos de características de servidor.

3.3.7. Rack de comunicaciones.

El rack de comunicaciones se encuentra en la planta baja del edificio cuyas dimensiones son 2135 mm x 530mm x 390 mm de profundidad; es un rack abierto de piso de 42 UR en él que se ubican 3 switchs, 1 Router CISCO, 1 Wireless Controller, 2 Access Point, el Servidor DHCP y de Telefonía.

- Posee un Firewall FortiGate 60D sin configurar.
- No cuenta con un generador eléctrico de respaldo.
- Tiene un sistema de puesta a tierra.

Las características técnicas de los dispositivos de enuncian en la Tabla 8:

Tabla 8.
Equipamiento del rack de comunicaciones

Cantidad	Dispositivos
1	Router cisco 800
1	Switch Cisco SG300-10MP
1	Switch Cisco SF200-24P
1	Switch Cisco 2950
1	Switch DLink 1210-08
1	Servidor de telefonía IP
1	Servidor DHCP
1	Cisco Wireless LAN Controller 2504
1	Access Point AIR-LAP1041N-A-K9
1	Access Point APWA321

Nota. Obtenido de Empresa Sinfotecnia

3.3.8. Servidores de Red.

Servidor DHCP

El servidor de DHCP encargado de asignar direcciones de forma dinámica usa como sistema operativo CentOS de 64 bits.

Servidor FreeNAS

En este servidor se encuentra almacenado la memoria técnica para las inspecciones, el sistema contable y también es usado para la compartición de archivos, carpetas.

Servidor de Antivirus

Encargado de instalar y actualizar en antivirus ESET NOD32 versión 6 los equipos terminales y usa como sistema operativo Windows Server 2012 de 64 bits.

3.3.9. Equipos de conectividad.

Esta pequeña empresa cuenta con un Router Cisco 881 en la capa de red para la conexión en la red local y la red externa, una controladora de red inalámbrica Cisco para controlar los Access Point WAP 321, destinados a la conexión de dispositivos móviles en la LAN, y los switches de capa enlace encargados de segmentar la red para reducir la carga en cada distribución, la Tabla 9 muestra las características de cada uno de los switches instalados.

- ***Switch Cisco Catalyst***

Tabla 9.

Características de los Switch disponibles

Switch Cisco *Modelo: SG300-10MP*	**Switch Cisco** *Modelo: SF200-24P*	**Switch Cisco Catalyst** *Modelo: 2950*
		
Especificaciones: • Switch administrable de capa 3 • Velocidad Gigabit Ethernet • Puertos: * 8 puertos PoE 10/100/1000 • * 2 puertos para • fibra SFP.	Especificaciones: • Switch de capa 2 • Velocidad Fast Ethernet • Puertos: * 24 puertos 10/100 • 2 puertos para fibra SFP.	Especificaciones: • Switch de capa 2 • Velocidad Fast Ethernet • Puertos: * 24 puertos PoE 10/100/1000 • 2 puertos para fibra SFP. • Soporte VLAN

• Soporte VLAN • Dispone DHCP, ACL • Soporte de telefonía IP integrada.	• Funcionalidad PoE está disponible en 12 de los 24 puertos. • Soporte VLAN. • Inteligencia de QoS para dar prioridad al tráfico sensible.	• Standars MDI/MDIX, IEEE 802.1p (Prioridad de etiquetas), IEEE 802.1q (VLAN), IEEE 802.1d (Spanning Tree), IEEE 802.1s (Multiple Spanning Tree)
• Configura automáticamente teléfonos IP conectados con la VLAN correcta y QoS parámetros de calidad de servicio para priorizar el tráfico de voz. • Compatibilidad de Ipv6 y la Ipv4 tradicional.	• Seguridad de puertos IEEE 802.1X para controlar el acceso a su red. • Compatibilidad de Ipv6 y la v4 tradicional.	

Nota. Adaptado de Datasheet de Cisco

- ***Router Cisco 881***

Este modelo de Router posee o puertos 10/100 Fast Ethernet switch, así como 2 puertos (PoE) para la alimentación de los teléfonos IP o puntos de acceso externos; además proporcionan una función de seguridad avanzada, incluyendo la prevención de intrusiones, GET VPN, dinámico multipunto VPN. Los protocolos de enrutamiento que maneja son RIPv1, v2, BGP, OSPF[10], EIGRP.[11]

- ***Cisco Wireless LAN Controller 2504***

Este controlador inalámbrico tiene 4 puertos y soporta la conexión de 5 puntos de acceso. Proporciona las políticas de seguridad centralizadas, sistema inalámbrico de prevención de intrusiones (WIPS) capacidades, el galardonado de gestión de RF, y la calidad de servicio (QoS) para voz y vídeo (Cisco, s.f.).

[10] OSPF (Primer Camino Más Corto): Protocolo de encaminamiento de tipo enlace y estado.
[11] EIGRP (Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado): protocolo de enrutamiento del tipo vector distancia avanzado

3.3.10. Equipos Terminales

Entre los equipos terminales que se encuentra instalados están cámaras IP, Teléfonos IP, impresoras, computadoras de escritorio y laptops teniendo en la Tabla 10 el siguiente inventario de dispositivos.

Tabla 10.

Equipos terminales

Cantidad	Dispositivo
12	Computadoras de escritorio/Laptop
4	Impresoras
2	Cámaras IP
9	Teléfonos IP

Nota. Obtenido de Empresa Sinfotecnia

- **Teléfonos IP.**

La empresa Sinfotecnia maneja tres tipos de modelos de teléfonos IP en la Tabla 11 se detalla las características de cada uno de ellos.

Tabla 11.

Modelos de Teléfonos IP Cisco

Cisco IP Phone *Modelo: CPA 303*	**Cisco IP Phone** *Modelo:* CPA 502G	**Cisco IP Phone** *Modelo: C*PA 525G
		

Características: • Teléfono IP de 3 líneas. • Posee dos puertos Ethernet conmutados. • Soporta protocolos SIP versión 2 y SPCP. • Maneja estos códecs G.711, G.726, G.729 AB, G.722.	Características: • Teléfono IP de 1 líneas. • Posee dos puertos Ethernet conmutados. • Soporta protocolos SIP versión 2 y SPCP. • Permite la opción para configurar etiquetado VLAN • Admite estos códecs G.711ª, G.711u, G.726_32, G.729ab y G.722 • No admite Bluetooth • Acepta mecanismos de seguridad como: HTTPS, SRTP, SIP sobre TLS, AES.	Características: • Teléfono IP de 3 líneas. • Posee dos puertos Ethernet conmutados. • Soporta protocolos SIP versión 2 y SPCP. • Admite estos códecs G.711ª, G.711u, G.726_32, G.729ab y G.722 • No admite Bluetooth • Acepta mecanismos de seguridad como: HTTPS, SRTP, SIP sobre TLS, AES.

Nota. Adaptado de Datasheet de Cisco

3.3.11. Servicio de Telefonía

En la actualidad Sinfotecnia cuenta con el servicio telefónico a través de líneas convencionales las que son proporcionadas por la empresa CNT (Corporación Nacional de Telecomunicaciones).

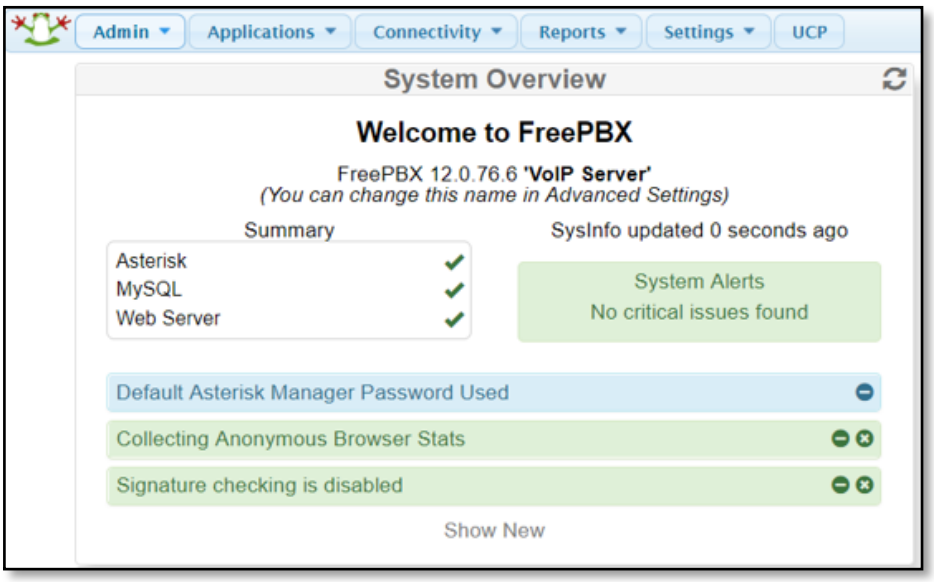
La oficina matriz tiene la línea telefónica convencional con el # 062957127 para recibir y hacer llamadas locales, regionales y celulares; en cambio la sucursal tiene la línea telefónica con el # 032850037.

- ***Telefonía IP.***

La empresa Sinfotecnia tiene implementado sobre la plataforma Asterisk, la consola de administración FreePBX en la versión 12.0.76.6, en un sistema Operativo CentOS 6.8 y como se puede apreciar en la Figura 21 se muestra la interfaz con las funcionalidades específicas del sistema de VoIP, además se visualiza que solo tiene la instalación básica sin ningún tipo de complemento adicionales.

Figura 21.

Consola de administración de Free PBX



Nota. Obtenido de Empresa Sinfotecnia

En la Tabla 12 se describen las características del servidor en el cual está alojado la central de VoIP.

Tabla 12.

Elementos de la central de telefonía IP

Servidor de Telefonía IP Proliant HP de la serie ML110 con 3 GB de memoria DDR3 y una capacidad almacenamiento de 1 TB**.**	
Tarjeta de telefonía para conectar con la troncal Es de la marca Digium AXE410 con 4 puertos FXS/FXO y Digitales para usar con Asterisk.	

Nota. Adaptado de Empresa Sinfotecnia

3.3.11.1. Distribución de las extensiones.

En la matriz principal de la empresa se maneja la siguiente distribución de extensiones, como la cantidad de oficinas es poca solo se maneja una estructura de 3 dígitos, especificados en la Tabla 13.

Tabla 13.

Extensiones distribuidas en las diferentes áreas

Extensión	Descripción
101	Recepción
103	Ventas
104	Soporte Técnico 1
105	Soporte Técnico 2
106	Administración
107	Ingeniería en Redes
108	Gerencia
109	Capacitación
110	Casa

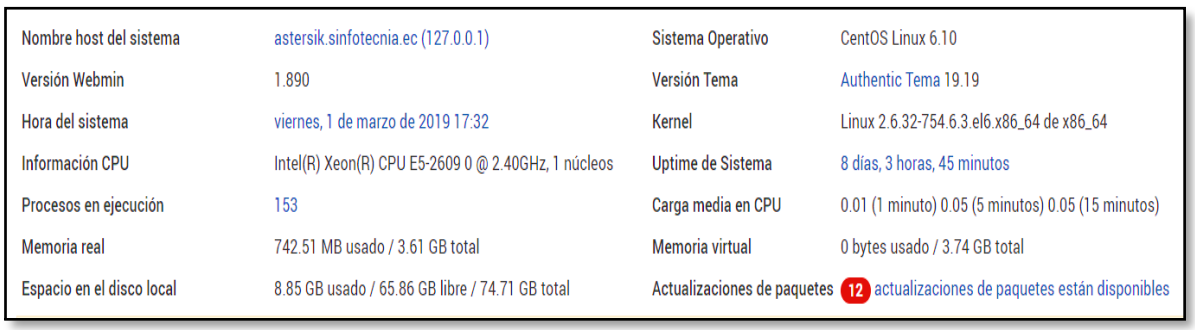
Nota. Adaptado de Empresa Sinfotecnia

3.3.11.2. Webmin

Webmin es la interfaz web utilizada para la administrar el sistema de Telefonía IP, entre otros servicios principales como la base de datos, DHCP, SSH lo que facilita la edición de archivos manualmente. En la Figura 22 se muestras detalles del servidor.

Figura 22.

Webmin para visualización del estado del servidor de VoIP



Nota. Obtenido de Empresa Sinfotecnia

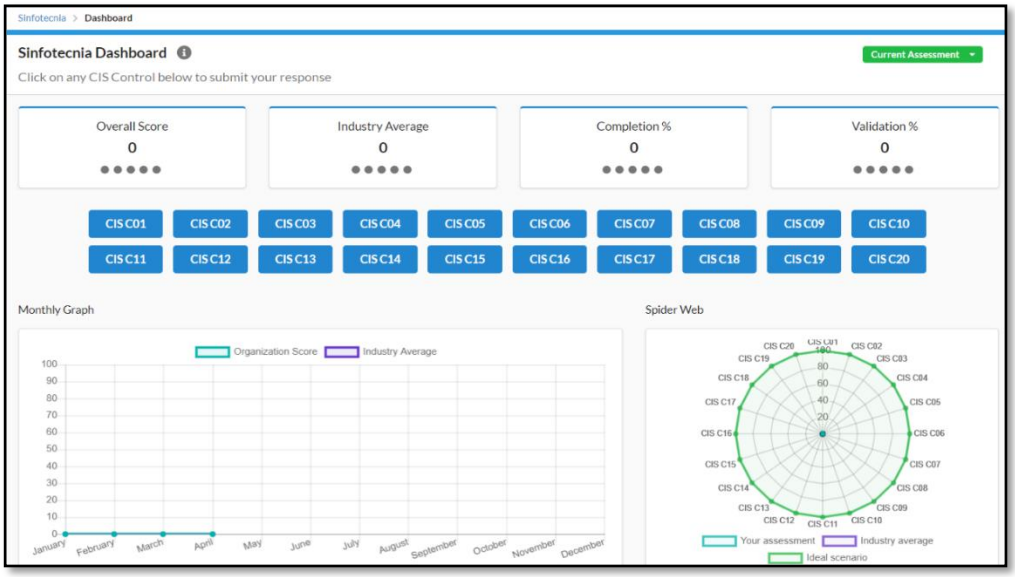
3.4.Análisis de Riesgos.

El análisis de riesgos tiene como propósito determinar las amenazas de la empresa u institución examinando los controles actuales que tiene implementados para de esta manera valorar el grado de riesgo al que está expuesto desde una perspectiva tecnológica. La herramienta de autoevaluación que se utilizó para llevar a cabo este primer análisis mediante preguntas al administrador de red en la empresa Sinfotecnia se llama CIS SAT, la cual se basa en los controles del marco de seguridad cibernética (CSF) de la metodología NIST SP 800-53.

La herramienta de controles CIS es una aplicación web gratuita, basada en 20 controles principales los cuales están divididos en tres categorías: básicos, fundacionales y organizacionales, además esta plataforma muestra gráficos de los resultados obtenidos en cada uno de los sub-controles como se muestra en la Figura 23, para de esta manera establecer las salvaguardas que se debe aplicar para prevenir y mitigar el daño de las amenazas encontradas.

Figura 23.

Panel principal de la herramienta CIS SAT

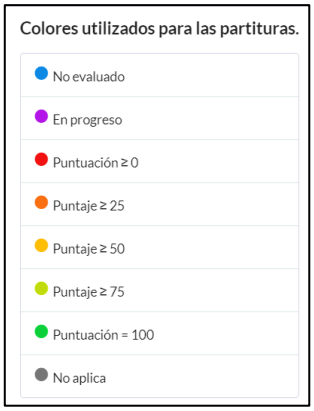


Nota. Obtenido de (Centro de Seguridad de Internet, 2020).

La herramienta evalúa los controles y con una puntuación de (0-100) identificando cada partitura con los colores que se muestran en la Figura 24.

Figura 24.

Colores que identifican el nivel de riesgo



Nota. Obtenido de (Centro de Seguridad de Internet, 2020)

3.4.1. Aplicación de los controles CIS.

Cada control de la herramienta CIS SAT se basa en varios apartados de las cuales se debe seleccionar únicamente los que adapten a las características y a las necesidades de la empresa en cuestión, teniendo así una política aplicable en cada caso:

3.4.1.1.Controles Básicos

Estos son controles de seguridad de uso general que cada organización debe implementar para garantizar la disponibilidad de una defensa informática básica (ManageEngine, 2020), en la Figura 25 se muestra el nivel de riesgo de los 6 primeros controles.

Figura 25.

Valoración de los controles CIS básicos

Nota. Obtenido de (Centro de Seguridad de Internet, 2020)

Control 1: Inventario de Dispositivos autorizados y no autorizados.

Este control se basa en el inventario de los activos que tiene la empresa, y si el administrador de la red maneja alguna herramienta para el descubrimiento de equipos no autorizados, a continuación en la Tabla 14 se muestra que el resultado del *Control 1* tiene un riesgo alto puesto a que solo se ha realizado escaneos de manera eventual y no hay un registro actualizado de todos los activos de hardware conectados a la red.

Tabla 14.

Parámetros evaluados en el Control 1

Preguntas de Control CIS C01	Tipo de Activo	Seguridad
-Utiliza una herramienta de descubrimiento activo	Equipos	
-Utiliza una herramienta de descubrimiento pasivo	Equipos	
-Gestiona los activos no autorizados.	Equipos	
-Utiliza certificados clientes para autenticar activos hardware.	Equipos	

Nota. Obtenido de la Herramienta CIS SAT.

Control 2: Inventario de Software autorizado y no autorizado.

En este control se hace referencia a una lista actualizada de todo el software autorizado que es requerido en la empresa para fines de negocio en la Tabla 14 se muestra que resultado promedio del *Control 2* tiene un riesgo medio ya red si se encuentra segmentada para la distribución de servidores.

Tabla 15.

Parámetros evaluados en el Control 2

Preguntas de Control CIS C02	Tipo de Activo	Seguridad
-Rastrea información de inventario de software.	Aplicaciones	
-Segrega física o lógicamente las aplicaciones de alto riesgo	Aplicaciones	

Nota. Obtenido de la Herramienta CIS SAT.

Control 3: Gestión continua de vulnerabilidades.

Este control se toma en cuenta para conocer si el administrador de la red realiza escaneos de vulnerabilidades de manera continua y periódica, la Tabla 16 indica que no se realiza este tipo de procesos en los sistemas de la organización por tal razón el nivel de riesgo del *Control 3* es de nivel alto.

Tabla 16.

Parámetros evaluados en el Control 3

Preguntas de Control CIS C03	Tipo de Activo	Seguridad
-Ejecuta herramientas de exploración de vulnerabilidad automatizadas	Aplicaciones	
-Realiza escaneo de vulnerabilidad autenticado	Aplicaciones	
-Implementa herramientas automatizadas de administración de parches de software	Aplicaciones	
-Compara escaneos de vulnerabilidades consecutivos	Aplicaciones	
-Utiliza un proceso de calificación de riesgo.	Aplicaciones	

Nota. Obtenido de la Herramienta CIS SAT.

Control 4: Uso controlado de privilegios administrativos.

El promedio del *Control 4* tiene un nivel de riesgo considerable como se observa en la Tabla 17, debido a que están establecidas ciertas políticas pero de manera informal en referencia a las contraseñas administrativas y algunas de ellas no son únicas y se repiten en varios servidores y aplicaciones.

Tabla 17.

Parámetros evaluados en el Control 4

Preguntas de Control CIS C04	Tipo de Activo	Seguridad
-Cambia contraseñas predeterminadas	Usuarios	
-Usa estaciones de trabajo dedicadas para todas las tareas administrativas.	Usuarios	

Nota. Obtenido de la Herramienta CIS SAT.

Control 5: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores.

Para la configuración de los servidores la empresa si emplea la herramienta Webmin para el monitoreo de aplicaciones en los sistemas, pero no tiene instalada ninguna herramienta de gestión referente a la configuración automatizada, la Tabla 18 muestra que el indicador para este Control 5 es de riesgo Considerable.

Tabla 18.

Parámetros evaluados en el Control 5

Preguntas de Control CIS C05	Tipo de Activo	Seguridad
-Establece configuraciones seguras.	Aplicaciones	
-Implementa herramientas de administración de configuración del sistema	Aplicaciones	
-Implementa sistemas automatizados de monitoreo de configuración	Aplicaciones	

Nota. Obtenido de la Herramienta CIS SAT.

Control 6: Mantenimiento, monitoreo y análisis de registros de auditoría.

En la empresa no hay un proceso de análisis de registro establecido en el que se especifique el tipo de evento, fecha, usuario direcciones involucradas, por este motivo los parámetros en este control tienen el riesgo Alto, pues en caso de una vulnerabilidad no hay un detalle de los eventos producidos, para recuperarse de ataques a futuro.

Tabla 19.

Parámetros evaluados en el Control 6

Preguntas de Control CIS C06	Tipo de Activo	Seguridad
-Activar registros de auditoria	Red	
-Revisar regularmente los registros	Red	

Nota. Obtenido de la Herramienta CIS SAT.

3.4.1.2.Controles Fundacionales.

Estos son controles que las organizaciones deben implementar para contrarrestar amenazas técnicas más específicas (ManageEngine, 2020) en la Figura 26 se muestra el nivel de riesgo de los controles 7 hasta el 16.

Figura 26.

Valoración de los controles CIS fundacionales

Nota. Obtenido de (Centro de Seguridad de Internet, 2020).

Control 7: Protecciones de correo electrónico y navegador web.

Los parámetros de este control validan si los empleados utilizan navegadores seguros y los mismos tienen instalados filtros de contenidos, bloqueadores de ventanas emergentes que puedan originar contenido malicioso, en referencia a los correos se evalúa si hay manejo de filtros de spam que minimice actividades de phishing, de esta manera la Tabla 20 indica que el resultado promedio de este control es de riesgo medio.

Tabla 20.

Parámetros evaluados en el Control 7

Preguntas de Control CIS C07	Tipo de Activo	Seguridad
-Asegura el uso de navegadores y clientes de correo electrónico que cuenten con soporte.	Red	
- Habilita plugins innecesarios de navegadores o clientes de correo electrónico	Red	

Nota. Obtenido de la Herramienta CIS SAT.

Control 8: Defensas de Malware.

Este control se basa principalmente en comprobar si hay software antimalware que defienda continuamente los computadores de los trabajadores así como a los servidores, además las bases de datos de firmas deben están actualizadas, por tanto las medidas evaluadas indican que el riesgo en este control es considerable.

Tabla 21.

Parámetros evaluados en el Control 8

Preguntas de Control CIS C08	Tipo de Activo	Seguridad
-Utiliza software anti-malware de gestión centralizada	Equipos	
-Asegura de que el software y las firmas de Anti-Malware estén actualizados.	Equipos	
-Habilita el registro de consultas DNS	Red	

Nota. Obtenido de la Herramienta CIS SAT.

Control 9: Limitación y control de puertos, protocolos y servicios de red.

La Tabla 22 muestra que el resultado de las medidas analizadas en cuento a la realización de escaneo de puerto no se lo realiza de manera frecuente, resultando así que este control tenga el riesgo alto por falta de aseguramiento en los puertos, protocolos y servicios admitidos.

Tabla 22.

Parámetros evaluados en el Control 9

Preguntas de Control CIS C09	Tipo de Activo	Seguridad
-Asegúrese de que solo se ejecutan los puertos, protocolos y servicios aprobados.	Equipos	
-Realiza escaneos de puertos automatizados regulares	Equipos	
-Implementa aplicaciones de firewalls	Equipos	

Nota. Obtenido de la Herramienta CIS SAT.

Control 10: Capacidades de recuperación de datos.

Los parámetros de este control evalúan la frecuencia con que se realiza las copias de seguridad y los respaldos de los principales servidores de la empresa, además que el proceso de restauración con estas copias se las haga de manera correcta garantizando así la integridad de la información, la Tabla 23 muestra que en la empresa los respaldos no están asegurados con información actualizada.

Tabla 23.

Parámetros evaluados en el Control 10

Preguntas de Control CIS C010	Tipo de Activo	Seguridad
-Asegura copias de seguridad automatizadas regulares	Datos	
-Realizar copias de seguridad completas del sistema.	Datos	
-Datos de prueba en medios de copia de seguridad.	Datos	
-Proteger copias de seguridad.	Datos	

Nota. Obtenido de la Herramienta CIS SAT.

Control 11: Configuración segura para dispositivos de red, como contrafuegos, enrutadores y conmutadores.

El Control 11 se basa en verificar la configuración de seguridad de la infraestructura de red, si posee la versión más estable de una actualización de seguridad en los equipos de red, en la Tabla 24 muestra que la empresa tiene un promedio de riesgo medio pues si existen ciertas normas instaladas y además las conexiones de red están separadas por VLAN.

Tabla 24.

Parámetros evaluados en el Control 11

Preguntas de Control CIS C011	Tipo de Activo	Seguridad
-Mantiene configuraciones de seguridad estándar para los dispositivos de red.	Red	
-Utiliza herramientas automáticas para verificar configuraciones de dispositivos estándar y detectar cambios.	Red	
-Tiene instalada la versión más estable de las actualizaciones relacionadas con la seguridad de los dispositivos de red.	Red	
-Gestiona la infraestructura de red a través de una red dedicada.	Red	

Nota. Obtenido de la Herramienta CIS SAT.

Control 12: Defensas de Límites.

Los parámetros de este control evalúan que los firewalls de capa aplicación filtren el tráfico de red hacia o desde Internet y evitar conexiones no autorizadas.

La Tabla 25 indica que la empresa tiene un firewall instalado pero no tiene un sistema de monitoreo o un sistema de detección de intrusos, como resultado su riesgo es alto.

Tabla 25.

Parámetros evaluados en el Control 12

Preguntas de Control CIS C012	Tipo de Activo	Seguridad
-Mantiene un inventario de límites de red.	Red	
-Administra todos los dispositivos iniciando sesión de forma remota en la red interna	Red	
-Busca conexiones no autorizadas a través de límites de red de confianza	Red	
-Deniega comunicaciones con direcciones IP maliciosas conocidas.	Red	
-Deniega la comunicación sobre puertos no autorizados.	Red	
-Implementa sistemas de prevención de intrusiones basados en la red.	Red	

Nota. Obtenido de la Herramienta CIS SAT.

 *Control 13: Protección de datos.*

El Control 13 se basa en el manejo de información sensible de la empresa, si esta se elimina y se supervisa de manera responsable, si los dispositivos de almacenamiento USB, discos duros son configurados para que no se sobrescriban, los resultados de este control se muestran en la Tabla 26 obteniendo un riesgo alto puesto no se analiza estas medidas protección.

Tabla 26.

Parámetros evaluados en el Control 13

Preguntas de Control CIS C013	Tipo de Activo	Seguridad
-Elimina datos o sistemas confidenciales a los que la organización no accede regularmente	Datos	
-Supervisa y bloquea el tráfico de red no autorizado	Datos	
-Gestionar las configuraciones de lectura/escritura de sistemas para medios removibles externos	Datos	

Nota. Obtenido de la Herramienta CIS SAT.

 *Control 14: Control de acceso basado en la necesidad de conocer.*

La empresa si tiene segmentación de red y la información está clasificada en los servidores pero estos datos en tránsito no se manejan de manera cifrada por lo que como resultado en la Tabla 27, el riesgo para este control es considerable.

Tabla 27.

Parámetros evaluados en el Control 14

Preguntas de Control CIS C014	Tipo de Activo	Seguridad
-Segmenta la red en base a la sensibilidad.	Datos	
-Utiliza una herramienta de detección activa para identificar datos confidenciales.	Red	

Nota. Obtenido de la Herramienta CIS SAT.

Control 15: Control de acceso inalámbrico.

La organización si controla los puntos de acceso y sistema de cliente inalámbricos ya que tiene instalado una Cisco Wireless LAN Controller 2504 que alerta sobre puntos de acceso inalámbrico no autorizados conectados a la red por esta razón el promedio de riesgo en el *Control 15* es de nivel medio, como se muestra en la Tabla 28.

Tabla 28.

Parámetros evaluados en el Control 15

Preguntas de Control CIS C015	Tipo de Activo	Seguridad
-Crea una red inalámbrica separada para dispositivos personales y no confidenciales.	Red	
-Detecta puntos de acceso inalámbricos conectados a la red cableada.	Red	
-Deshabilita el acceso inalámbrico en dispositivos si no es requerido.	Equipos	
-Limita el acceso inalámbrico en dispositivos cliente.	Equipos	

Nota. Obtenido de la Herramienta CIS SAT.

Control 16: Monitoreo y control de cuentas.

El control 16 se basa en asegurar las cuentas, monitoreando los accesos a cuentas que hayan sido ya desactivadas por el administrador de red y vigilando que haya un bloque automático si los trabajadores no están utilizando las estaciones, la Tabla 29

indica que el nivel promedio de riesgo en este caso es considerable, ya que no se practica un inventario de cuentas los usuarios de la empresa.

Tabla 29.

Parámetros evaluados en el Control 16

Preguntas de Control CIS C016	Tipo de Activo	Seguridad
-Bloquea sesiones de estaciones de trabajo después de inactividad.	Usuarios	
-Mantiene un inventario de cuentas.	Usuarios	
-Desactiva cuentas inactivas.	Usuarios	

Nota. Obtenido de la Herramienta CIS SAT.

3.4.1.3.Controles Organizacionales.

Los controles C17-20 no están enfocados en controles técnicos, sino las líneas de seguridad se orientan en las personas y los procesos de planes de formación y concientización del personal, la Figura 27 muestra el nivel de riesgo del último rango de controles.

Figura 27.

Valoración de los controles CIS fundacionales

Nota. Obtenido de (Centro de Seguridad de Internet, 2020).

Control 17: Programa de capacitación y concientización sobre seguridad.

Este control se trata sobre la capacitación a los empleados sobre las diferentes formas de ataques de ingeniería social, fraudes telefónicos, phishing, llamadas de suplantación entre otras que puedan comprometer información de negocios de la empresa. La Tabla 30 muestra los resultados de la empresa en los que si se ha hablado

sobre estos temas pero solo de manera informal y se los realiza semestral o anualmente resultando un riesgo alto a corto o mediano plazo.

Tabla 30.

Parámetros evaluados en el Control 17

Preguntas de Control CIS C017	Seguridad
-Realiza un análisis de brechas de habilidades	
-Implementa un programa de conciencia de seguridad	
-Capacita a la fuerza laboral en la identificación de ataques de ingeniería social.	
-Capacita a la fuerza laboral en el manejo de datos confidenciales.	
-Capacita a la fuerza laboral sobre las causas de la exposición involuntaria de datos.	

Nota. Obtenido de la Herramienta CIS SAT.

Control 18: Seguridad del desarrollo de software.

El control 18 no fue considerado en la autoevaluación porque la empresa no desarrolla ningún tipo de software internamente por esta razón el lenguaje de programación no se basa en ninguna norma de codificación segura.

Control 19: Respuesta y manejo de incidentes.

En la empresa no se lleva a cabo simulaciones de escenarios de incidentes para crear conciencia a la hora de manejar amenazas reales, es así que en la Tabla 31 se muestra los resultados consultados al administrador que manifiesta que si se encuentra asignadas las personas responsables cuando se presente estos eventos, y todos los incidentes informáticos no cuentan con los informes respectivos por esto se considera a este control con un riesgo de nivel medio.

Tabla 31.

Parámetros evaluados en el Control 19

Preguntas de Control CIS C019	Seguridad
-Asigna cargos y responsabilidades para la respuesta a incidentes	
-Designa personal de administración para apoyar el manejo de incidentes	
-Mantiene información de contacto para reportar incidentes de seguridad	
-Publica información sobre informes de anomalías e incidentes informáticos	

Nota. Obtenido de la Herramienta CIS SAT.

Control 20: Pruebas de penetración.

El último control se basa en conocer si la empresa realiza pruebas de penetración tanto internas como externas para identificar y detener ataques en los que se utilice herramientas de exploración de vulnerabilidades, en la Tabla 32 se indica que no se lleva a cabo ningunas de estas pruebas por lo que el riesgo es alto y es la razón principal de esta investigación y por la que se lleva a cabo un pentesting detallado en el capítulo 4.

Tabla 32.

Parámetros evaluados en el Control 20

Preguntas de Control CIS C020	Seguridad
-Establece un programa de pruebas de penetración	●
-Lleva a cabo pruebas de penetración interna y externa	●
-Utiliza herramientas de pruebas de penetración y exploración de vulnerabilidades	●
-Asegura que los resultados de la prueba de penetración estén documentados usando estándares abiertos y legibles	●
-Control y seguimiento de cuentas asociadas a pruebas de penetración.	●

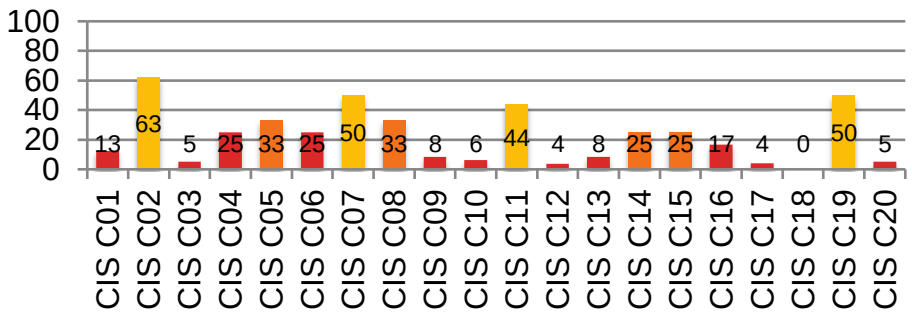
Nota. Obtenido de la Herramienta CIS SAT.

3.4.2. Resultados de la autoevaluación con CIS SAT.

Después de haber realizado el análisis en todos los controles de la herramienta CIS SAT, los resultados obtenidos se muestran a continuación en la Figura 28:

Figura 28.

Resultados de la evaluación de los controles CIS del 1-20



Nota. Obtenido de (Centro de Seguridad de Internet, 2020).

Tabla 33.

Resumen Controles CIS

Puntaje	Controles CIS	Estado	Riesgo
> = **50**	C02, C07, C011, C019	Implementado	Medio
> = **25**	C05, C08, C014, C015	Documentado	Considerable
> **0**	C01, C03, C04, C06, C09, C10, C012, C013, C16, C017, C020	Definido (Inicial)	Alto

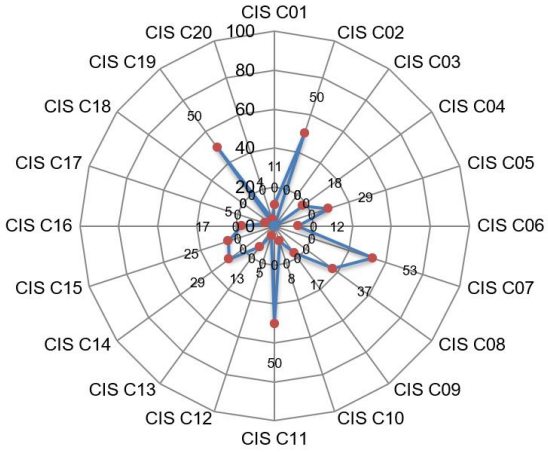
Nota. Obtenido de (Centro de Seguridad de Internet, 2020).

En resumen, en la Tabla 33 se tiene que los controles con el riesgo más alto a posibles ataques son los relacionados en los ejes de: limitación y control de puertos, protocolos y servicios de la red puesto a que no existe una defensa de limite en la capa de red, ni en la capa de aplicación. Otra debilidad bastante considerable es la falta de supervisión en las cuentas y protección de los datos privilegiados debido a que no existe un programa de conciencia de la seguridad de la información en los empleados, por lo que es necesario que el administrador de red tome las medidas correctivas necesarias para mitigar estas falencias que en este caso corresponden a la limitación del tráfico no autorizado mediante reglas de firewall, cerrado de puertos innecesarios, inventario de activos, certificados y licencias de software para tener conexiones más seguras, en la Figura 29 se muestra el Diagrama de Radar con los parámetros evaluados en cada control.

Los controles con riesgo considerable tienen definidas ciertas políticas, pero algunos de ellos no han sido implementados en todos los departamentos de la empresa, como es el caso de las contraseñas predeterminadas y configuraciones estándar para los dispositivos de la red, en este caso para mejorar estos controles es necesario establecer contraseñas robustas tanto en los equipos como en las cuentas de los usuarios.

Figura 29.

Diagrama de Radar



Nota. Obtenido de (Centro de Seguridad de Internet, 2020).

Los resultados de la evaluación de los controles CIS del 1-20 en un estado inicial quedarían como se muestra en la Tabla 34.

Tabla 34.

Estado Inicial de Controles CIS

Controles	**Riesgo**	**Valoración**
C01. Inventario y control de activos de hardware		Alto
C02. Inventario y control de activos de software		Medio
C03. Gestión continua de vulnerabilidades		Alto
C04. Uso controlado de los privilegios administrativos		Alto
C05.Configuración segura para el hardware y el software de las estaciones de trabajo y servidores		Considerable
C06.Mantenimiento, monitoreo, y análisis de logs de auditoría		Alto
C07. Protección de correo electrónico y navegador web		Medio
C08. Defensas contra malware		Considerable

C09. Limitación y control de puertos de red, protocolos y servicios	🔴	Alto
C10. Funciones de recuperación de datos	🔴	Alto
C11.Configuración segura para dispositivos de red, tales como firewalls, routers y switches	🟡	Medio
C12. Protección perimetral	🔴	Alto
C13. Protección de datos	🔴	Alto
C14. Control de acceso basado en la necesidad de saber	🟠	Considerable
C15. Control de acceso inalámbrico	🟠	Considerable
C16. Monitoreo y control de cuentas	🔴	Alto
C17. Implementar un programa de concienciación y capacitación en seguridad	🔴	Alto
C18. Seguridad del software de aplicación	No considerado	-
C19. Respuesta y gestión de incidentes	🟡	Medio
C20. Pruebas de penetración y ejercicios de equipo rojo	🔴	Alto

Nota. Elaboración propia

Además uno de aspectos que se debe tener cuenta en estos controles es el grupo de implementación en los que están considerados cada uno de ellos, teniendo así:

Grupo IG1: Corresponde a pequeñas o medianas empresas con recursos limitados de TI y con un mínimo conocimiento en ciberseguridad para proteger los activos y la sensibilidad de la información que se maneja en la empresa es baja.

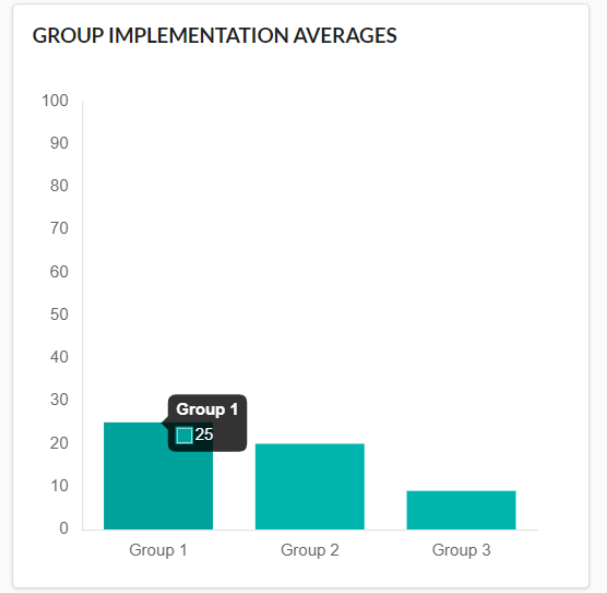
Grupo IG2: Comprende a medianas y grandes empresas con múltiples departamentos en donde se maneja y almacena información sensible de los clientes.

Grupo IG3: Las grandes empresas con recursos significativos y exposición de alto riesgo para el manejo de activos y datos críticos deben asignar las salvaguardias bajo IG3 junto con IG1 e IG2 (CIS CSAT Pro, 2018).

En la gráfica 30 se observa que las salvaguardas que tiene implementadas en la empresa son de 25 en el grupo de IG1 pues la empresa Sinfotecnia al ser una pequeña empresa con pocas dependencias está en esta categoría. Y para ayudar mejorar las salvaguardas que no es tan definidas ni aplicadas se realiza el proceso de las etapas PTES en el capítulo 4.

Figura 30.

Salvaguardas IG1 implementadas en la empresa Sinfotecnia.



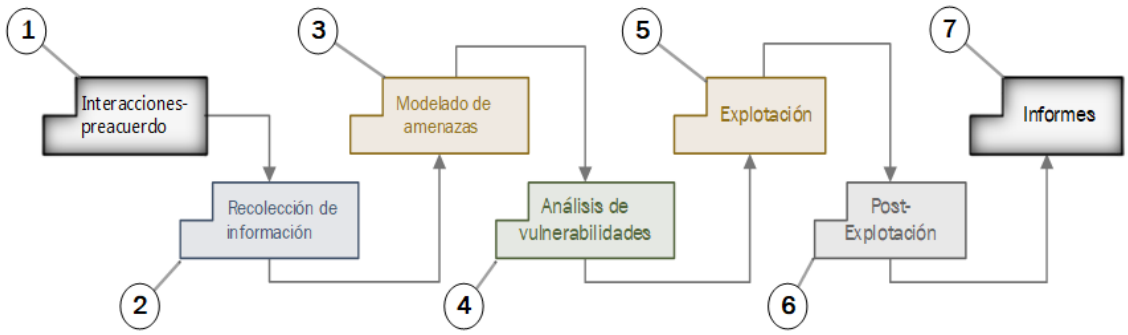
Nota. Obtenido de la Herramienta CIS SAT.

4. CAPÍTULO IV. Desarrollo del Modelo de Seguridad para VoIP.

Después de haber efectuado el análisis del sistema de Telefonía VoIP en la empresa Sinfotecnia, se procede a seguir las 7 etapas basándose en la metodología PTES como se muestra en la Figura 31, además de las herramientas definidas en cada etapa, teniendo en cuenta el estándar en el que se encuentra definida esta metodología y las secciones que se encuentren enfocadas en la tecnología de voz sobre IP.

Figura 31.

Fases de un pentesting usando PTES



Nota. Adaptado de (Pentest Standard, 2012)

4.1. PRIMERA ETAPA. Interacciones Preacuerdo.

En la primera etapa se determina el alcance del proyecto que demuestre que el cliente conoce y aprueba las actividades del auditor, estableciendo los términos y condiciones sobre lo que se puede esperar de una prueba de penetración exhaustiva, brindando las facilidades necesarias durante la ejecución por parte de la empresa a ser auditada. Además de discutir la carta de compromiso y las reglas de operación con el fin de evitar malentendidos y falsas perspectivas.

4.1.1. Introducción al alcance

Como primer paso es importante definir con el gerente de la Empresa Sinfotecnia el alcance que tendrá este test de intrusión, el cual se describe a continuación:

> "Este Modelo de Seguridad sobre la Telefonía VoIP tiene como alcance el desarrollo de las 7 etapas de la metodología PTES con el fin de detectar las vulnerabilidades, el nivel de acceso y el grado de seguridad externo e interno, mediante la ejecución de pruebas no maliciosas que no perjudiquen el desempeño normal de la empresa, para de esta forma plantear las medidas preventivas ante las debilidades encontradas; las mismas que estarán detalladas en un informe de políticas de seguridad logrando así conseguir una mayor seguridad en las comunicaciones".

4.1.2. Test de Intrusión.

En esta investigación se emplea el testeo de CAJA BLANCA, ya que se tiene la autorización del gerente de la Empresa Sinfotecnia para tener el acceso a las instalaciones, así como a la información que se requiera para la elaboración de estas pruebas de penetración, como se muestra en el **ANEXO A**.

- **Pruebas de caja negra.**

Son pruebas funcionales en las que no se tiene conocimientos específicos sobre el mecanismo interno del sistema, tampoco se tiene acceso al código fuente ni a ninguna estructura lógica interna del sistema. Estas pruebas s e realizan a nivel exterior en las que se imite el procedimiento que realiza un atacante externo a la organización. (Chaudhary & Falakbanu, 2016)

- **Prueba de caja blanca.**

Son pruebas estructurales en las que se tiene acceso y conocimiento sobre el código, documentos y estructura lógica del sistema de manera que permitan revelar datos, errores y vulnerabilidades de la arquitectura. Además, tiene mayor cobertura al momento de crear casos de pruebas internas al sistema.

- **Prueba de caja gris.**

Es una combinación de caja blanca y negra en la que se tiene información limitada del sistema, pero se tiene acceso a nivel exterior, es decir las pruebas realizadas son más efectivas porque se trata de examinar los defectos debido a la infraestructura incorrecta o el uso inadecuado de aplicaciones.

4.1.3. Objetivos y tiempo de duración.

Los objetivos generales y específicos para este Modelo de Seguridad se encuentran detallados en el capítulo 2 en el aparatado de los antecedentes, además se define las fechas para cada prueba y el tiempo estimado que tomará la ejecución de este pentest. **(**Ver **Tabla 35** y **ANEXO B**).

Tabla 35.

Distribución de horarios

IMPLEMENTACIÓN PTES	**Tiempo de Ejecución**	**% de avance**
FASE I. Planeación y definición de acuerdos.	2 semana	10%
FASE II. Recopilación de la información.	2 semanas	30%
FASE III. Modelado e identificación de amenazas.	4 semanas	45%
FASE IV. Análisis de las vulnerabilidades	6 semanas	55%
FASE V. Explotación de la información encontrada.	3 semanas	70%
FASE VI. Post Explotación.	3 semanas	85%
FASE VII. Entrega de Informes	6 semanas	100%
TOTAL TIEMPO ESTIMADO	26 semanas	

Nota. Elaboración propia

4.1.4. Reglas de compromiso.

El auditor tendrá la responsabilidad de cumplir con las siguientes premisas y firmar un acuerdo de no divulgación en el que las dos partes interesadas estén de acuerdo en los procedimientos a llevarse a cabo (**Ver ANEXO C**).

I. Los test de vulnerabilidad se deberán realizarán con mucho cuidado para no tener fallas de servidores, inactividad de operaciones u otros inconvenientes causados por actividades de escaneo.

II. Por ningún motivo se autoriza al auditor a divulgar la información obtenida de la Empresa Sinfotecnia en este proceso investigativo.

III. En caso de obtener un resultado destructivo, la prueba deberá ser interrumpida inmediatamente y ser informada al Gerente Técnico y en caso de ser el caso realizar tareas de recuperación.

IV. Se debe entregar toda la información recopilada en la que ninguna de las partes utilizará información de la otra para su beneficio independiente.

V. Impedir la copia o declaración de información privada a terceros, a excepción de tener la aprobación por parte del Gerente de la Empresa.

VI. Se debe entregar un informe ejecutivo que detalle la información obtenida en el análisis de vulnerabilidades, pruebas de testeo con las debidas correcciones, sugerencias y conclusiones a los problemas encontrados.

VII. Debe constar un acta suscrita de finalización de actividades entre las dos partes de manera que se haya cumplido con los objetivos de esta auditoría y obtenido el resultado que se esperaba.

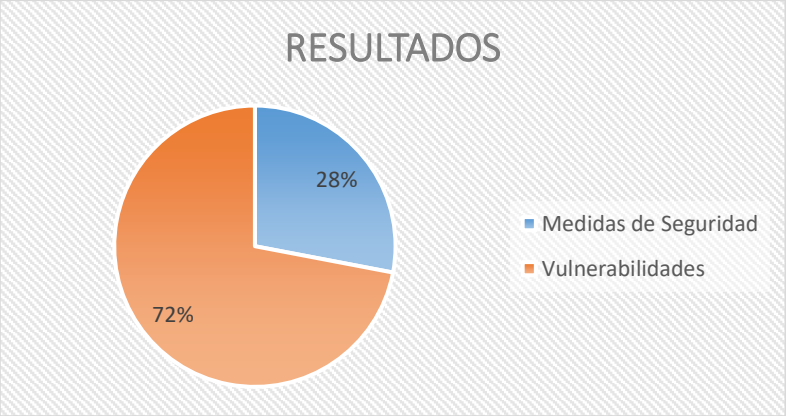
4.1.5. Entrevista técnica.

La entrevista técnica tiene como finalidad discutir lo que se va a analizar, conocer los posibles riesgos a los que se encuentra expuesta la red de VoIP para obtener información relevante desde el punto de vista del Gerente Técnico.

El modelo de entrevista planteada se basa en preguntas informativas y dicotómicas cuyas respuestas deberían ser afirmativas para obtener el máximo nivel de seguridad a esta evaluación de vulnerabilidades (Ver **Figura 32** y **ANEXO D**).

Figura 32.

Resultados de las vulnerabilidades que existen en Sinfotecnia



Nota. Autoría propia

- **Análisis:**

Como se puede apreciar en la figura 32 el porcentaje de medidas de seguridad adoptadas por la empresa Sinfotecnia representa solo el 28% mientras que las vulnerabilidades que existen actualmente abarcan el 72% por lo que es necesario llevar a cabo el proceso del pentest a fin de poder mitigar esas fallas y tener un mayor porcentaje en cuanto a recomendaciones de seguridad que se deben implementar.

Como primera observación se registra que la empresa no cuenta con un firewall empresarial, o con algún sistema de IDS/IPS que permita la detección de intrusos.

4.1.6. Herramientas para el análisis de vulnerabilidades en VoIP.

Para llevar a cabo una prueba de penetración completa es necesario la ejecución de varias herramientas seguridad las cuales pueden ser libre y de ámbito comercial; a continuación, se detallan las que se considera más idóneas para la explotación de redes de VoIP.

- **KALI LINUX:** Es el sucesor de la plataforma de pruebas de penetración BackTrack. Contiene varias herramientas que permiten llevar a cabo varias funciones como pentest, análisis forense, gathering o la explotación entre otras (González, Sanchéz, & José, 2015).
- **NMAP:** Es una herramienta de exploración de puertos que permite escanear hosts para identificar los servicios que se ejecutan en cada uno de estos.
- **SVMAP:** Es un escáner de red para SIP que se encarga de escanear la red buscando dispositivos y puertos específicos es similar a Nmap (González, Sanchéz, & José, 2015).
- **SVWAR:** Esta herramienta está diseñada para obtener usuarios de una PBX o de un servidor VoIP (González, Sanchéz, & José, 2015).
- **ETTERCAP**: Es un sniffer para los ataques MiT y es compatible con muchos protocolos, e incluye muchas características para el análisis de la red y de host.
- **WIRESHARK:** Es un analizador de protocolos, utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, porque permite ver todo el tráfico que pasa a través de una red.
- **NESSUS**: Es un programa de escaneo de vulnerabilidades que resulta útil para encontrar y documentar vulnerabilidades principalmente desde el interior de una red dada (Pentest Standard, 2012).

4.2. SEGUNDA ETAPA. Recolección de Información.

Esta fase consiste en recopilar cualquier información que se pueda obtener sobre la Empresa afectada, es decir desde la información pública posteada en redes sociales, listas de organización en anuncios de empleo, perfiles de LinkedIn de empleado, y artículos de noticias recientes, Google hacking, hasta el fingerprinting en el cual ya se utiliza herramientas más específicas. La información que se logre recopilar dará la pauta sobre los tipos de controles de seguridad que la empresa tiene ejecutada actualmente.

4.2.1. Reconocimiento Pasivo

El reconocimiento pasivo e indirecto no implica una interacción directa con la red de destino y permite descubrir información de los objetivos sin tener contacto con los sistemas de una red.

Este se centra en los negocios, entorno de la empresa y los empleados, cuya información de este tipo está disponible en Internet u otras fuentes públicas llamado también Inteligencia de código abierto (OSINT) (Beggs, 2014).

4.2.1.1.Inteligencia de código abierto OSINT

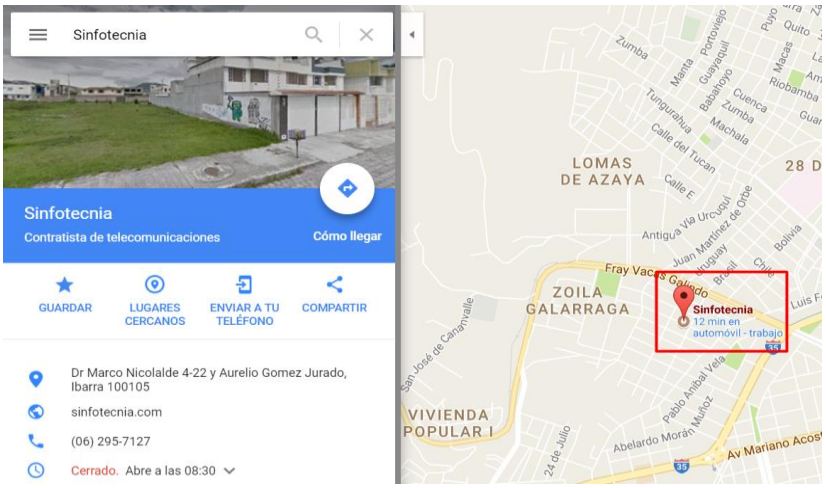
Es una forma de utilizar la información abierta de fácil acceso para adquirir datos sobre un determinado objetivo. La recolección de OSINT especialmente comienza con una revisión de la presencia en línea del objetivo esto puede ser en sitio web, blogs, páginas de medios sociales que incluye lo siguiente:

- *Ubicación geográfica de las oficinas matriz y sucursales en caso de tenerlas.*

Para tener la ubicación del objetivo, se utiliza la aplicación web Google Maps, la cual proporciona la dirección exacta de la Empresa Sinfotecnia como se puede observar en la Figura 33.

Figura 33.

Ubicación geográfica de la empresa Sinfotecnia



Nota. Obtenido de http://www.google.com/maps

También se puede verificar la información de contacto y de ubicación en la página web de la empresa la cual es https://sinfotecnia.com y como se puede observar en la Figura 34, la página web solo es informativa acerca de sus servicios y productos; no es una página de e-commerce por lo que no han información relevante que se deba analizar.

Figura 34.

Página Web de la Empresa Sinfotecnia

Nota. Obtenido de http://www.sinfotecnia.com/

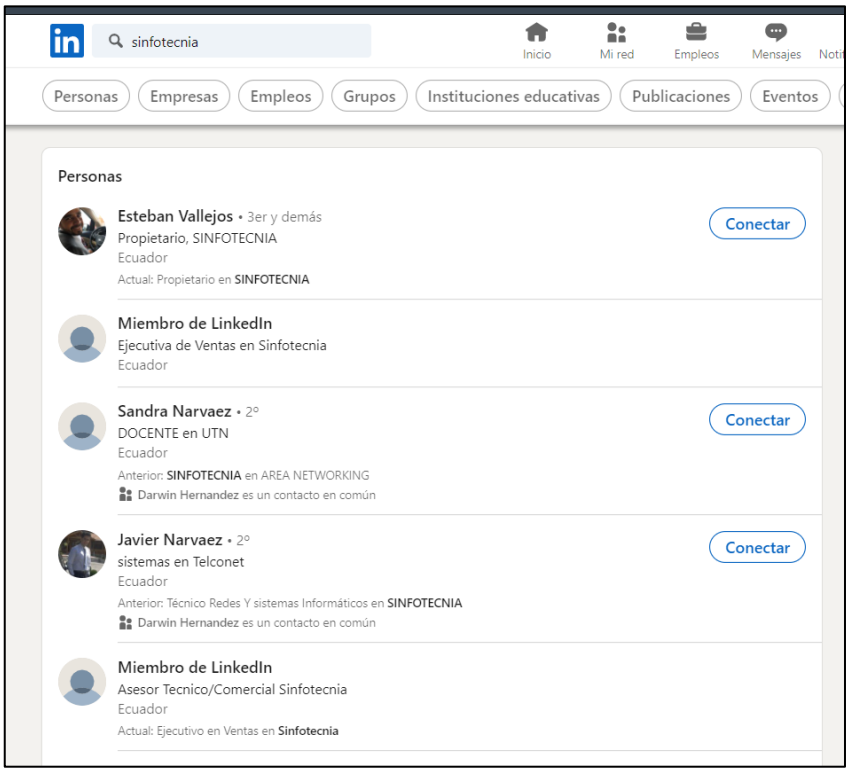
- ***Redes sociales*** *(LinkedIn, Facebook, Instagram y Twitter).*

Las redes sociales tienen un gran impacto en el ámbito profesional por lo que a través de la plataforma LinkedIn se puede encontrar el currículo de una persona, su grupo de contactos y las personas que se encuentra vinculadas a una determinada empresa.

En este caso si se busca la empresa Sinfotecnia en LinkedIn como se muestra en la Figuras 35 y 36, se obtiene como resultado la identidad de varias personas que encuentran trabajando o que prestaron sus servicios en años atrás, de las cuales se puede obtener contactos y correos electrónicos, etc.

Figura 35.

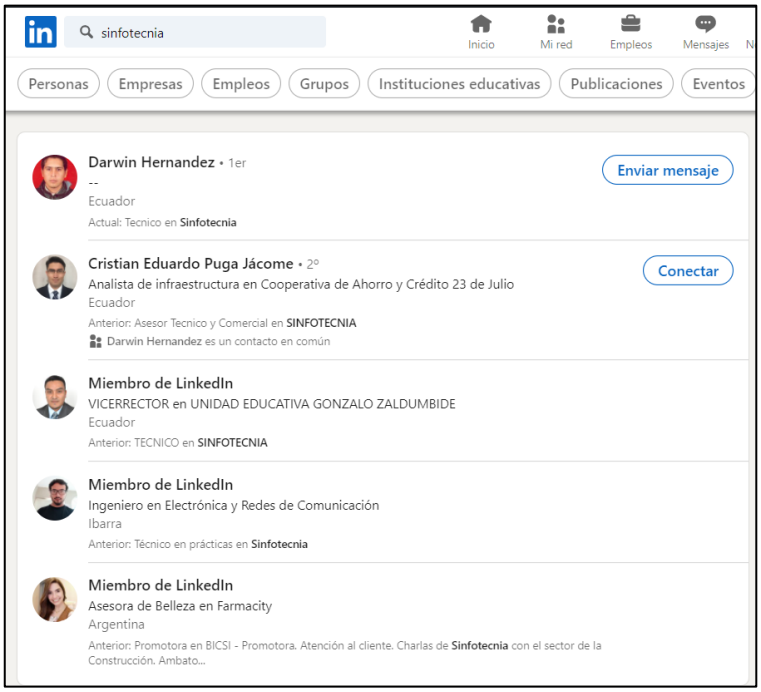
Empleados de la empresa Sinfotecnia



Nota. Obtenido de:
https://www.linkedin.com/search/results/index/?keywords=sinfotecnia&origin=GLOBAL_SEARCH_HEADER

Figura 36.

Empleados de la empresa Sinfotecnia

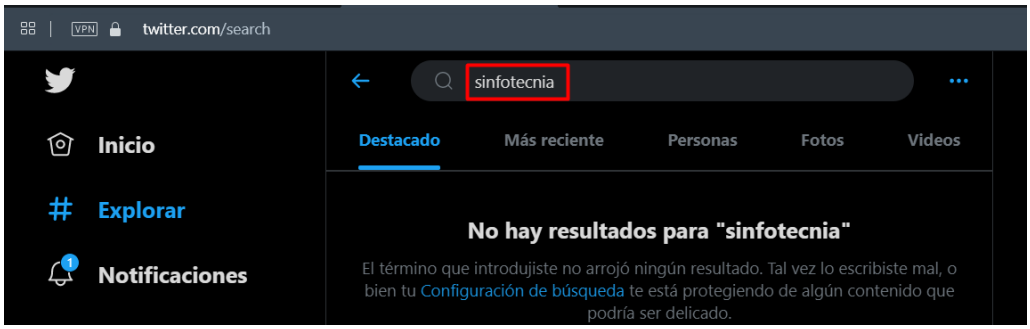


Nota. Obtenido de: https://www.linkedin.com/search/results/all/?keywords=sinfotecnia&origin=GLOBAL_SEARCH_HEADER&page=2

En Twitter en la Figura 37 se observa que no se encuentra creada una cuenta oficial sobre la empresa por lo que no hay posteado ningún tipo de información o coincidencias importantes en esta red social,

Figura 37.

Sinfotecnia en Twitter



Nota. Obtenido de https://twitter.com/search?q=sinfotecnia&src=typed_query

La empresa tiene una página oficial en Facebook como se observa en la Figura 38, pero no se tiene ninguna información relevante sobre clientes o empresa asociadas a ella, al igual que la pagina solo es informativa y no es usada para ventas.

Figura 38.

Sinfotecnia en Facebook

Nota. Obtenido de https://www.facebook.com/pages/SINFOTECNIA/126910157350529?pnref=lhc

En la plataforma de Instagram de la Figura 39 se visualiza que la cuenta tiene pocos seguidores y solo hay publicaciones de marketing por lo que se concluye que no hay un registrado en las redes sociales.

Figura 39.

Sinfotecnia en Instagram

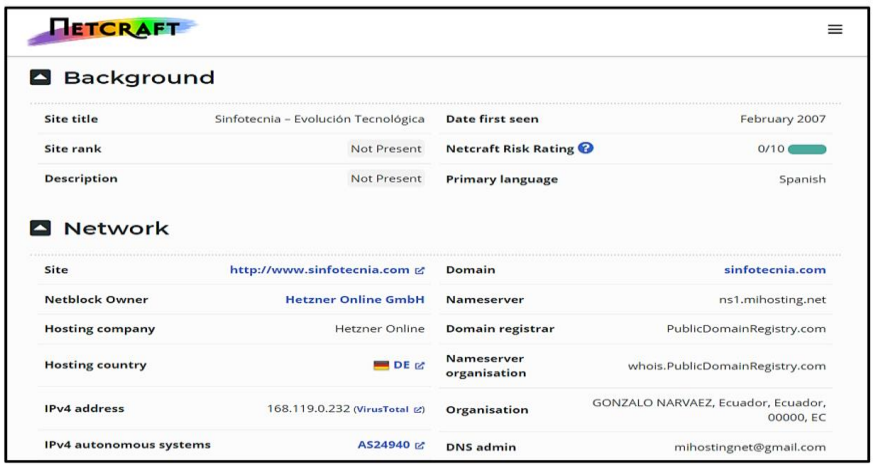
Nota. Obtenido de https://www.instagram.com/sinfotecnia.ec/

- ***Sitios que facilitan búsquedas de información DNS, rutas y servidores***

Ingresando el dominio www.sinfotecnia.com en el sitio Netcraft, se obtiene información sobre la ubicación de la empresa como se observa en la Figura 40, además se obtiene el tipo de servidor web cuya versión es un Nginx.

Figura 40.

Página principal de Netcraft

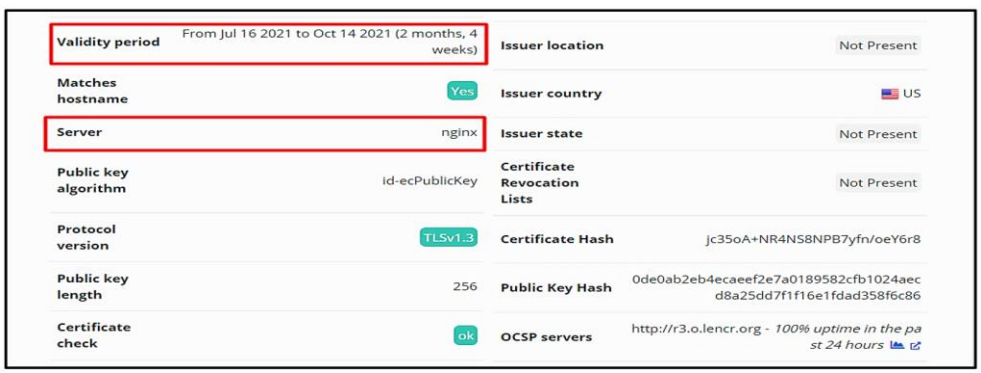


Nota. Obtenido https://sitereport.netcraft.com/?url=http://www.sinfotecnia.com

Adicionalmente en la Figura 41 y en el reporte de https se tiene página relacionas con este dominio, así como el periodo de validación de los certificados SSL y los certificados del hash de la página web de la empresa.

Figura 41.

Información del sitio web de Sinfotecnia



Nota. Obtenido http://searchdns.netcraft.com/

4.2.1.2.Whois

Es un protocolo TCP basado en una petición/respuesta para realizar consultas a través de líneas de comandos sobre el propietario de un nombre de dominio o dirección IP pública. Como se realizó anteriormente están consultas también se las puede hacer a través de sitios de búsquedas de una página web a través de un dominio (González, Sanchéz, & José, 2015).

Además, permite realizar búsquedas para localizar otros dominios alojados en el mismo servidor y de esta manera el atacante puede explotarlos para obtener acceso administrativo al servidor pudiendo así comprometer el servidor de destino. (Beggs, 2014).

En la herramienta Kali Linux ingresar el siguiente comando: #**whois** dominio-empresa

En la figura 42 se puede observar que el código 303 indica que el recurso solicitado por el navegador se encuentra alejado por un tercero por lo que está fuera de alcance de esta prueba de penetración y lo único que se tiene es el correo que utilizo el administrador para el registro.

Figura 42.

Información del DNS de Sinfotecnia

Nota. Autoría propia.

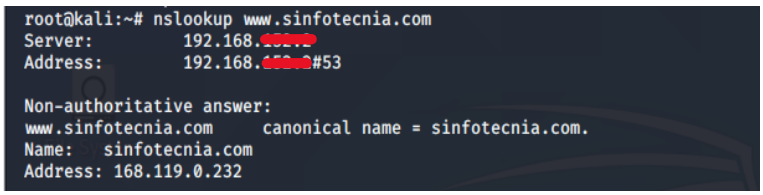
4.2.1.3.Nslookup

Para obtener la dirección pública del dominio sinfotecnia.com se utilizará el comando **nslookup** en el terminal de una computadora con sistema Linux.

En el terminal de Kali Linux aparece solo las direcciones del DNS principal y secundario como se muestra en la Figura 43.

Figura 43.

Obtención de la IP pública de Sinfotecnia en Kali-Linux



Nota. Autoría propia

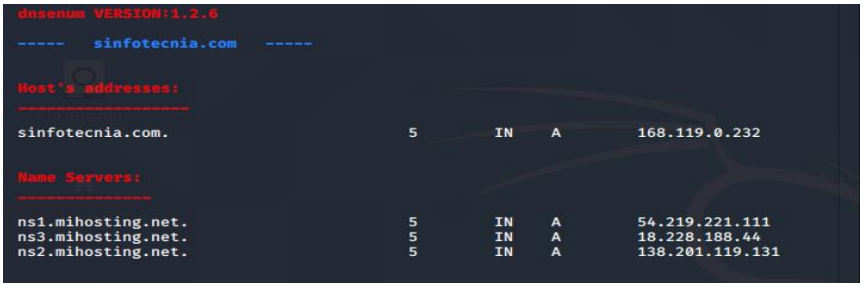
4.2.1.4.DNS- Dnsenum.

Permite obtener información de los servidores DNS en la que se puede apreciar la transferencia de zona habilitado ingresando este comando: **#dnsenum dominio-web**

Si el servidor DNS está configurado para permitir una transferencia de zona a cualquier solicitante podrá obtener nombres de host y direcciones IP de sistemas (Beggs, 2014), pero en este caso en la Figura 44 no se evidencia ninguna dirección correspondiente a la empresa.

Figura 44.

Descubriendo servidores DNS

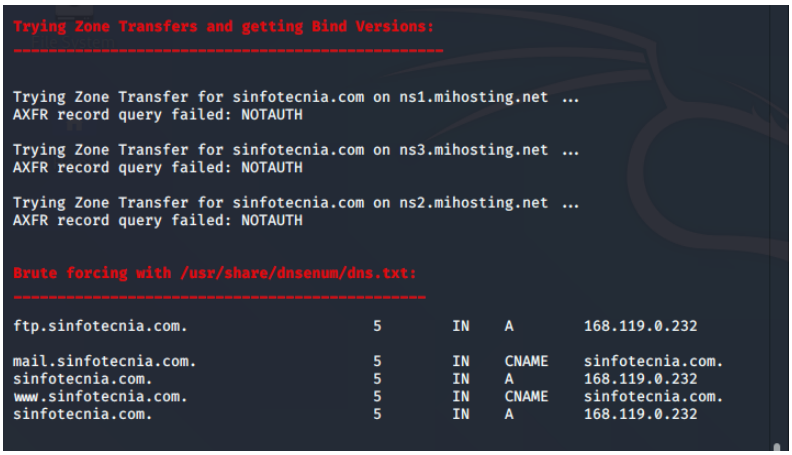


Nota. Autoría propia

La captura de pantalla de la Figura 45 muestra que la petición a la zona de transferencia es no autorizada por esta razón no es posible obtener las direcciones de otros servidores.

Figura 45.

Zona de transferencia DNS



Nota. Autoría propia

A través de la opción **dnsrecon** también es posible obtener el registro SOA, servidores de nombres NS, hosts de intercambio de correo MX y servidores que envían mensajes de correo electrónico (Beggs, 2014). En la figura 46 se muestra que no hay una búsqueda de los registros SRV los cuales se utilizan por ejemplo en protocolos SIP.

Figura 46.

Empleando comando dnsrecon

Nota. Autoría propia

4.2.2. Reconocimiento Activo.

El reconocimiento activo implica consultas directas con el sistema que va a ser infiltrado y este se basa en los resultados obtenidos en la inteligencia de código abierto cuyo reconocimiento es casi indetectable. En primera instancia se debe verificar la información proporcionada por el administrador de la red de la empresa Sinfotecnia en relación con el direccionamiento de la red local.

4.2.2.1.Conectividad de la Red

Las Vlans se encuentran configuradas en el Switch de capa3 (Cisco SG 300) para verificar su estado se puede ingresar al router mediante SSH y través del comando **show vlan** se verifica los puertos designados a cada una de ellas como muestra la Figura 47.

Figura 47.

Verificación de distribución de Vlans en Sw1

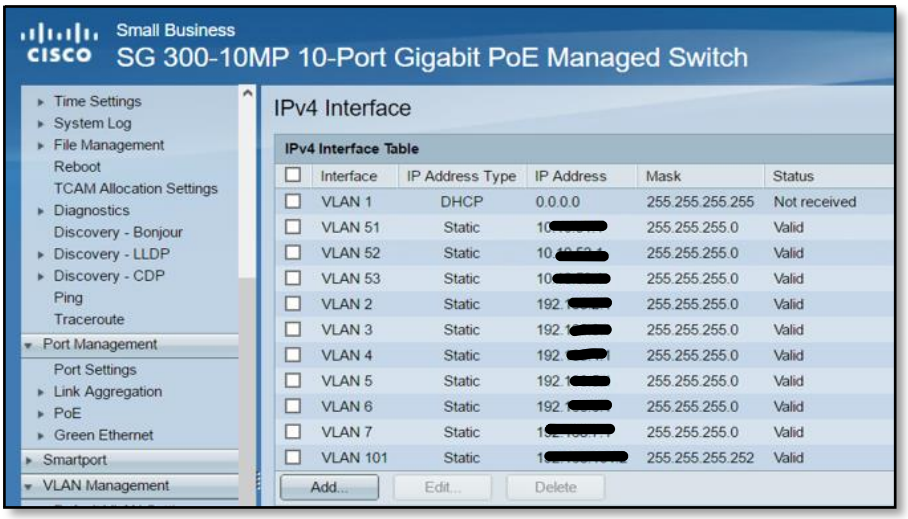
```
SW1-Sinfo#show vlan

Vlan       Name                  Ports                Type      Authorization
---- ----------------- ------------------------- ------------ -------------
 1          1              gi8,gi10,Po1-8          Default      Required
 2         DATOS                gi8               permanent    Required
 3          VOZ                gi6,gi8             permanent    Required
 4       WIRELESS             gi8,gi10             permanent    Required
 5      VIGILANCIA              gi8                permanent    Required
 6      INGENIERIA            gi2,gi8,gi10         permanent    Required
 7         ADMIN              gi1,gi8,gi10         permanent    Required
 8          8                    gi8               permanent    Required
 9          9                    gi8               permanent    Required
10         10                    gi8               permanent    Required
11         11                    gi8               permanent    Required
12         12                    gi8               permanent    Required
13         13                    gi8               permanent    Required
14         14                    gi8               permanent    Required
15         15                    gi8               permanent    Required
16         16                    gi8               permanent    Required
17         17                    gi8               permanent    Required
18         18                    gi8               permanent    Required
19         19                    gi8               permanent    Required
20         20                    gi8               permanent    Required
30        IPV6                   gi8               permanent    Required
51   ADMIN-WIRELESS            gi2-5,gi8           permanent    Required
52     WIFI_GADMA              gi2,gi4,gi8          permanent    Required
53   WIFI_INVITADOS            gi2,gi4,gi8          permanent    Required
101      INTERNET                gi7-8             permanent    Required
```

Nota. Autoría propia

En la Figura 48 también ingresando al Switch de manera gráfica se puede observar las vlans que se encuentran creadas con su respectiva dirección IP.

Figura 48.

Interfaz gráfica del Switch 1



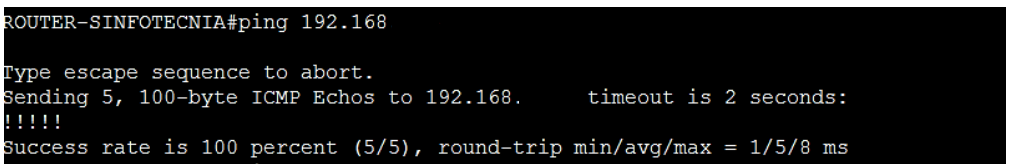
Nota. Autoría propia

Ping desde el Router hacia las distintas subredes (VLANs).

- *Efectuando un ping desde el Router hacia la red de datos ver en la Figura 49.*

Figura 49.

Ping desde Router a la Vlan de datos

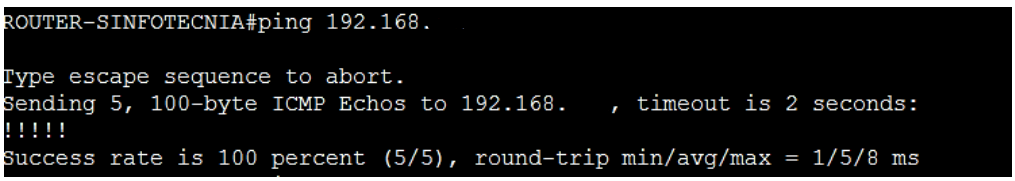


Nota. Autoría propia

- *Figura 50 muestra el ping desde el Router hacia la red de telefonía.*

Figura 50.

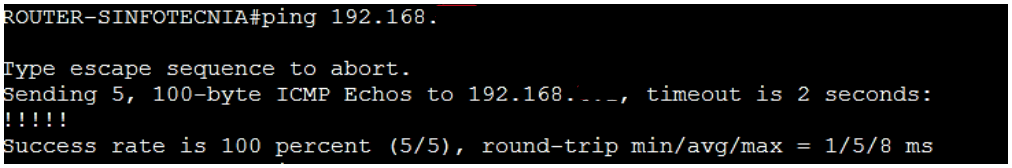
Ping desde Router a la Vlan de telefonía



- *Ping desde el Router hacia la red inalámbrica se indica en la Figura 51.*

Figura 51.

Ping desde Router a la Vlan Wireless.



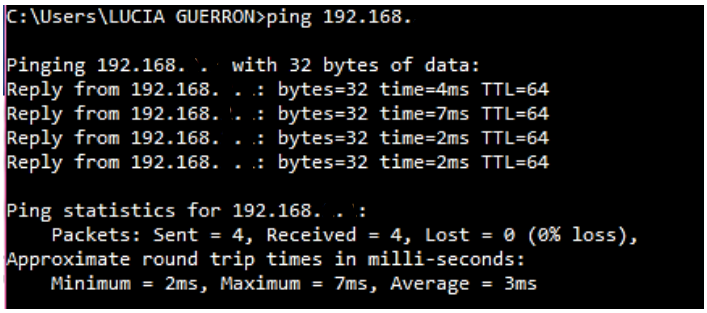
Nota. Autoría propia

Ping desde un equipo terminal hacia las distintas subredes (VLANS).

- *Verificando el ping desde una PC hacia la red de datos ver en la Figura 52.*

Figura 52.

Ping realizado a la Vlan de datos

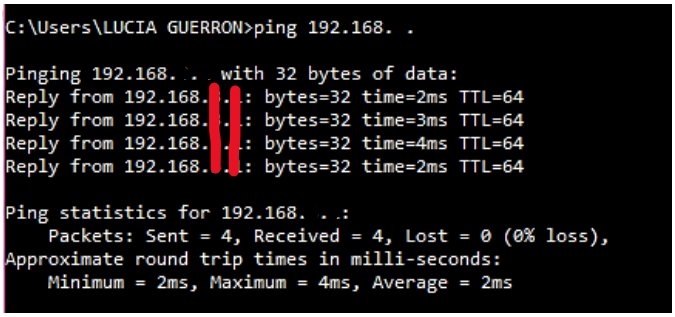


Nota. Autoría propia

- *La Figura 53 muestra la conexión desde una PC hacia la red de telefonía.*

Figura 53.

Ping desde PC a la Vlan de telefonía

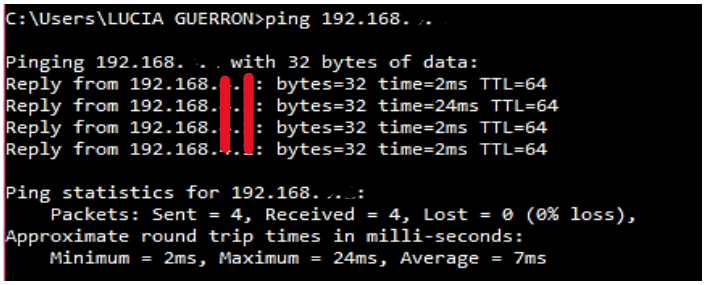


Nota. Autoría propia

- *Ping desde una PC hacia la red Wireless, se visualiza en la Figura 54.*

Figura 54.

Ping desde PC a la Vlan Inalámbrica



Nota. Autoría propia

4.2.2.2.Escaneo de puertos.

Una vez reconocido el rango de direcciones destino a través del reconocimiento pasivo y de los datos proporcionados en el paso anterior el siguiente paso es realizar un escaneo de puerto para encontrar aquellos que se encuentran activos.

Se debe recordar que los puertos pueden estar clasificados de la siguiente manera:

Puertos bien conocidos ➔ Puertos con numeración inferior a 1024.

Puertos registrados ➔ Puertos numerados entre 1024 a 49151.

Puertos privados ➔ Puertos numerados entre 49152 a 65535.

- **Nmap**

Para iniciar el testeo de puertos mediante la herramienta Nmap se debe conocer la sintaxis del comando nmap, el cual tiene la siguiente estructura:

#nmap <Tipos de escaneo> <Opciones >< ip servidor, red>

En la Tabla 36 se muestra los comandos para escanear conexiones tipo UDP Y TCP y verificar puertos abiertos y cerrados.

Tabla 36.

Tipos de escaneo que se puede realizar con Nmap

Tipos de escaneo	Descripción
-sT	Se usa para establecer una conexión TCP con todos los puertos.
-sS	No abre una conexión TCP completa.
-sP	Se usa si solo se necesita conocer que nodos se encuentran activos
-sU	Se usa para saber que puertos UDP están abiertos.

Nota. Adaptado de *(DocShare, 2017)*

También se puede realizar escaneos más específicos para descubrir otro tipo de parámetros como se muestra en la Tabla 37.

Tabla 37.

Opciones generales que se utiliza en los comandos de Nmap

Opciones	Descripción
-PT <# de puerto> 1-1024	Especifica los puertos TCP que se van a escanear
-PU <# de puerto>	Especifica los puertos UCP que se van a escanear
-R	Resuelve DNS de todos los nodos.
-o	Informa sobre el Sistema Operativo
-p-	Todos los puertos
-sV	comprobar las versiones del software que escucha en los puertos
-PO	Realiza ping por protocolo
-Pn	No realiza un ping previo.
-n	Sin resolución de DNS.

Nota. Adaptado de *(DocShare, 2017)*

Para comprobar los puertos habilitados en la VLAN Telefonía IP, primero se empezará con el análisis de los puertos TCP como se muestra en la Figura 55.

Figura 55.

Análisis de puertos TCP en la Vlan de Telefonía

Después se lleva a cabo el análisis de los puertos UDP habilitados en la Vlan de telefonía IP utilizando el comando nmap -sU [dirección del servidor] obteniendo los siguientes resultados en la Figura 56.

Figura 56.

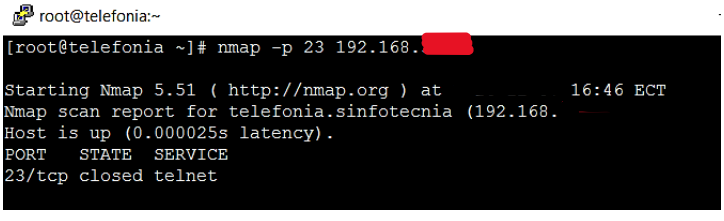
Análisis de puertos TCP en la Vlan de Telefonía

Nota. Autoría propia

El puerto 23 se encuentra inhabilitado, el mapeo de ese puerto se ve en la Figura 57.

Figura 57.

Puerto telnet cerrado en la Vlan de telefonía IP



Nota. Autoría propia

En resumen, se tiene una lista de los puertos TCP que están abiertos y cerrados en la Tabla 38.

Tabla 38.

Enumeración de puertos TCP en el Servidor de VoIP

Puerto	Estado	Servicio
22/TCP	Abierto	SSH
23/TCP	Cerrado	TELNET
25/TCP	Cerrado	SMTP
80/TCP	Abierto	HTTP
143/TCP	Cerrado	IMAP
443/TCP	Abierto	HTTPS
993/TCP	Cerrado	IMAPS
995/TCP	Cerrado	POP3S
3306/TCP	Abierto	MYSQL

Nota. Autoría propia

La Tabla 39 en cambio muestra los Puertos UDP que están abiertos y cerrados después de haber ejecutado la herramienta Nmap en el servidor de Telefonía.

Tabla 39.

Enumeración de puertos UDP en el servidor de VoIP

Puerto	Estado	Servicio
69/UDP	Abierto	TFTP
123/UDP	Abierto	NTP
631/UDP	Abierto	IPP
5060/UDP	Abierto	SIP

Nota. Autoría propia

- **Svmap.**

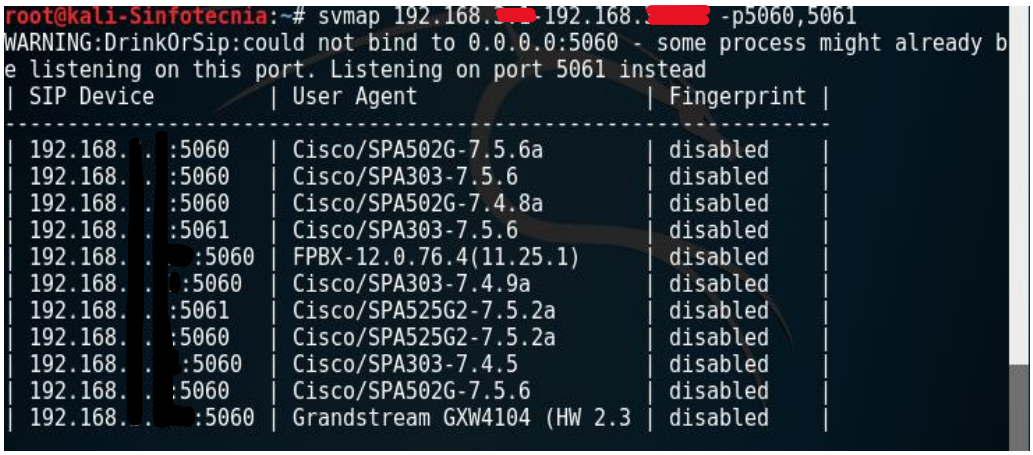
Ahora para conocer si hay dispositivos SIP en la red ejecutamos en el siguiente comando que consta del rango de direcciones y lo puertos 5060 y 5061

```
#Svmap<Rango de direcciones IP>
```

En la Figura 58 al ejecutar la herramienta svmap se aprecia los teléfonos IP disponibles que la mayoría son teléfonos Cisco con su respectiva dirección y puerto 5060, además también se muestra la versión de la plataforma Free PBX e indica que es una versión bastante desactualizada porque actualmente ya se cuenta con la versión 16.

Figura 58.

Enumeración de dispositivos SIP con svmap



Nota. Autoría propia

4.3. TERCERA ETAPA. Modelado de amenazas.

Con esta etapa se procede a identificar la amenaza interna y externa existente en los sistemas de comunicación en este caso específicamente en el sistema de telefonía de VoIP. El modelado de amenazas determinará el método de ataque más efectivo, el tipo de información que busca y cómo podría ser atacada la empresa. Es decir, esta fase implica mirar a una organización como un enemigo y tratar de explotar las debilidades como lo haría un atacante, por lo que se analiza la información de marketing, la competencia en el mercado y un análisis de activos.

4.3.1. Información de productos.

Entre los productos y servicios que ofrece la empresa se encuentra: equipos de Networking, infraestructura TI, Virtualización, cableado estructurado, cámaras de seguridad, soporte técnico entre otras como lo indica la Figura 59.

Figura 59.

Productos y servicios que ofrece la empresa

Nota. Obtenido de https://sinfotecnia.com

4.3.2. Información de marketing

- Datos de empresas competencia en Ibarra.

En la cuidad de Ibarra se ha visto un incremento de las empresas de telecomunicaciones por lo que hay mayor competencia, a continuación en la Tabla 40 se enumeran las más relevantes:

Tabla 40.

Empresa de Telecomunicaciones en Ibarra

Empresa	Descripción	Contacto
INGELCOM	• Desarrollo de soluciones integrales en el campo eléctrico • Comercialización de productos y servicios industriales. • Servicios Integrales de Ingeniería • Instalaciones Industriales Eléctricas. • Sistemas Eléctricos de Distribución.	https://www.ingelcom.com.ec
PLUS	• Servicios de internet por Wireless y fibra óptica con cobertura en la zona norte de la provincia.	https://iplus.com.ec
WORLD COMPUTERS	• Comercialización de equipos y partes tecnológicas. • Mantenimiento técnico y reparación de equipos.	http://worldcomputers.com.ec/
SMART SOLUTIONS	• Servicios de instalación, configuración, y mantenimiento en: videovigilancia • Cableado estructurado • Sistema de alarmas • Control de acceso, domótica	luis_hnando@live.com
I2E	• Diseño, asesoramiento y de obras de ingeniería Eléctrica y Electrónica. • Instalaciones eléctricas. • Redes Telefónicas • Cableado estructurado.	http://www.i2e.com.ec/

Nota. Autoría propia

- *Clientes a los cuales la empresa Sinfotecnia prestó sus servicios*

En la tabla 41 se puede observar que la principal actividad realizada es la instalación de cableado estructurado tanto categoría 6 como 5e a entidades públicas como privadas, destacando especialmente las cooperativas.

Tabla 41.

Clientes de Sinfotecnia

Cliente	Actividades realizadas por la empresa Sinfotecnia	Contacto
COOPERATIVA ATUNTAQUI. LDTA IBARRA	• Sistema de cableado estructurado categoría 6 (certificado).	https://finacoop.atuntaqui.fin.ec/atuntaquiltda/
UNIVERSIDAD CATÓLICA SEDE IBARRA PUCESI.	• Sistema de cableado estructurado categoría 6 (certificado).	http://www.pucesi.edu.ec/web/
MUNICIPIO DE COTACACHI	• Sistema de cableado estructurado categoría 5e. • Enlace inalámbrico punto a punto.	http://www.cotacachi.gob.ec/
EMELNORTE. S. A	• Sistema de cableado estructurado categoría 6 (certificado).	http://www.emelnorte.com/eern/
ECU 911-IBARRA	• Sistema de cableado estructurado categoría 6 (certificado).	http://www.ecu911.gob.ec/
BANCO DEL AUSTRO-IBARRA	• Sistema de cableado estructurado categoría 5e.	https://www.bancodelaustro.com/
COOPERATIVA DE AHORRO Y CREDITO 23 de JULIO-OTAVALO	• Sistema de cableado estructurado categoría 5e.	http://www.coop23dejulio.fin.ec/es/inicio
COLEGIO SANCHEZ Y CIFUENTEZ - IBARRA	• Sistema de cableado estructurado categoría 5e.	http://www.salesianosibarra.edu.ec/
COPERATIVA DE AHORRO Y CREDITO TULCAN. LDTA - TULCAN	• Enlace inalámbrico punto a punto.	https://www.cooptulcan.coop/
HOSTERIA PUEBLO VIEJO - ATUNTAQUI	• Implementación de sistemas de Red.	http://www.hpuebloviejo.com.ec/
EMPRESA PRO-DISPRO - IBARRA	• Sistema de cableado estructurado categoría 5e.	https://www.facebook.com/pages/Prodispro-Parque-Industrial/1655813514636637
UNIVERSIDAD TÉCNICA DEL NORTE	• Instalación Datacenter FICA.	http://www.utn.edu.ec/web/uniportal/

Nota. Autoría propia

4.3.3. Análisis de activos.

- *Activos físicos*

Como se detalló en el capítulo 2, la información técnica fue proporcionada por el administrador de red, el cual además facilito contraseñas de super usuario para poder realizar las pruebas correspondientes en los equipos de interconexión, la Tabla 42 resume la cantidad de dispositivos en la empresa.

Tabla 42.

Activos físicos de la empresa Sinfotecnia

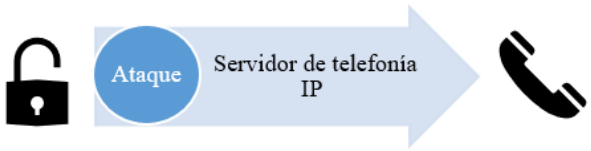
Cantidad	Dispositivos
1	Router
1	Switch Capa 3
3	Switch Capa 2
1	Servidor de telefonía IP
1	Servidor DHCP
1	Wireless LAN Controller
2	Access Point
12	Computadoras de escritorio/Laptop
4	Impresoras
2	Cámaras IP
9	Teléfonos IP

Nota. Autoría propia

Por lo cual en la Figura 60 el activo físico a ser atacado sería el servidor de VoIP

Figura 60.

Objetivo de Ataque



Nota. Autoría propia

- *Activos Humanos.*

Los activos humanos son aquellos que podrían aprovecharse para divulgar información, manipularse para tomar decisiones o acciones que afectarían maliciosamente a la organización. Según (Pentest Standard, 2012): “Los activos humanos indicados en la Figura 61 no son necesariamente los más altos dentro de la jerarquía corporativa, sino que son personal clave que están relacionados con activos de negocios previamente identificados, o están en posiciones para permitir el acceso a dichos activos”.

Figura 61.

Activos Humanos

Nota. Autoría propia

- Datos de empleados.

Los datos de los trabajadores de la empresa se obtuvieron de la red profesional LinkedIn, considerando los más importantes los presentados en la Tabla 43.

Tabla 43.

Contactos de los empleados de Sinfotecnia

Empleado	Cargo	E-mail	Teléfono
Ing. Esteban Vallejos	Gerencia General	gerencia@sinfotecnia.com	[redacted]
Ing. Darwin Hernández	Departamento Técnico	darwinolayo@gmail.com	[redacted]
Ing. Sandra Narváez	Departamento Administrativo-Proyectos	ingenieria@sinfotecnia.com	[redacted]
Ing. Cristian Puga	Departamento Comercial	ventas2@sinfotecnia.com	

Nota. Datos obtenidos de la red LinkedIn.

4.3.4. Agentes de Amenaza

Si se analiza el campo interno se tiene que las personas que trabajan directamente para la empresa bajo un contrato a tiempo parcial o a tiempo completo como se indica en la Tabla 44. En general, no se consideran como una grave amenaza ya que la mayoría de ellos están confiando en la empresa para ganarse la vida y, suponiendo que se tratan bien, están dispuestos a proteger a la empresa en lugar de hacerle daño. A menudo participan en incidentes de pérdida de datos o compromiso accidental.

En casos raros, pueden ser motivados por personas externas para ayudar en las intrusiones o pueden realizar actos maliciosos por su cuenta.

Tabla 44.

Agentes de Amenazas internos y externos

Campo Interno	Campo Externo
Empleados	Compañeros de negocio
Gestión ejecutiva	Competencia
Administradores de red	Contratistas
Desarrolladores	Proveedores
Ingenieros	Cracker
Técnicos	Crimen organizado

Nota. Adaptado de *(Pentest Standard, 2012)*

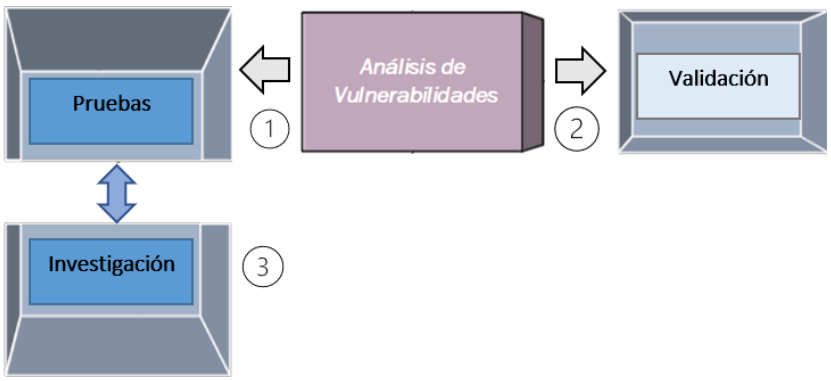
4.4.CUARTA ETAPA. Análisis de vulnerabilidades.

El Análisis de Vulnerabilidad se utiliza para identificar y evaluar los riesgos que presentan las amenazas identificadas en las fases anteriores pues se considera que una "vulnerabilidad de seguridad es una debilidad en un producto que podría permitir a un usuario mal intencionado comprometer la integridad, disponibilidad o confidencialidad de dicho producto" (González, Sanchéz, & José, 2015). De esta manera el proceso de vulnerabilidad se simplifica a dos etapas principales como indica la Figura 62:

- Identificación: La tarea primordial en esta fase es descubrir la vulnerabilidad (pruebas e investigación).
- Validación: Que consiste en reducir el número de vulnerabilidades identificadas a solo aquellas que son realmente válidas.

Figura 62.

Etapas de la fase de Análisis de amenazas



Nota. Adaptado de (González, Sanchéz, & José, 2015)

4.4.1. Pruebas

Las pruebas deben estar adaptadas con el fin de satisfacer los requisitos de profundidad para alcanzar los objetivos porque para realizar un análisis de vulnerabilidad de cualquier tipo, el auditor debe determinar el alcance de la prueba de la profundidad aplicable y amplitud para cumplir los objetivos o requisitos del resultado

deseado. La profundidad de las pruebas siempre debe validarse para garantizar que los resultados de la evaluación cumplan con las expectativas. Los valores de amplitud pueden incluir elementos tales como redes objetivo, segmentos, hosts, aplicaciones, inventarios, etc.

4.4.1.1.Pruebas Activas

Las pruebas activas implican una interacción directa con el componente que se analiza para detectar vulnerabilidades de seguridad. Hay dos formas distintas de interactuar con el objetivo: automatizada o manual.

1. *Automatizada:* Se emplea software especializado en escanear los servicios para de esta manara generar determinadas peticiones y examinar las respuestas que se obtienen.

Usando estas herramientas, uno puede identificar si las redes de VoIP son potenciales para acceder a sistemas de infraestructura central o grabar conversaciones telefónicas en una red objetivo. (Pentest Standard, 2012)

2. *Manual: S*e recomienda ejecutar conexiones manuales directas a cada protocolo o servicio disponible en un sistema para probar ataques previamente no identificados.

En este caso el software escogido para el escaneo de vulnerabilidades es el programa Nessus porque no causa efectos adversos en los sistemas ya que cuenta con la opción por defecto de comprobaciones seguras lo que permite controlar el grado de agresividad del escaneo dependiendo del caso de estudio.

- ***Nessus.***

Configuración de Nessus

Después de haber descargado e instalado Nessus se debe abrir el navegador web e ingresar la dirección IP, o este caso como se instaló en una dependencia de Kali se ingresa la siguiente URL:

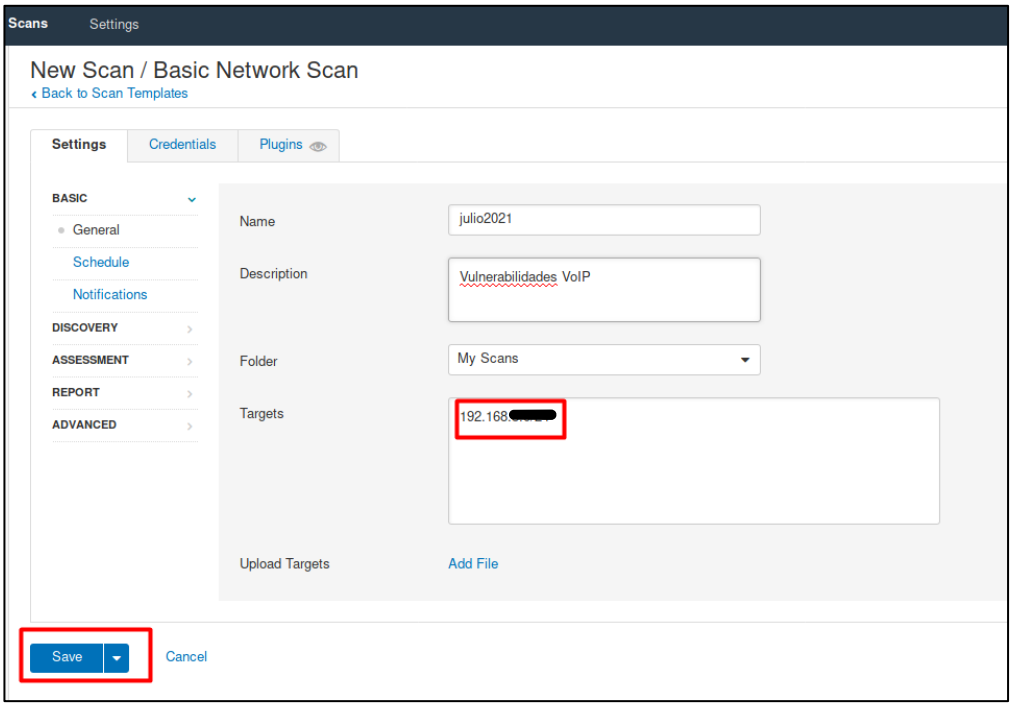
https://kali:8834 /

Iniciar sesión en Nessus utilizando las credenciales que se creó durante la instalación, a continuación, empezar un escaneo básico de la red

Y en el cual se debe ingresar el rango de direcciones que se quiere escanear como se muestra en la Figura 63.

Figura 63.

Configuración de escaneo en Nessus

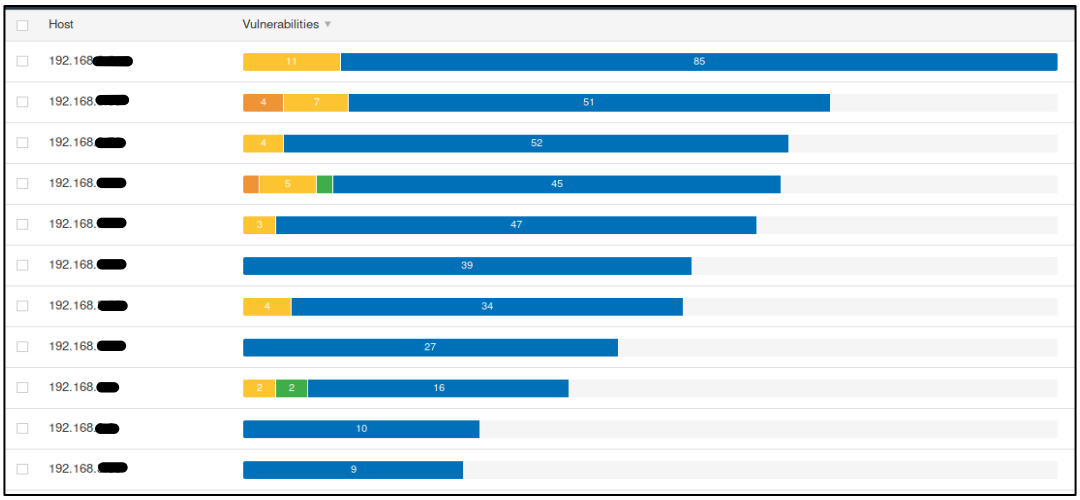


Nota. Captura obtenida del programa Nessus.

Una vez completado el escaneo como se muestra en la Figura 64 aparecerá los hosts con vulnerabilidades encontradas en cada uno de ellos.

Figura 64.

Vulnerabilidades encontradas en la VLAN de Telefonía

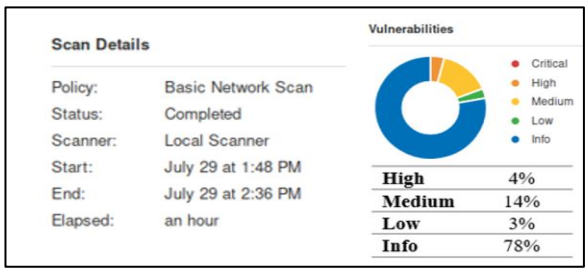


Nota. Captura obtenida del programa Nessus.

A su vez aparece un informe en el cual se clasifica los problemas de acuerdo a su grado de vulnerabilidad, como se observa en la figura 65 no existe ninguna vulnerabilidad con nivel crítico sin embargo si existen debilidades con nivel alto y medio que deben ser investigadas adecuadamente.

Figura 65.

Detalles de escaneo en la red de VoIP

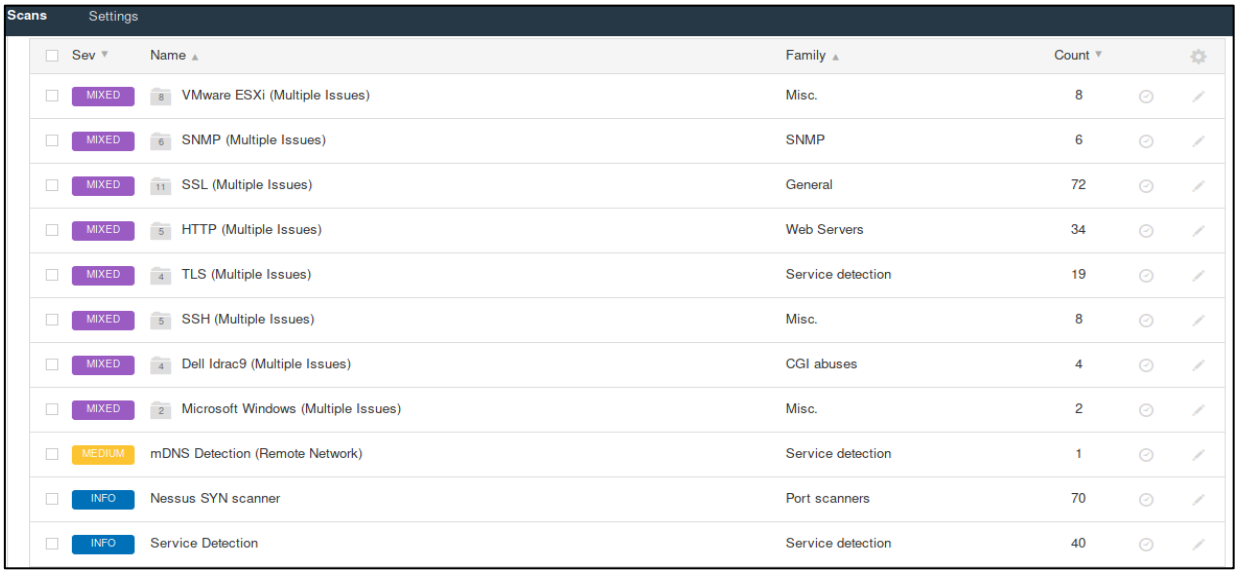


Nota. Captura obtenida del programa Nessus.

A continuación, Nessus genera un reporte con la descripción y solución de las vulnerabilidades encontradas, en la figura 66 se observa el escaneo al servidor de VoIP en el que se distingue el tipo, familia, puerto, referencia del riesgo encontrado.

Figura 66.

Vulnerabilidades encontradas en la VLAN de Telefonía



Nota. Captura obtenida del programa Nessus.

4.4.1.2.Pruebas pasivas

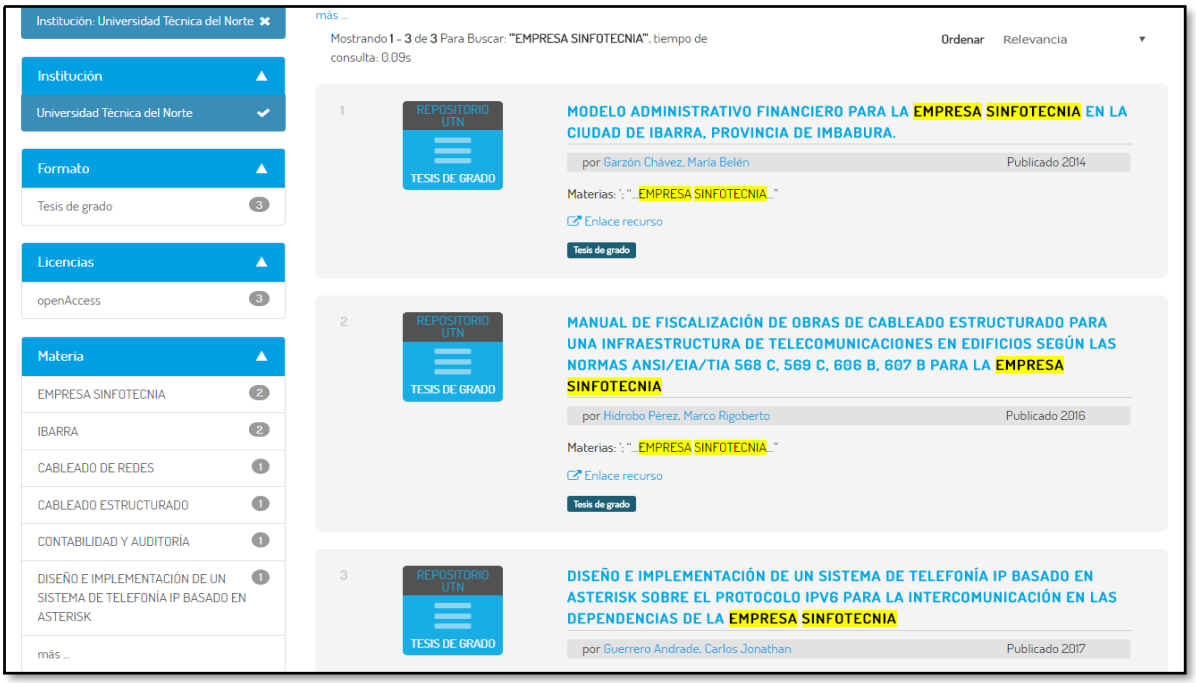
Cualquier metadato al que un atacante pueda acceder de forma pasiva (sin atacar directamente al objetivo) debe considerarse un problema de seguridad, es por esto que estas pruebas están relación con la fase anterior de recogida pasiva de información con la diferencia de que en este apartado no se busca especificar la información sino analizar información confidencial en documentos que puedan suponer una vulnerabilidad. (González, Sanchéz, & José, 2015) (Análisis de tráfico).

Por motivos de confidencialidad se debe evitar mostrar en su totalidad el *direccionamiento IP* de la empresa implicada pues se compromete su disponibilidad al revelar información relevante sobre la misma y en la que cualquier usuario malintencionado podría acceder y comprometer un servicio.

En la figura 67 se observa que las tesis de grado revelan este tipo de información confidencial convirtiéndola así en un posible vector de ataque.

Figura 67.

Proyectos de titulación enfocados en la empresa Sinfotecnia



Nota. Obtenido de la Red de Repositorios RRAAE.

4.4.2. Validación

Los resultados obtenidos deben tener cierta correlación entre ellos y las herramientas que se usaron para analizarlos y dicha correlación puede ser ejecutada de dos maneras distintas:

- Correlación específica: Es aquella que se relaciona con un problema específico, como el ID de vulnerabilidad, CVE, etc.
- Correlación categórica: Es aquella que se relaciona con una estructura categórica para problemas tales como en los marcos de cumplimiento NIST SP, PCI, etc, (Pentest Standard, 2012).

Para fines de este proyecto se utilizará la correlación específica, pues el software Nessus utiliza la información basada en el código CVE (Common Vulnerabities and Exposures) que se le asigna a la vulnerabilidad encontrada en el análisis. Por ejemplo, analizando las vulnerabilidades más peligrosas en el servidor de VoIP se tiene las siguientes en la Tabla 44.

Tabla 44.

Listado de vulnerabilidades en el servidor de VoIP

Vulnerabilidad	**Puerto/ Protocolo**	**Riesgo**	**Puntuación CVSS**	**Familia**	**CVE**
VMware ESXi 6.0 / 6.5 / 6.7 verificación remota	443 / tcp / www	Alto	7.2	Remoto	CVE-2019-5518 CVE-2019-5519
VMware ESXi 5.5 / 6.0 / 6.5 / 6.7 DoS	443 / tcp / www	Medio	4	Aplicación	CVE-2018-6972
Agente SNMP, nombre de comunidad por defecto	161/ udp / snmp	Alto	7.5	SNMP	CVE-1990-0517
Certificado SSL X.509	10000 / tcp / www	Medio	Sin puntaje	General	-
Omisión de autenticación del protocolo SSH	22 / tcp /ssh	Medio	6.4	General	CVE-2018-10933
Detección de protocolo TLS versión 1.0	8009/ tcp	Medio	6.1	Detección de Servicios	-

Nota. Elaboración propia.

Vulnerabilidad 1 ➔ VMware ESXi 6.0 / 6.5 / 6.7 (RIESGO ALTO)

Solución: Para evitar el problema, la controladora USB 1.1 virtual debe quitarse de la máquina virtual, la descripción del problema se visualiza en la Figura 68.

Figura 68.

Vulnerabilidad 1 en el servidor de VoIP.

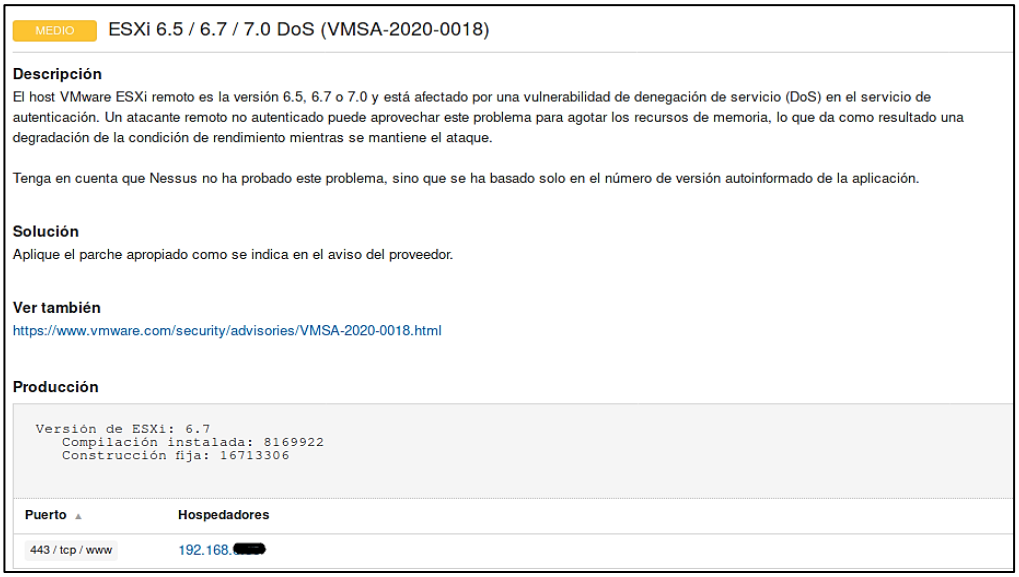
Nota. Captura obtenida del programa Nessus.

Vulnerabilidad 2 ➔ VMware ESXi 5.5 / 6.0 / 6.5 / 6.7 DoS (RIESGO MEDIO)

Solución: Como se muestra en la Figura 69 esta vulnerabilidad es de riesgo medio y necesario aplicar el parche según la versión del VMware para no verse afectado por una vulnerabilidad de denegación de servicio lo que ocasionaría que las máquinas virtuales dejen de responder.

Figura 69.

Vulnerabilidad 2 en el servidor de VoIP



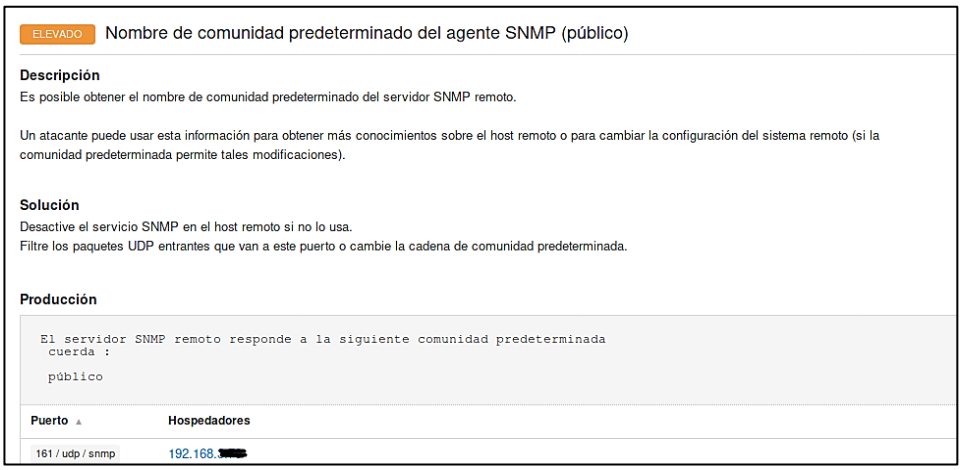
Nota. Captura obtenida del programa Nessus.

Vulnerabilidad ➔ Agente SNMP, nombre de comunidad por defecto (RIESGO ALTO)

Solución: Para contrarrestar esta Vulnerabilidad con riesgo Alto como se muestra en la Figura 70 se debe cambiar el nombre de comunidad configurado por defecto (*public*) por lo que un usuario ajeno al sistema puede obtener gran cantidad de información acerca del mismo utilizando el protocolo SNMP.

Figura 70.

Vulnerabilidad 3 en el servidor de VoIP.



Nota. Captura obtenida del programa Nessus.

Vulnerabilidad 4 ➔ Certificado SSL X.509 (RIESGO MEDIO)

Solución: En la Figura 71 como s sugerencia se debe generar un certificado que cumpla con las condiciones de confianza de un certificado SSL.

Figura 71.

Vulnerabilidad 3 en el servidor de VoIP

Nota. Captura obtenida del programa Nessus.

Vulnerabilidad 5 ➔ Omisión de autenticación del protocolo SSH (RIESGO MEDIO)

Solución: Para esta vulnerabilidad de riesgo medio que se muestra en la Figura 72 se debe actualizar la librería SSH a una versión más estable y reciente.

Figura 72.

Vulnerabilidad 5 en el servidor de VoIP

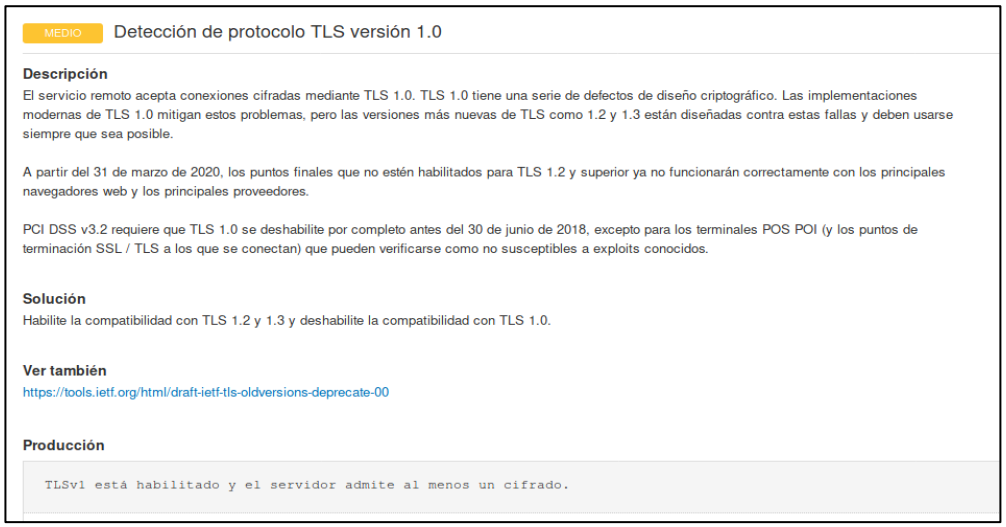
Nota. Captura obtenida del programa Nessus.

Vulnerabilidad 6 ➔ Omisión de autenticación del protocolo SSH (RIESGO MEDIO)

Solución: El riesgo de esta vulnerabilidad es medio como indica la Figura 73 y como sugerencia se tiene que habilitar TLS 1.2 y 1.3 y desactivar el cifrado con la versión 1.0

Figura 73.

Vulnerabilidad 6 en el servidor de VoIP



Nota. Captura obtenida del programa Nessus.

4.4.3. Investigación

- Investigación pública

Se procede a investigar sobre el impacto que causa el problema reportado tiendo en cuenta que las vulnerabilidades poseen base de datos de exploits de disponibilidad pública, guías de fortificación, foros sobre errores de configuración del sistema entre otros (Pentest Standard, 2012).

- Investigación privada

Esta investigación permite simular una réplica de entorno para así de esta manera probar las configuraciones e identificar las posibles vías de acceso que tendría el objetivo en cuestión.

Los escenarios se detallan en el *capítulo 5* en el que se recrean los principales ataques a los cuales está expuesta la red de VoIP, y entre los cuales de detalla las amenazas a nivel de red y de aplicación en la Tabla 45.

Tabla 45.

Vulnerabilidades encontradas en la red de VoIP de Sinfotecnia

Amenazas en la red	**Amenazas en los sistemas**	**Amenazas en las aplicaciones**
Eavesdropping ➔ Interpretación de la comunicación	***DoS ➔ Ataque Denegación de servicios***	***Errores en las configuraciones***
Este ataque en el servidor de VoIP se lo demuestra en la captura de audio de las llamadas a través de la técnica Man in the Middle (MitM).	Flooding en los dispositivos telefónicos, con el envió de paquetes *TCP, SNY/UDP*. Desactualización de los parches de las máquinas de virtualización	La red de VoIP actualmente cuenta con el protocolo *(SIP* sin *TLS)* lo que facilita la captura de paquetes, de los cuales se puede obtener los hash *(MD5),* de las contraseñas.
Firewall Deshabilitado	***Ataques a passwords***	
El firewall de A*stetix* se encuentra deshabilitado, por lo que está propenso a diversos ataques.	La red *VoIP* es vulnerable a un descifrado de contraseñas por usar contraseñas y configuraciones por defecto	---
Puertos innecesarios abiertos El servidor *Asterisk cuenta* puertos abiertos, los cuales son una vulnerabilidad, producida por una instalación por defecto.	----	----

Nota. Elaboración propia

- **Ataque Eavesdropping**

Consiste en espiar las conversaciones o comunicaciones de un objetivo con el objetivo de extraer información sin que éste se entere. Esto se lo intenta interceptando comunicaciones derivadas como videos, audios y todo tipo de escritos que puedan resultar útiles (Jiménez, 2016).

- **Ataque de denegación de servicio.**

Se trata de enviar datos innecesarios y masivos a un servidor para sobrecargarlo y conseguir entorpecer alguna de las propiedades (Jiménez, 2016).

- **Ataque MITM: man in the middle**

Consiste cuando un atacante se interpone entre dos dispositivos conectados en modo promiscuo sin que ninguno de los interlocutores sepa que está ahí, capturando todo el tráfico. El objetivo suele ser extraer información mediante el secuestro de las sesiones (Jiménez, 2016).

4.5. QUINTA ETAPA. Explotación.

La fase de explotación de una prueba de penetración se basa en establecer el acceso a un sistema o recurso evitando las restricciones de seguridad. El objetivo principal es identificar el punto de entrada principal en la organización e identificar activos objetivo de alto valor (Pentest Standard, 2012).

4.5.1. Desarrollo de la etapa 5.

Después de encontrar las vulnerabilidades, se debe tratar de explotar esas vulnerabilidades para violar el sistema y su seguridad.

Para la explotación se utilizan diferentes marcos y software en este caso se usa *Kali Linux el cual pro*porciona una base de datos denominada *exploits-db para* realizar la búsqueda de exploits, de acuerdo a la vulnerabilidad de la aplicación encontrada.

- Exploit: es un pequeño fragmento de código que busca aprovecharse del fallo de configuración, programación, ejecución, etc. para llevar a cabo acciones generalmente maliciosas.
- Payload: es el pequeño fragmento de código contenido dentro del exploit, cuyo objetivo es ejecutarse en la memoria de la máquina de la víctima.

4.5.1.1.Metasploit en VoIP

Para realizar Fingerprinting a través de una red de VoIP se debe ejecutar el siguiente módulo auxiliar el mismo q servirá para encontrar los dispositivos que tiene habilitación SIP:

msf > use auxiliary/scanner/sip/options

msf auxiliary (options) > show options

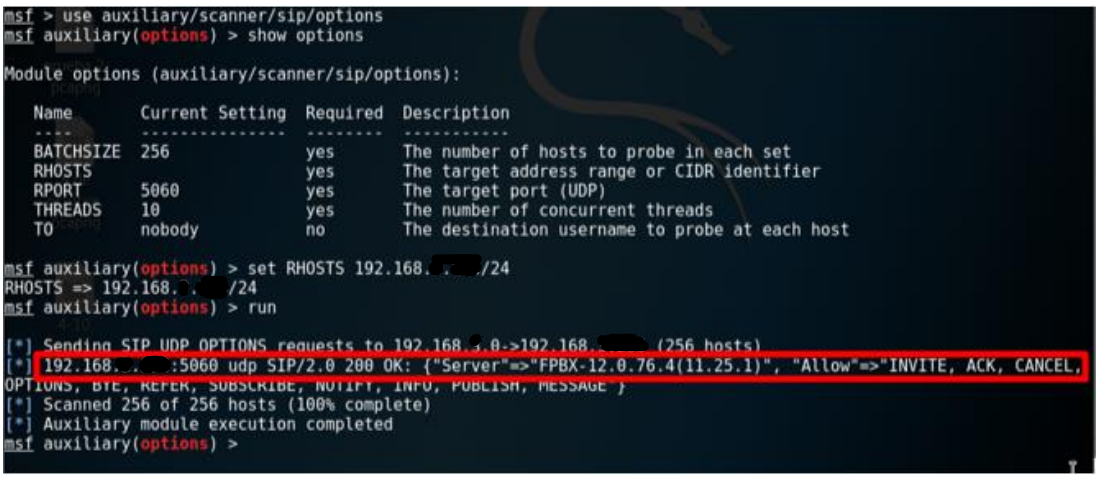
msf auxiliary (options) > set RHOSTS X.X.X.X (rango IP)

msf auxiliary (options) > run

La información proporcionada contiene el nombre y la versión de la PBX y los tipos de solicitud admitidos por la PBX, como se muestra en la Figura 74.

Figura 74.

Escaneo de servicios SIP en la red



Nota. Autoría propia

Para analizar y enumerar a los usuarios de los servicios de VoIP se debe ingresa el siguiente módulo auxiliar:

msf > use auxiliary/scanner/sip/enumerator

msf auxiliary (enumerator) > show options

A continuación, para delimitar la búsqueda de extensiones SIP en la red se debe definir un mínimo (MINEXT) y máximo (MAXEXT) que en este caso estará en un rango de (0 a 200) extensiones puesto a que son los típicos números que usan los administradores para configurar usuarios en el servidor de VoIP.

msf auxiliar (enumerator) > set MINEXT 100

msf auxiliar (enumerator) > set MAXEXT 200

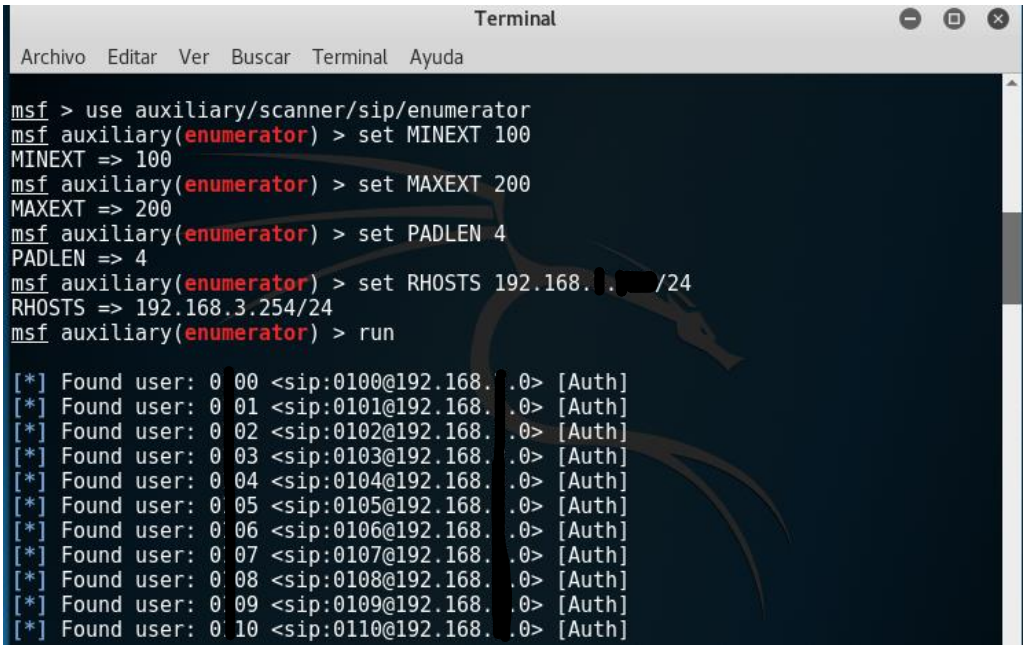
msf auxiliar (enumerator) > set RHOSTS X.X.X.X (rango IP)

msf auxiliar (enumerator) > run

Como se observa en la figura 75 las extensiones configuradas en la central telefónica PBX van desde la 100 a la 110 siendo estas vulnerables a solicitudes de invitación falsa, pues al usar este rango típico de extensiones es fácil de descifrarlas.

Figura 75.

Extensiones SIP habilitadas en la empresa Sinfotecnia.



Nota. Autoría propia

4.6. SEXTA ETAPA. Post-Explotación.

La post-explotación proporciona la información procesada de los sistemas examinados, identifica infraestructura crítica, registra los datos que la compañía valora más y que tiene que asegurar con mayor prioridad. También permite demostrar los ataques que tendrían el mayor impacto comercial.

4.6.1. Integrando Nessus y Metasploit

Tomando en cuenta que en la etapa anterior se utilizó la herramienta Nessus para el análisis de vulnerabilidades se considera aquella que posee un exploit como se observa en la Tabla 46.

Tabla 46.

Vulnerabilidad que tienen exploit

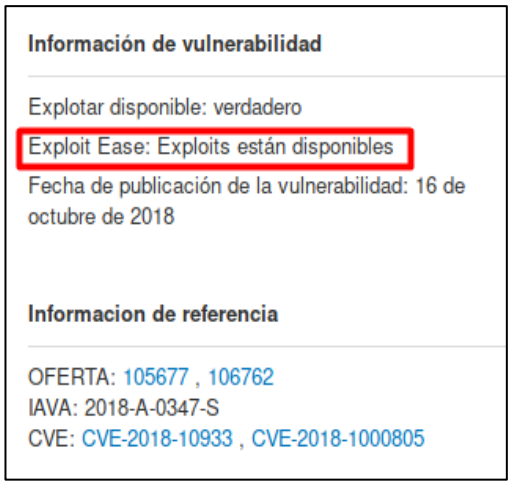
Vulnerabilidad	CVE
Omisión de autenticación del protocolo SSH	CVE-2018-10933

Nota. Autoría propia

Además en el Figura 76 se indica que si posee un exploit disponibles para indagar.

Figura 76.

Referencias de la vulnerabilidad

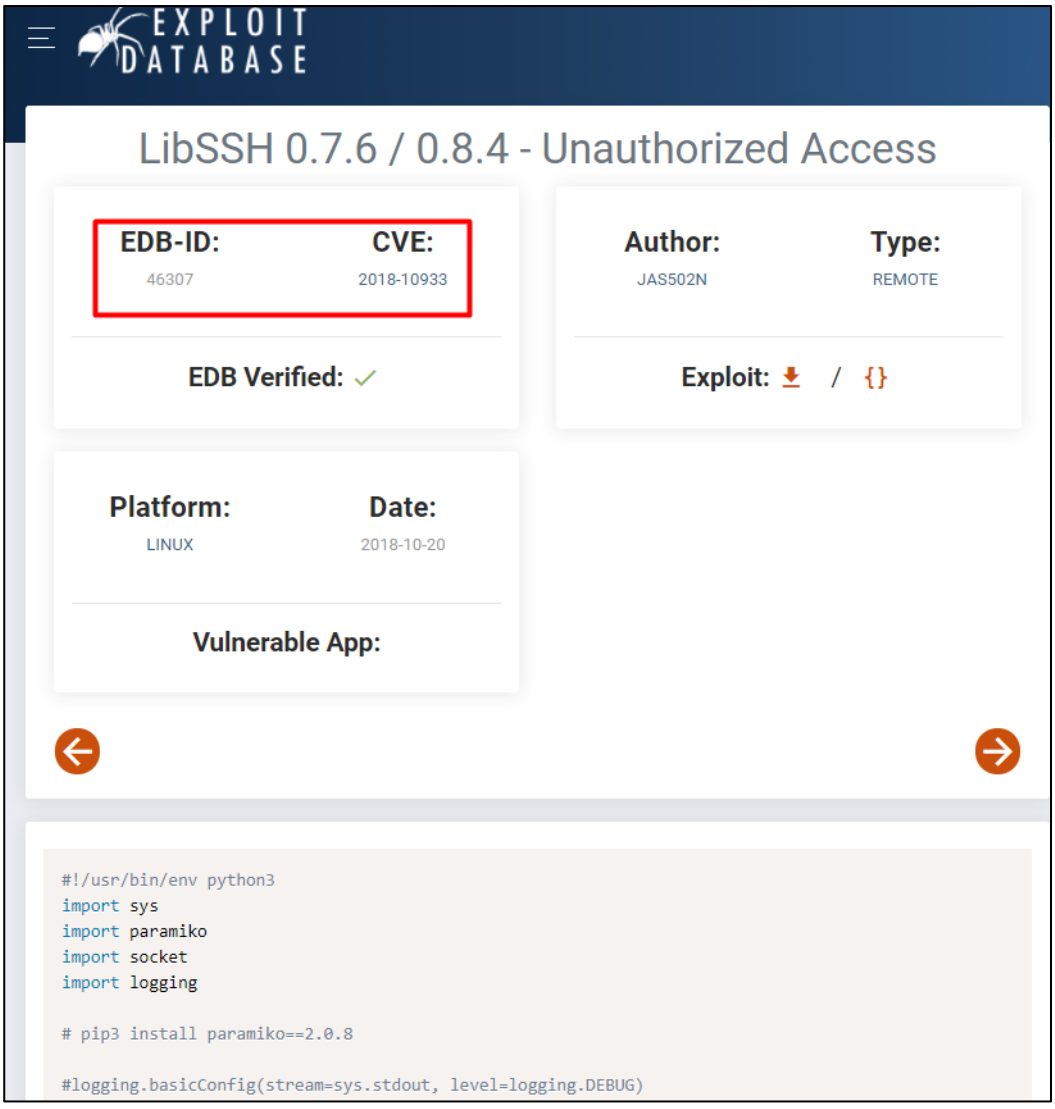


Nota. Captura obtenida del programa Nessus.

El framework Metasploit lleva asociada una base de datos online consultable para buscar el exploit que se considere más significativo, en este apartado se buscó el CVE-2018-10933, en la página web www.exploit-db.com/exploits como se indica en la Figura 77.

Figura 77.

Base de datos de exploit online.



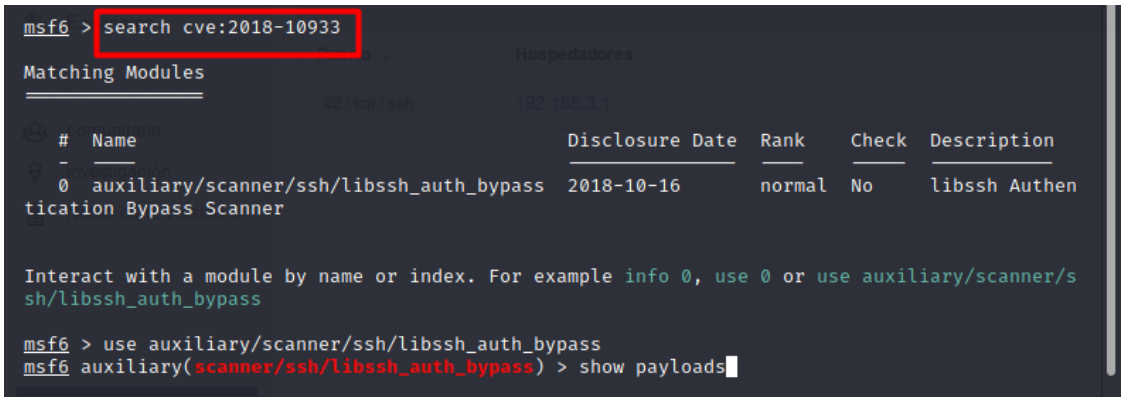
Nota. Obtenido de https://www.exploit-db.com/exploits/46307

Para buscar la vulnerabilidad CVE en Metasploit se debe ingresar el siguiente comando como se indica en la Figura 78.

msf > search cve: (código ID vulnerabilidad)

Figura 78.

Explorando código CVE de la vulnerabilidad



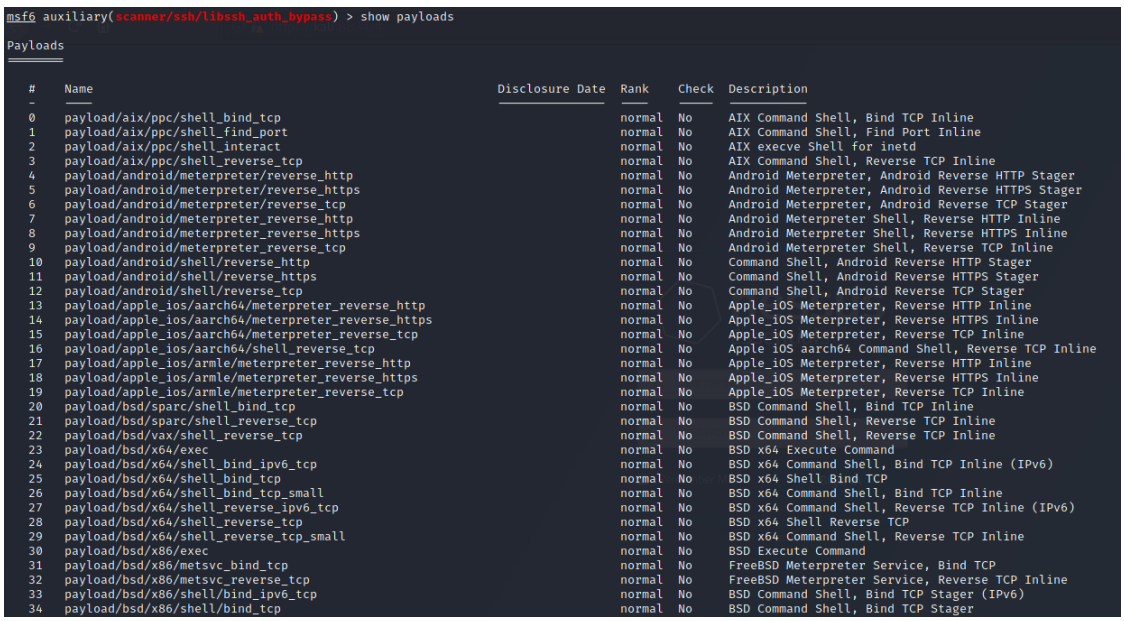
Nota. Autoría propia

A continuación en la Figura 79 se muestra los Payload que tiene esa vulnerabilidad

msf > show payloads

Figura 79.

Payloads de la vulnerabilidad ingresada



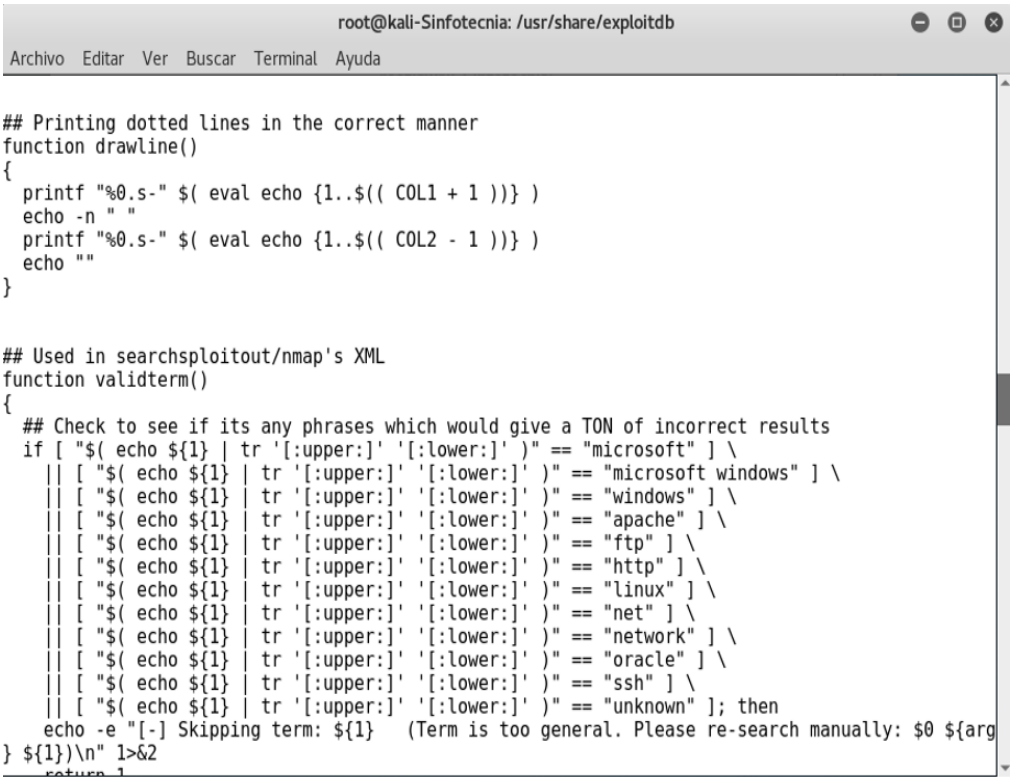
Nota. Autoría propia

De esta manera si algunos de estos paylods funcionan se podría ingresar al Shell en la maquina víctima, pudiendo de esta manera descarga/instalación de un archivo, creación de un usuario, etc. En la Figura 80 se muestra la información de un payload.

msf > set payload (elegir de la lista anterior)

Figura 80.

Acceso a información del payload



Nota. Autoría propia

4.7. SÉPTIMA ETAPA. Informes.

Los informes o reportes son el elemento más importante de una prueba de penetración ya que en ellos se comunica lo que el auditor hizo, cómo lo hizo y cómo la empresa debe arreglar los problemas descubiertos durante la prueba de penetración. La información que se obtiene durante una prueba es vital para el mejorar la seguridad en general y para detener futuros ataques.

Es recomendable dividir el informe en un resumen ejecutivo y en resultados técnicos. Los resultados técnicos serán utilizados por el cliente para remediar las brechas de seguridad de su organización que es el objetivo principal de esta prueba de penetración (Pentest Standard, 2012).

4.7.1. Resumen Ejecutivo.

- **Antecedentes**

En vista de que la empresa SINFOTECNIA tenía la necesidad de mejorar la seguridad de sus comunicaciones entre sus distintas oficinas y sucursales de manera que se pueda minimizar los ataques e infiltraciones que se registraron en los últimos meses la alternativa planteada que permitió analizar e identificar las posibles amenazas existentes en el servicio de telefonía IP de la empresa, fue el desarrollo de un modelo de seguridad basado en la metodología PTES para de esta manera aplicar las fases de ejecución de una prueba de penetración y adoptar medidas preventivas en la red de telefonía IP.

4.7.1.1.Hallazgos en la red de VoIP.

Después de aplicar las etapas de la prueba de penetración se obtiene que los ataques a los cuales está expuesto la central de VoIP en la empresa Sinfotecnia se exponen en la Tabla 47, con el indicador de su respectivo riesgo.

Tabla 47.

Perfil de Riesgo en los ataques de VoIP

Ataque VoIP	Ataque a la empresa	Probabilidad/escala	Riesgo
Eavesdropping	SI	8-9	Elevado
Complementos de la Central PBX desactivados	SI	7-9	Elevado
(DoS) por inundación	SI	7-9	Elevado
Cracking de contraseñas	NO	7-9	Elevado
Captura de tráfico	SI	8-9	Elevado
Puertos innecesarios abiertos.	SI	8-9	Elevado
Firewall deshabilitado	SI	10-12	Alto

Nota. Autoría propia

Los riesgos que predominan, en los activos de comunicación son: ***(firewall desactivado, descifrado de contraseñas, denegación de servicios e interpretación de la comunicación)***, se los definió como elevados, porque todo el personal que se encuentra laborando en la empresa, realiza intercomunicaciones con el fin de agilizar sus tareas, un ejemplo de ello es la funcionalidad de la central telefónica, por ser el medio de transmisión de mensajes al gerente, administrativo, técnico, entre otros.

4.7.2.1 Soluciones a las amenazas en la red de VoIP.

En la Tabla 48 se muestra las principales soluciones que se puede dar a las vulnerabilidades encontradas con estado elevado.

Tabla 48.

Soluciones a las vulnerabilidades de VoIP

SOLUCIONES A LAS POSIBLES AMENAZAS EN LA RED DE VOIP		
Eavesdropping **➔ Interpretación de la comunicación**	***DoS*** **➔ Ataque Denegación de servicios**	**Errores en las configuraciones**
La solución para esta amenaza es implementar protocolos de seguridad TLS ya que la información se transmite por canales cifrados de comunicación**.**	Configurar la herramienta *FAIL2BAN* misma que actúa penalizando o bloqueando las conexiones remotas que intentan accesos por fuerza bruta	La solución a esta vulnerabilidad se contrarresta con la implementación de protocolos de seguridad ya que actualmente los paquetes no cuentan con seguridad alguna

Firewall Deshabilitado	Ataques a passwords	Puertos innecesarios abiertos
En Webmin es posible configurar el módulo de seguridad que incluye la central PBX o en su caso configurar reglas de IPTABLES.	Usar contraseñas fuertes con mayúsculas, minúsculas, caracteres especiales evitando así las típicas contraseñas por defecto.	En este caso es recomendable cerrar los puertos innecesarios

Nota. Autoría propia

A continuación en la Tabla 49 en cambio se muestra las soluciones de las vulnerabilidades encontradas en la herramienta de Nessus.

Tabla 49.

Soluciones a las vulnerabilidades encontradas en Nessus

VULNERABILIDAD	SOLUCION
VMware ESXi y VMware DOS	Aplicar el parche según la versión del VMware para prevenir una vulnerabilidad de control remoro o de denegación de servicio en las máquinas virtuales.
Agente SNMP, configurado con comunidad predeterminada	Cambiar el nombre de comunidad configurado por defecto (*public*)
Omisión por autentificación SSH	Actualizar la librería SSH a una versión más estable y reciente
Certificado SSL X.509	Se debe generar un certificado con todos los parámetros adecuados de un certificado SSL.
Detección de protocolo TLS versión 1.0	Se debe deshabilitar la versión 1 de protocolo TLS y activar las versiones 2 y 3.

Nota. Autoría propia

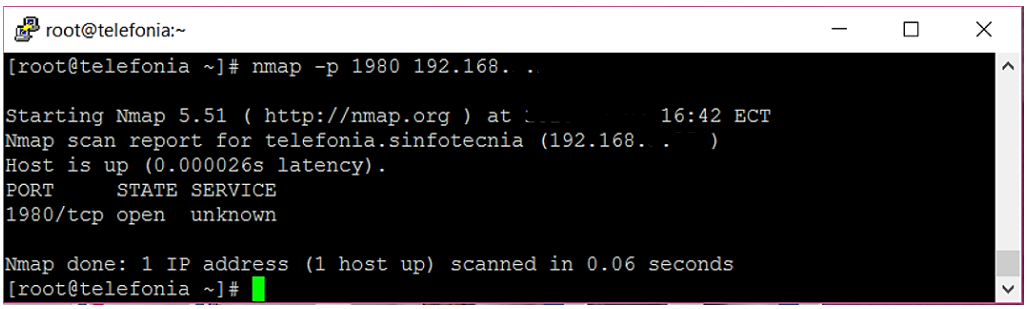
- **Cambiar el puerto por defecto SSH**

En vista de que hay formas muy conocidas para realizar accesos remotos como es el puerto 22 el cual trabaja *SSH*, se debe realizar ciertas modificaciones con el fin de dificultar la tarea de las personas que rastrean los servicios de *VoIP*, debido a ello se debe cambiar el acceso del puerto por defecto, con lo que evitaríamos exploits. Para ello se debe modificar el archivo: /etc/ssh/sshd_config

En la Figura 81 se observa que se puede reemplazar el puerto *22*➔ por el puerto *1980;* donde *(1980)* puede ser otro cualquier otro número de puerto disponible

Figura 81.

SSH funcionando en el puerto 1980



Nota. Autoría propia

En la interfaz Webmin como se aprecia en la Figura 82 se puede además visualizar el estado de los servidores que se encuentran activados en el Sistema:

Figura 82.

Servidores de la Empresa Sinfotecnia

Nota. Captura obtenida de Webmin

- **Configuración de Fail2ban**

Fail2ban es una herramienta que observa los intentos de login de variados servicios, tales como SSH, FTP, SMTP, HTTP, entre otros; y si encuentra intentos de login fallidos una y otra vez desde una misma IP, fail2ban rechazará estos intentos de login bloqueando con reglas de iptables a esas IPs que estaban intentando. En la Figura 83 se muestra el fichero de configuración de Fail2ban que se instala como complemento en una central Free PBX.

El archivo /etc/fail2ban/jail.local es un archivo como referencia válida funcionalmente para que el archivo de log que fail2ban revise los intentos de login.

Figura 83.

Configuración del fichero fail2ban

Nota. Captura obtenida de consola FreePBX

Para seguridad del complemento de fail2ban es necesario revisar el status de las reglas iptables del servicio de Asterisk como se muestra en la Figura 84, en esta listado aparecerán las IP que se encuentren baneadas por detección de intrusos y fallos reintentados de autentificación.

Figura 84.

Reglas Iptables para Fail2ban

Nota. Captura obtenida de la consola FreePBX

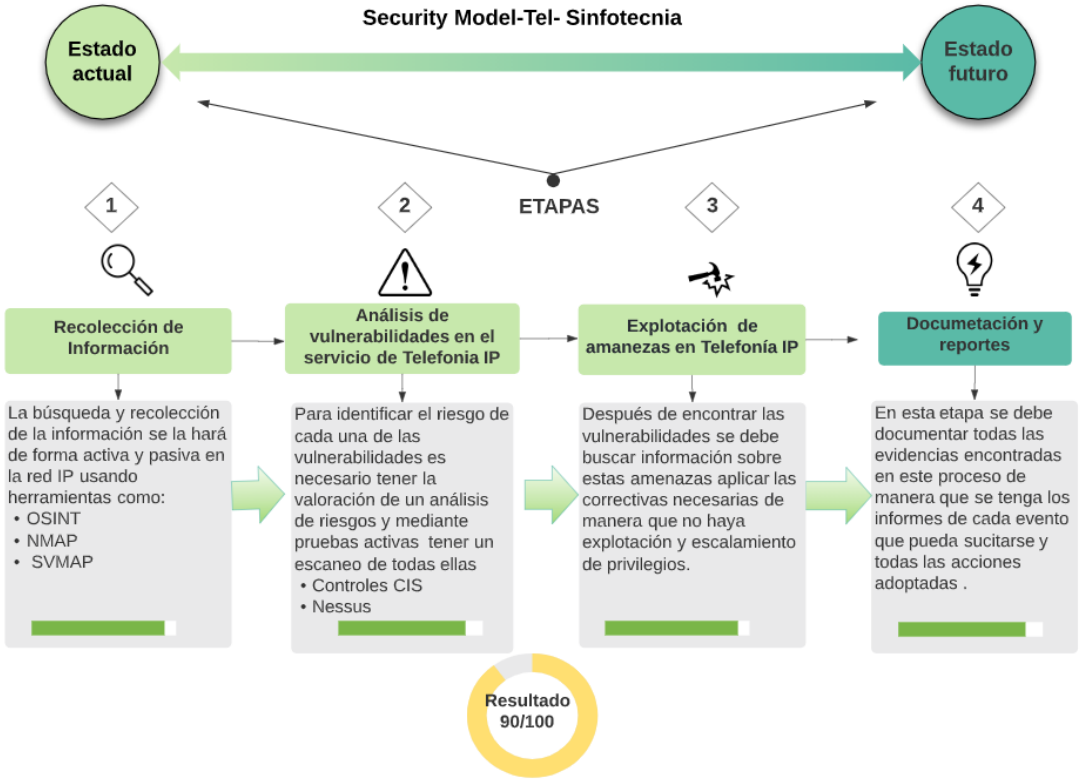
4.8. Propuesta de Modelo de Seguridad orientado a la Telefonía IP.

Esta propuesta se define luego de haber realizado las 7 etapas de la metodología PTES, en la cual se incluyeron técnicas de escaneo, reconocimiento activo y pasivo en la red de Telefonía IP, para plantear este modelo se simplificó y unificó las fases en 4 que se consideran elementales a hora de recuperar o mejorar el servicio, de tal forma que se eviten o minimicen futuros ataques a los activos de la empresa en cuestión.

En la Figura 85 se muestra proceso de las fases que se contempla en esta propuesta.

Figura 85.

Modelo de Seguridad Propuesto para Telefonía IP



Nota. Autoría propia.

4.8.1. Descripción de las etapas de la propuesta de este modelo.

El modelo denominado Security Model- Tel propone 4 etapas para que la detección, el impacto y la acción que el administrador debe realizar al momento de verificar la robustez y las medidas de seguridad en el servicio de VoIP, si este proceso se lleva en orden de manera adecuada y continua se puede tener un resultado de efectividad del 90% o más, puesto a que se debe tomar en cuenta los 3 parámetros en el marco de la seguridad de la información, como se describe en la Tabla 50.

Tabla 50.

Parámetros de Seguridad en la Telefonía

Activo	Parámetro	Descripción
Servicio de VoIP	Confidencialidad	Proteger el servicio de VoIP para que no sea afectado.
	Integridad	Minimizar los fallos en el uso del servicio telefónico.
	Disponibilidad	Asegurar que el servicio de VoIP esté disponible el mayor tiempo posible.

Nota. Elaboración propia.

Cada etapa establecida tendrá una valoración del 25% es decir al completarse las 4 etapas tendrá una puntuación de 90 a 100% según la ejecución y el procedimiento que se lleve en cada una de ellas.

A continuación se describe las 4 etapas del Security Model- Tel que consiste en:

Etapa 1. Recolección de Información.

Para obtener la información adecuada y útil de la empresa se recurre técnicas:

- Reconocimiento pasivo como el sniffing utilizando herramientas como wireshark, ettercap y sitios que muestren información de servidores como Netcraft, los cuales ayudarían a visualizar las direcciones y activos que puedan estar expuestos de manera externa en internet.

- Reconocimiento activo usando técnicas de escaneo de puertos con la herramienta NMAP para mostrar los puertos TCP y UDP abiertos innecesariamente, en la Tabla 51 se muestra el formato sugerido para documentar este proceso.

Tabla 51.

Listado de Puertos en etapa de reconocimiento Activo

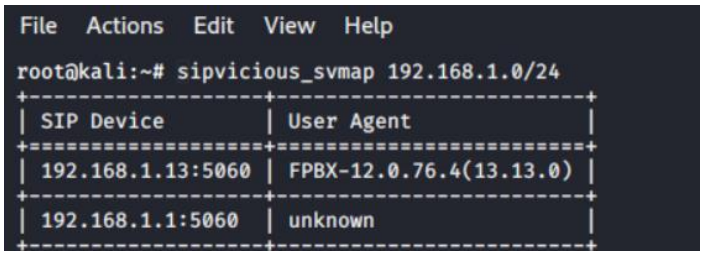
Sinfotecnia Evolución Tecnológica	**Fecha/Hora:** **Responsable:** **Procedimiento:**	**Reconocimiento activo/Listado de puertos.**	
Tipo de Puerto	# Puerto	Estado Actual	Estado Final
TCP	- - - -		
UDP	- - - -		

Nota. Elaboración propia.

Además es necesario tomar en cuenta las versiones de Sistemas operativos que se encuentre instalados en este caso la versión del Centos es una versión 6.8 como primer paso se debe actualizar a una versión 8. A su vez con la herramienta SVMAP se puede ver el tipo de central IP que se está usando, como se observa en la Figura 86 en una primera instancia la versión de Free PBX se encuentra con una versión muy desactualizada por lo que el segundo paso sería actualizarla a la versión 15.

Figura 86.

Reconocimiento de la versión de Free PBX con SVMAP

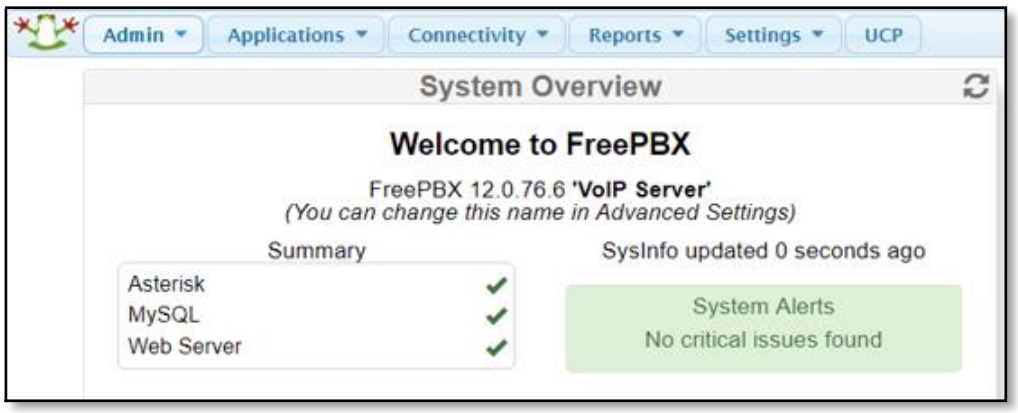


Nota. Autoría propia.

En la Figura 87 la versión actual no tiene instalado el complemento Fail2ban por lo que en la versión actualizada si se considerar la instalación de este complemento (ver Figura 88) que ayuda a evitar acceso no autorizado u autenticados en el servidor de Telefonía.

Figura 87.

Versión desactualizada de la Central FreePBX



Nota. Obtenido de la empresa Sinfotecnia

Figura 88.

Versión actualizada de la Central FreePBX

Nota. Elaboración propia.

Etapa 2. Análisis de Vulnerabilidades en el servicio de Telefonía IP.

En esta etapa se identifican las debilidades y las consecuencias después de realizar un análisis de riesgos, se puede basar en los controles CIS para establecer las salvaguardas que están ejecutadas y algunas que falten definirse en la empresa, entre los Riesgos y ataques que se pueden presentar en el servicio de Telefonía IP se encontraron los detallados en la Tabla 52.

Tabla 52.

Matriz de Riesgos de Seguridad en la Telefonía IP.

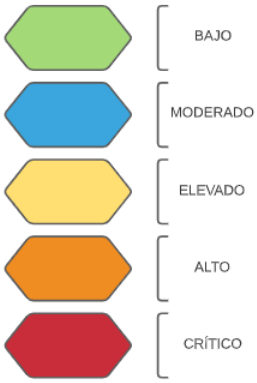
Código	Riesgo	Consecuencias	Impacto
R.1	Puertos innecesarios abiertos	Obtener acceso no autorizado a datos confidenciales	Elevado
R.2	Cracking de contraseñas	Obtener acceso como root por no tener contraseñas robustas.	Elevado
R.3	Eavesdropping	Acceso no autorizado y captura de streams.	Elevado
R.4	Captura de tráfico	Acceso no autorizado y rastreo de logs y paquetes.	Moderado
R.5	DoS por inundación	Indisponibilidad del servicio de Telefonía IP	Elevado
R.6	Falta de actualizaciones en servicios (Central PBX) y parches de seguridad	Obtención de información, acceso a otros servicios o base de datos.	Elevado
R.7	Falta de sistema de seguridad IDS/IPS/SBC	Acceso y control del acceso a la red por falta de monitorización del tráfico entrante	Alto

Nota. Elaboración propia.

Conociendo los tipos de vulnerabilidades a las que puede estar expuesta la red de Telefonía IP, se establece la siguiente escala de colores en la Figura 89 considerando cuatro tipos de impacto, que pueden suceder en un proceso de análisis, verificación y validación.

Figura 89.

Escala de impacto de vulnerabilidades

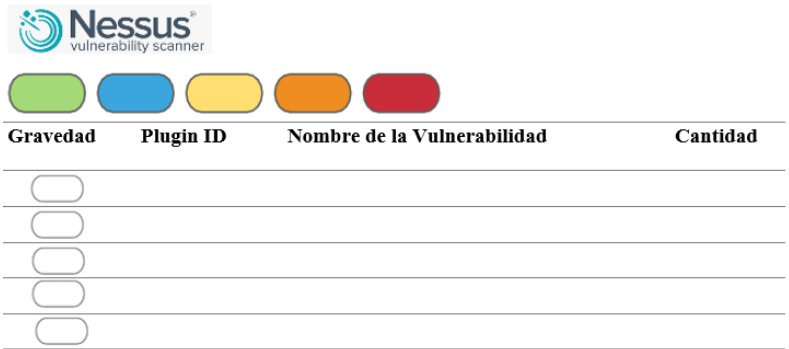


Nota. Elaboración propia.

En esta etapa también es recomendable utilizar la herramienta de Nessus para obtener los reportes de las vulnerabilidades encontradas en el análisis y sus posibles soluciones pues ahí indica el grado de severidad y el código de plugin ID, el código CVE con el que se puede investigar más información para contrarrestar estas debilidades las mismas que deben ser actualizadas, parchadas y mitigadas dependiendo de sus gravedad y así anticiparse a posibles ataques que puedan suceder posteriormente, en la Figura 90 se muestra el formato que tiene el reporte de Nessus y los cuales deben archivarse para tener un historial de fallas corregidas y no corregidas.

Figura 90.

Formato de reporte de vulnerabilidades de Nessus



Nota. Adaptado de Herramienta Nessus

En la Tabla 53 se muestra el formato de un Reporte de Fallos y Vulnerabilidades, en el que debe constar el tipo de Riesgo (R1-R7) según la Matriz de Riesgos descrita anteriormente, el tipo de Vulnerabilidad con el ID del plugin o CVE encontrado en Nessus, el Nivel de impacto y las medidas que se instalaron con fecha.

Tabla 53.

Formato de Reporte de Vulnerabilidades

<table>
<tr><td rowspan="2">  </td><td colspan="5">EMPRESA SINFOTECNIA</td></tr>
<tr><td colspan="5">Formato de Reportes de Riesgos y Vulnerabilidades</td></tr>
<tr><td>Número de Reporte</td><td colspan="2"></td><td>Responsable</td><td colspan="2"></td></tr>
<tr><td>Fecha de revisión</td><td colspan="2"></td><td>Fecha de Solución</td><td colspan="2"></td></tr>
<tr><td>Tipo de Riesgo (R1-R7)</td><td colspan="2"></td><td>Tipo de Vulnerabilidad ID (CVE)</td><td colspan="2"></td></tr>
<tr><td rowspan="2">Gravedad</td><td>Bajo</td><td>Moderado</td><td>Elevado</td><td>Alto</td><td>Crítico</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Problema o incidente</td><td colspan="5"></td></tr>
<tr><td>Detalle de procedimientos efectuados</td><td colspan="5"></td></tr>
<tr><td>Detalle procedimientos pendientes</td><td colspan="5"></td></tr>
<tr><td colspan="6">OBSERVACIONES

Entregado por: …….. Recibido por: ……..
Firma Firma</td></tr>
</table>

Nota. Elaboración propia

Etapa 3. Explotación de amenazas en Telefonía IP

Esta etapa se basa en buscar los indicios para que no se presente acceso a un sistema o recurso por parte de terceros es decir basado en los exploit o en la falta de parches que pudieron aparecer en las vulnerabilidades de la etapa anterior se debe examinar la seguridad de la red de Telefonía IP y considerar las siguientes alarmas que pueden surgir en el servicio.

- ✓ El servicio de Telefonía presenta algún retardo o existió indisponibilidad de la red por algún momento.
- ✓ Sobrecarga de operación en la central, se observa una gran cantidad de peticiones lo que evidenciaría un riesgo por ataque de Denegación de Servicio DoS por inundación.

Para tratar de supervisar el tráfico entrante es necesario que exista una inspección de y monitoreo de logs mediante Fail2Ban. A continuación en la Tabla 54 se muestra el tratamiento que debe darse a los riesgos definidos en la Etapa 2.

Tabla 54.

Matriz de mitigación de Riesgos en la Telefonía IP.

Código	Riesgo	Mitigación	Frecuencia de revisión
R.1	Puertos innecesarios abiertos	Cerrar los puertos que no se utilicen.	Semanal
R.2	Cracking de contraseñas	Establecer contraseña con al menos 8 dígitos, donde se combinen mayúsculas, minúsculas, números y caracteres especiales en las cuentas de administración. Las extensiones deben tener una contraseña individual para que no se repita en las extensiones de los otros departamentos.	

R.3	Eavesdropping	Revisar las reglas en el Firewall, monitoreo del tráfico de paquetes.	Semanal
R.4	Captura de tráfico	Revisar el listado de usuarios autenticados con sus respectivas direcciones y puertos.	Semanal
R.5	DoS por inundación	Identificar el origen del ataque DoS, restaurar los archivos de configuración del Servidor. Implementación de herramientas de monitoreo y alertas de logs.	Diario
R.6	Falta de actualizaciones en servicios (Central PBX) y parches de seguridad	Actualizar los servicios y paquetes a sus versiones más recientes.	Mensual
R.7	Falta de sistema de seguridad IDS/IPS/SBC	Implementar un equipo de borde y herramientas de monitoreo.	Diario

Nota. Elaboración propia

Etapa 4. Documentación y Reportes

La etapa final debe recabar todas las evidencias recolectadas durante las etapas anteriores de búsquedas y análisis de vulnerabilidades, cabe mencionar que ninguna empresa está exenta de una ataque o delito informático, pero al validar las políticas de configuración, y al realizar este tipo de pruebas de hacking ético la gravedad se minimiza, obteniendo alertas de prevención. Las premisas que contiene el informe técnico es el siguiente:

- ✓ Antecedentes
- ✓ Hallazgos en el servicio de Telefonía IP
- ✓ Listado de Puertos en etapa de reconocimiento
- ✓ Evaluación de Riesgos de Seguridad en la Telefonía IP.

- ✓ Formato de Reporte de Vulnerabilidades
- ✓ Reporte de Nessus
- ✓ Clasificación según el tipo de gravedad
- ✓ Matriz de soluciones a las amenazas en la red de VoIP
- ✓ Políticas de seguridad.

Este último ítem relacionado al procedimiento de las políticas de Seguridad se detalla en el Capítulo 5 cuyo formato consta de los siguientes campos como se muestra en la Tabla 55.

Tabla 55.

Formato de las políticas de Seguridad.

Empresa de Soluciones Integrales **SINFOTECNIA**		*Pág*: *Nro. Revisión:* 1
	Políticas de Seguridad de la información	Sinfotecnia Evolución Tecnológica

Dominio	Gestión de Seguridad	**Destinatario**
Control		Administrador de Red
Descripción		
1.		

Dominio	Gestión de Seguridad	**Destinatario**
Control		Administrador de Red
Descripción		
2.		

5. CAPITULO V. Pruebas de Simulación

5.1. Escenarios de Pruebas

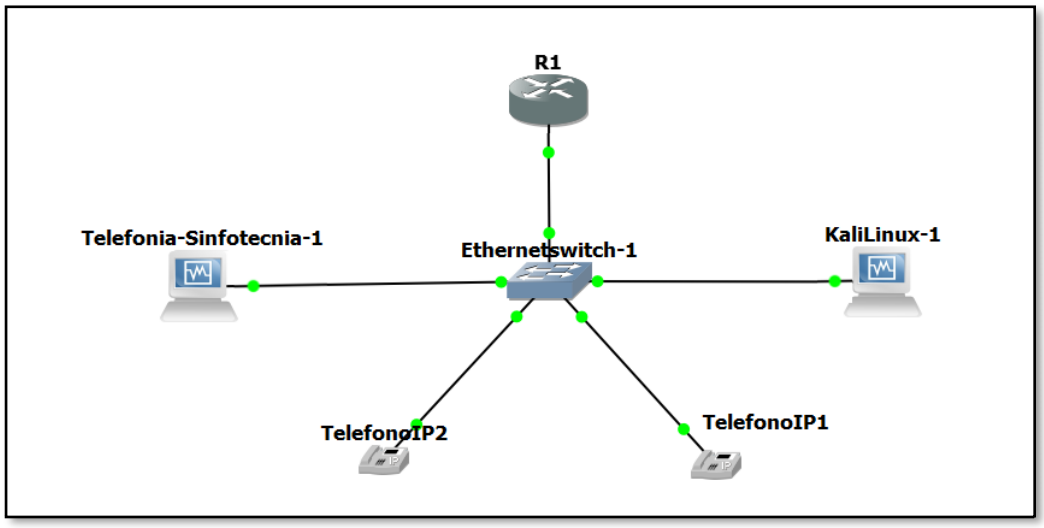
Para no interrumpir el servicio de las telecomunicaciones (VoIP) en la empresa Sinfotecnia, ya que la configuración es de prueba/error por ciertas descargas y actualizaciones de librerías y script se realizó los ataques en un escenario de pruebas, simulando un área de trabajo como se muestra en la Figura 91, en caso de que alguna configuración no funcionara de acuerdo con lo esperado.

El escenario se configura con los siguientes elementos:

- ✓ Servidor Asterisk con la misma versión PBX del servidor (VoIP)
- ✓ Una computadora acceso al servidor (atacante Kali Linux)
- ✓ 2 Softphones

Figura 91.

Escenario de VoIP en el realiza el pentesting



Nota. Autoría propia

5.1.1. Espionaje en una llamada de VoIP.

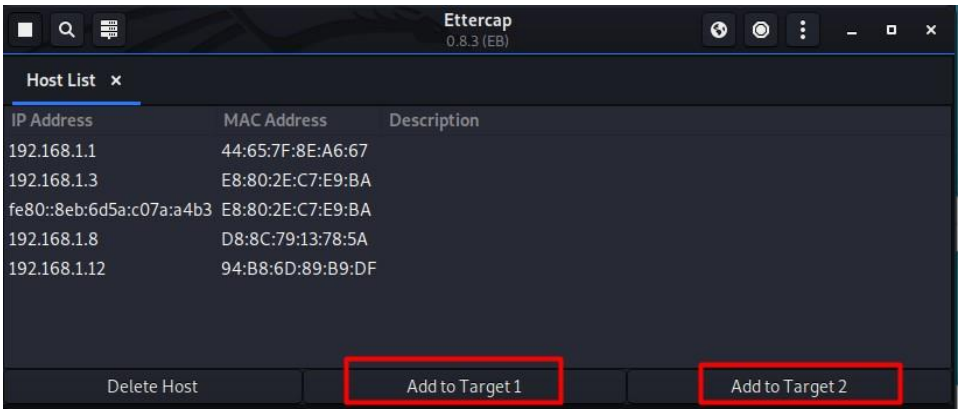
El espionaje de una llamada consiste en interceptar la comunicación entre 2 usuarios para obtener información, decodificarla a través de un sniffer y extraer el audio de lo que hablaron sin que las partes involucradas se enteren de esta acción.

Para llevar a cabo este ataque conocido como MitM se necesita de la aplicación Ettercap, en el cual el atacante se posiciona de manera intermedia envenenando las tables ARP (ARP Poisoning) con mensajes ARP falsos y así se logra asociar la dirección MAC del atacante con la IP del servidor o la dirección de un teléfono IP, para luego a través de Wireshark tener control del tráfico que pasa a través de él.

En esta simulación, se realiza un escaneo de la red a la cual tiene acceso para detectar los dos dispositivos o la puerta de enlace entre ellas. Como se observa en la figura 92 en la lista de Host se selecciona la dirección de un terminal que tiene instalado un Zoiper y la dirección de la puerta de enlace.

Figura 92.

Lista de host descubiertos en Ettercap



Nota. Autoría propia

192.168.1.12 ➔ Add Target 1

192.168.1.1 ➔ Add Target 2

Como se observa en la Figura 93 ya se tiene añadidos las direcciones tanto a la Target 1 como a la Target 2.

Figura 93.

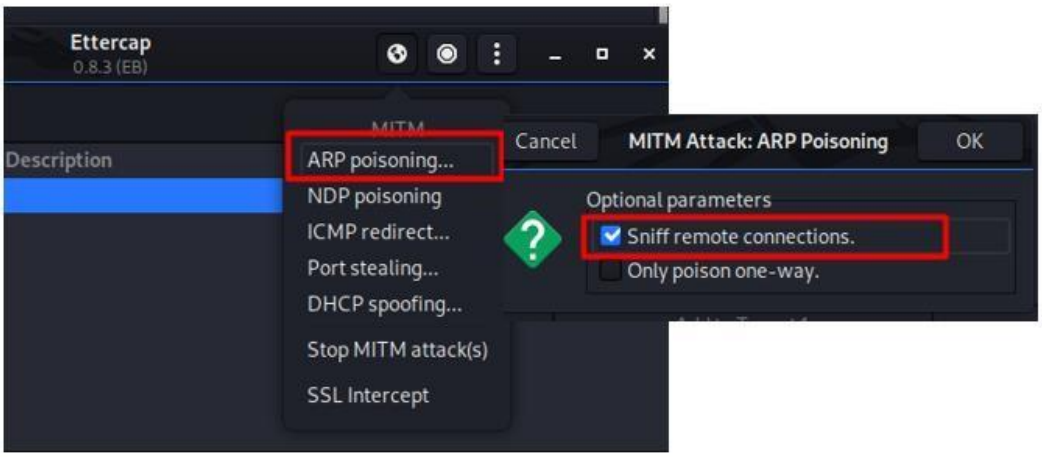
Añadiendo las direcciones de Target 1 y Target 2 en Ettercap

Nota. Autoría propia

Una vez agregados los hosts a las tarjetas en la opción MitM se escoge la opción ARP poisoning como muestra la Figura 94 y se checkea que haga un sniff de las conexiones remotas

Figura 94.

Escogiendo la opción ARP poisoning



Nota. Autoría propia

Una vez realizado esto se puede observar en la Figura 95 el siguiente mensaje con las victimas asignadas y para llevar a cabo su objetivo de espiar tendrá que esperar que se realice una llamada desde las partes involucradas.

Figura 95.

Victimas con envenenamiento ARP

Nota. Autoría propia

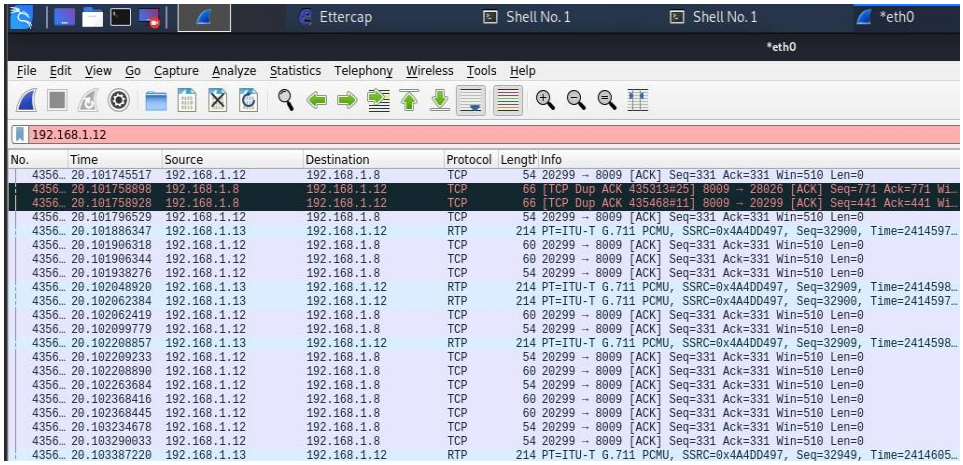
A su vez en wireshark el sniffer debe estar preparado para filtrar el tráfico entrante y la información que se está estableciendo a través del protocolo Real Time Transmision.

A diferencia de cuando se captura el tráfico en una llamada efectuada por un usuario registrado en la que hay un establecimiento con paquetes INVITE a través del protocolo SIP, en este caso no se observa este protocolo, solo muestra los paquetes RTP con las direcciones origen y destino SOURCE, DESTINATION, en cuya información no contiene tampoco las extensiones de los usuarios involucrados. (Ver Figura 96)

Cada una de las líneas representa cada paquete de datos transmitidos, el número de estos depende del tamaño o duración de la llamada.

Figura 96.

Captura de tráfico RTP en Wireshark

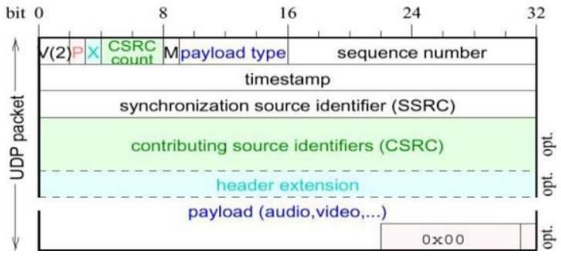


Nota. Autoría propia

Analizando estos paquetes RTP se tiene solo detalles de los siguientes campos según el Formato de paquete RTP en la Figura 97.

Figura 97.

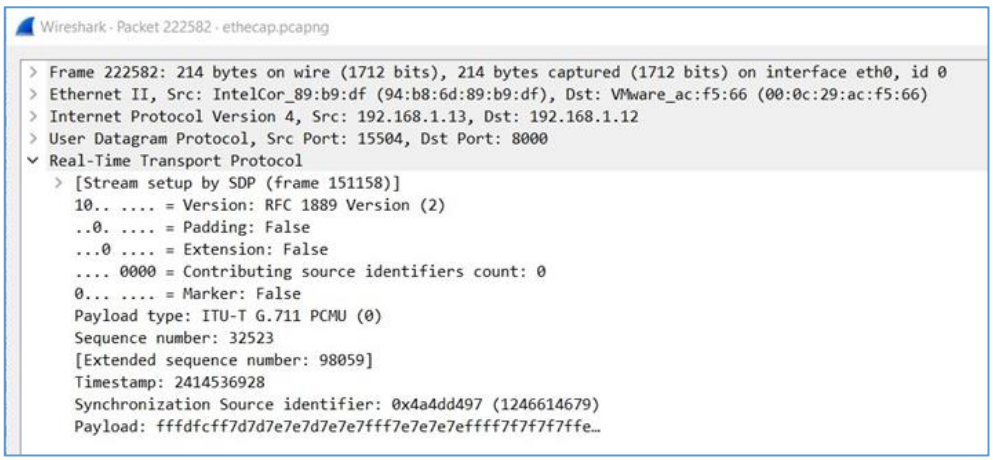
Formato paquete RTP



- Versión del Protocolo: se observa el número 2 en este campo
- Los campos de Padding (P) y de Extensión no contiene información valida.
- El tipo del formato de la carga: muestra información del códec que se utiliza.
- A continuación, muestra el número de secuencia del paquete, el timestamp para la sincronización de los datos, además del identificador de la fuente y los datos que se transportan en este paquete RTP como se muestra en la Figura 98.

Figura 98.

Análisis de paquete RTP en Wireshark

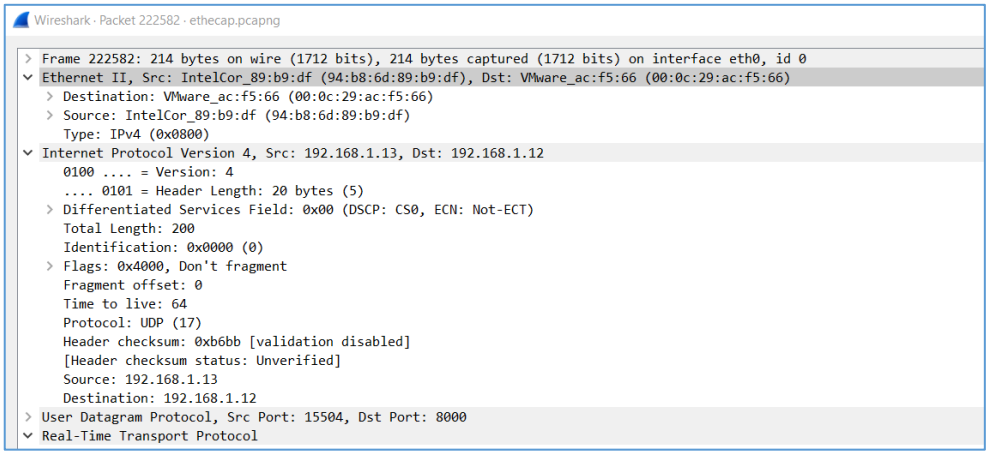


Nota. Autoría propia

La Figura 99 muestra que en la cabecera UDP se tiene la siguiente información de los puertos origen y destino respectivamente.

Figura 99.

Análisis de las cabeceras UDP en paquete RTP en Wireshark

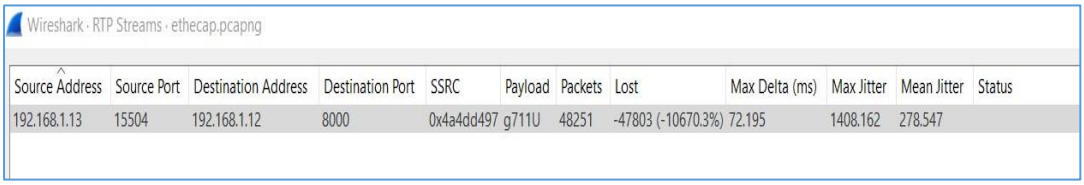


Nota. Autoría propia

Para visualizar aspectos importantes en el análisis del Protocolo RTP se escoge la opción Telephony ➔ RTP, Show All Streams para visualizar los streams que se generan en la llamada como se muestra en la Figura 100.

Figura 100.

Análisis de paquete RTP con la opción Telephony

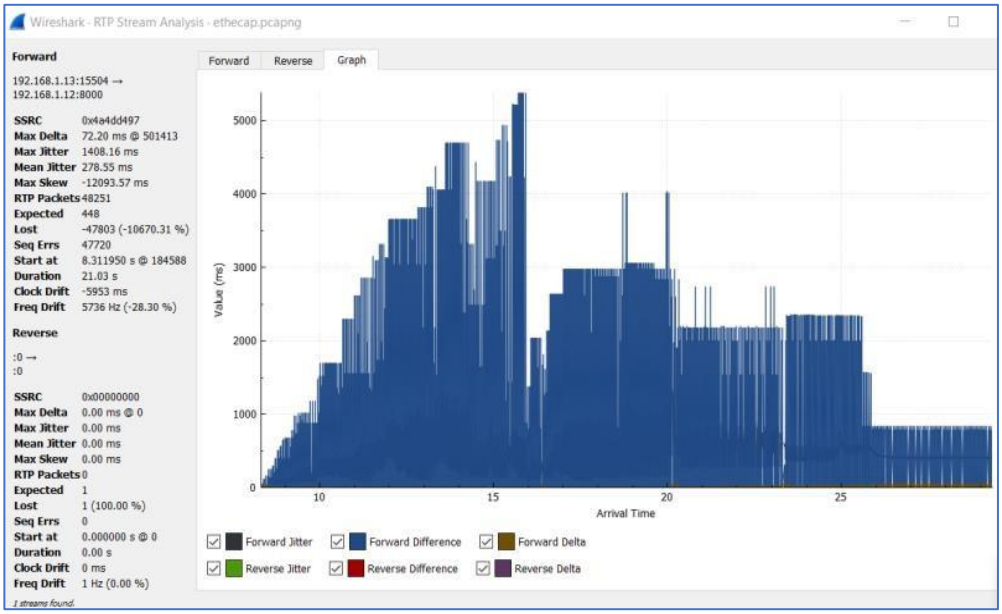


Nota. Autoría propia

En la Figura 101 se observa las estadísticas sobre los rangos mínimos y máximos del jiitter que hubo durante la llamada telefónica.

Figura 101.

Gráfico del tráfico y jitter en la llamada telefónica

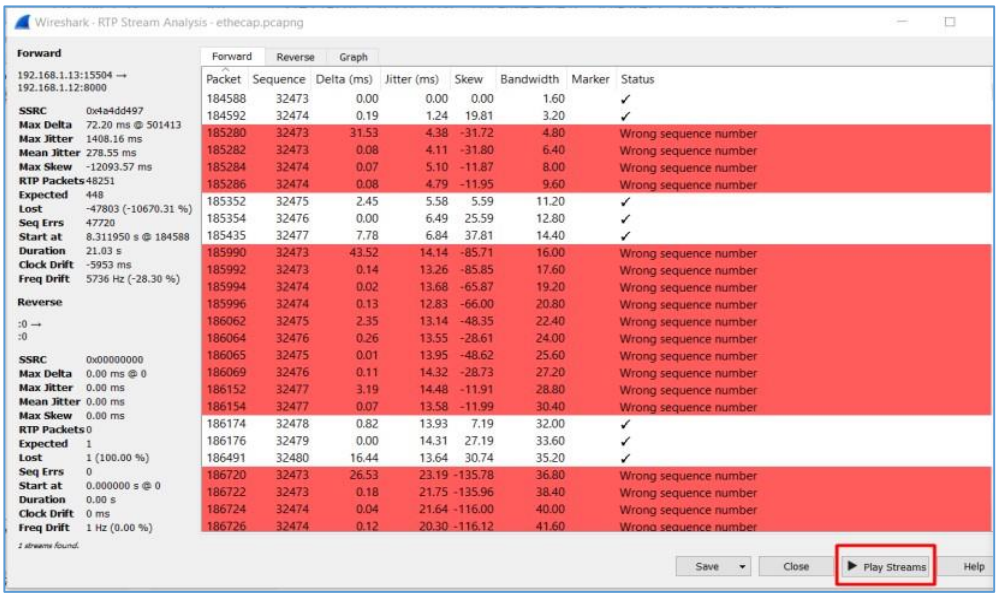


Nota. Autoría propia

Además, en la Figura 102 se evidencia los números de paquetes y la secuencia de cada uno de ellos, así como el ancho de ancho que se utiliza para trasmitir la voz

Figura 102.

Información sobre los paquetes, estado y ancho de banda



Nota. Autoría propia

Y finalmente para reproducir los stream y escuchar la grabación de la conversión se da click en play streams; como lo indica la Figura 103 para obtener el audio y en este caso el atacante podría obtener información confidencial que perjudique a la empresa.

Figura 103.

Reproducción del audio extraído en la llamada

Nota. Autoría propia

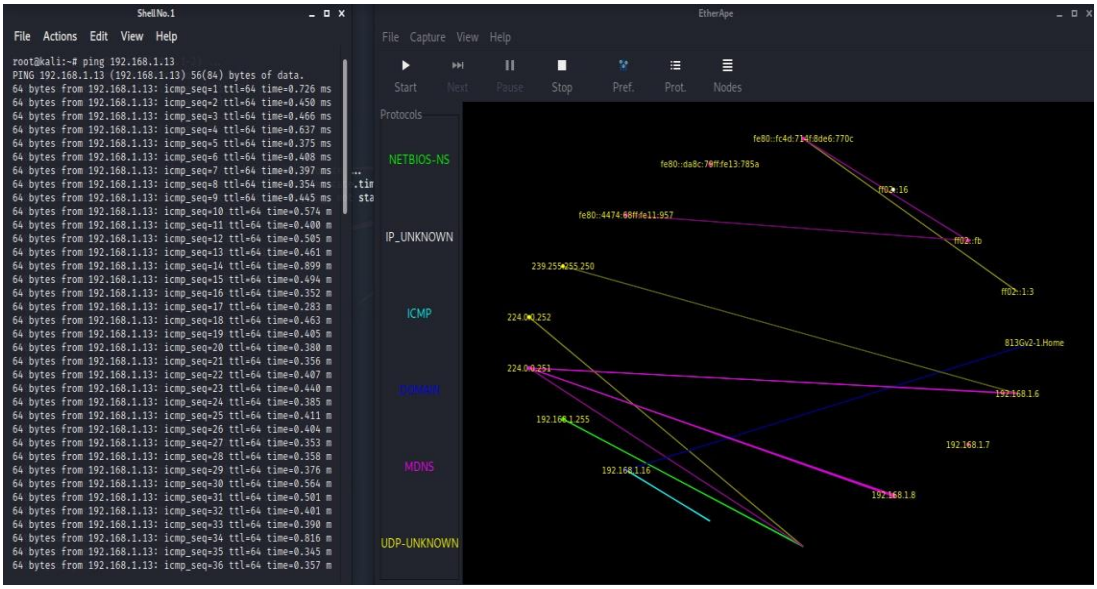
5.1.2. Denegación de servicio DoS

Este ataque consiste en saturar e inundar un sistema con la generación excesiva de mensajes INVITE, de manera que se perjudica la disponibilidad de los recursos de la red, logrando así que haya una congestión en la red y no se pueda realizar o recibir llamadas telefónicas desde cualquier terminal telefónica en este caso desde los zoiper.

Primeramente, se verifica si hay conectividad con la central de telefonía IP, se observa en la Figura 104 que el atacante si tiene acceso y puedo mapear las direcciones a través de la herramienta EtherApe, disponible en la distribución de Kali Linux.

Figura 104.

Host disponibles y visualizables desde la herramienta EtherApe



Nota. Autoría propia

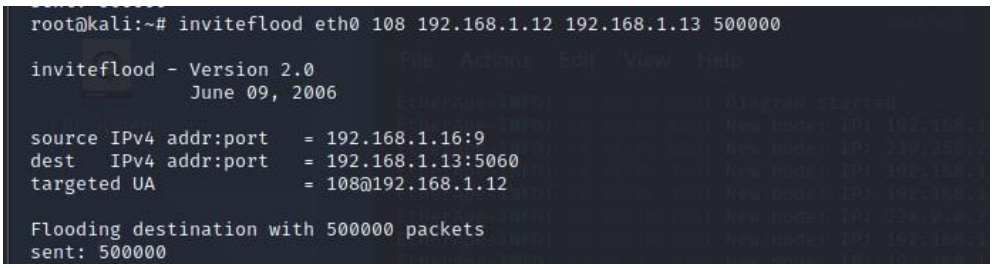
Para realizar el ataque se utiliza el método de invite flood que consiste en inundar a la víctima de paquetes con el siguiente comando y considerar los siguientes parámetros.

invite flood [interfaz][extensión][dirección origen] [dirección destino] Nro paquetes

En Kali se observa en la Figura 105 el flooding con la cantidad de paquete enviados.

Figura 105.

Inundación con paquetes INVITE a la victima

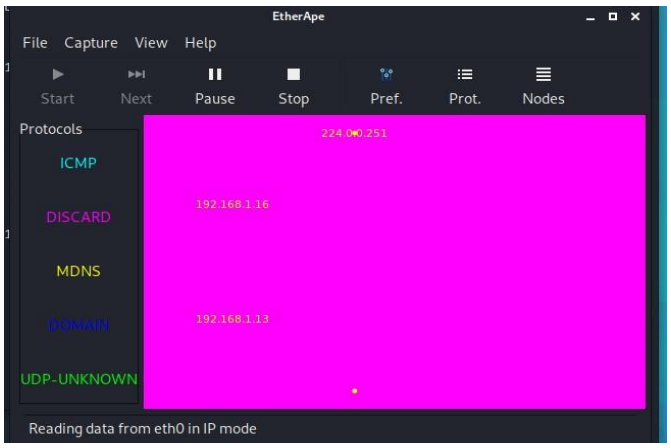


Nota. Autoría propia

Además, la herramienta EtherApe resulta muy útil al mostrar en la Figura 106 el tráfico que inunda la dirección de softphone de Gerencia, con lo cual el atacante verifica que el ataque está en proceso.

Figura 106.

Gráfica de la inundación con paquetes INVITE a la víctima.

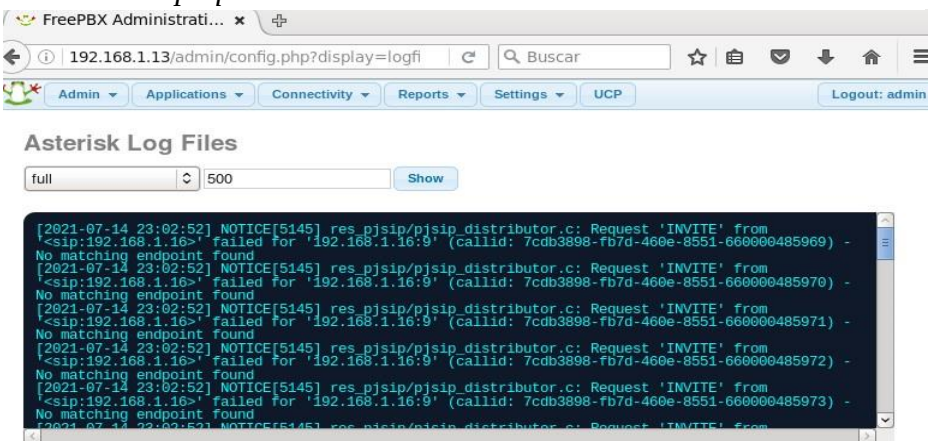


Nota. Autoría propia

También en la Figura 107 se puede evidenciar, que en la central de FreePBX en la pestaña Reportes ➔ Astersik Log Files muestra las notificaciones de los paquetes Invite que están llegando a la central y que al realizar una llamada desde Gerencia no se establece ninguna conexión.

Figura 107.

Notificaciones de los paquetes entrantes en la Central IP.

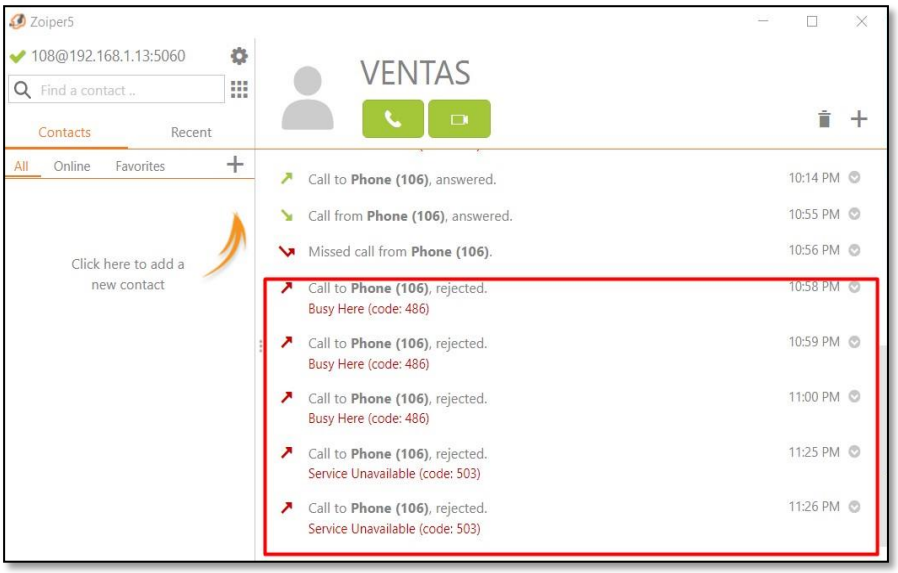


Nota. Autoría propia

En la aplicación Zoiper como indica la Figura 108 cuando se realiza la comunicación desde Origen: Gerencia con la extensión 108 hasta el destino: Ventas la llamada no se puede efectuar y muestra el código 503 de servicio no disponible, debido a que el servidor está en mantenimiento o demasiado sobrecargado.

Figura 108.

Llamada no establecida desde la extensión 108 hasta la 106.



Nota. Autoría propia

Este ataque se produjo porque en un inicio no estaba instalado el complemento Fail2ban de FreePBX y si se lo activa no satura la red y se puede realizar las llamadas sin que el servicio se vea afectando en gran manera. En la Figura 109 se observa el estado de este servicio.

Figura 109.

Fail2ban activado en FreePBX

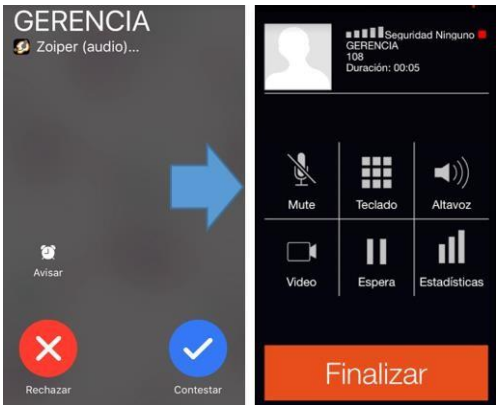
```
[root@telefonia ~]# service fail2ban status
Se está ejecutando fail2ban-server (pid  1960)...
Status
|- Number of jail:      7
`- Jail list:           apache-tcpwrapper, recidive, ssh-iptables, apache-badbot
s, pbx-gui, asterisk-iptables, vsftpd-iptables
```

Nota. Autoría propia

Por tal razón se observa en la Figura 110 que si se puede realizar las llamadas cuando este complemento se encuentra activo, no logra que la víctima que es la extensión 108 pueda contactarse con el departamento de ventas 106.

Figura 110.

Llamada desde Gerencia (108) hacia Ventas (106)



Nota. Autoría propia

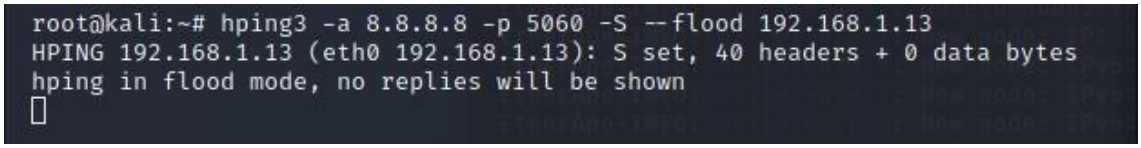
5.1.3. Denegación de servicio DDOS

A diferencia del anterior ataque en este se realiza una inundación SYN, es decir un ataque semiabierto que busca consumir todos los recursos disponibles del servidor ya que el atacante envía un gran volumen de paquetes SYN al servido las cuales pueden ser direcciones IP falsificadas, para que no se descubra su identidad (CLOUDFLARE, s.f.). En Kali linux como se indica en la Figura 111 hay una herramienta hping3 que se la ejecutará basados en los siguientes parámetros:

```
# hping3 -a [dirección origen] -p [puerto] -S – flood [dirección destino]
```

Figura 111.

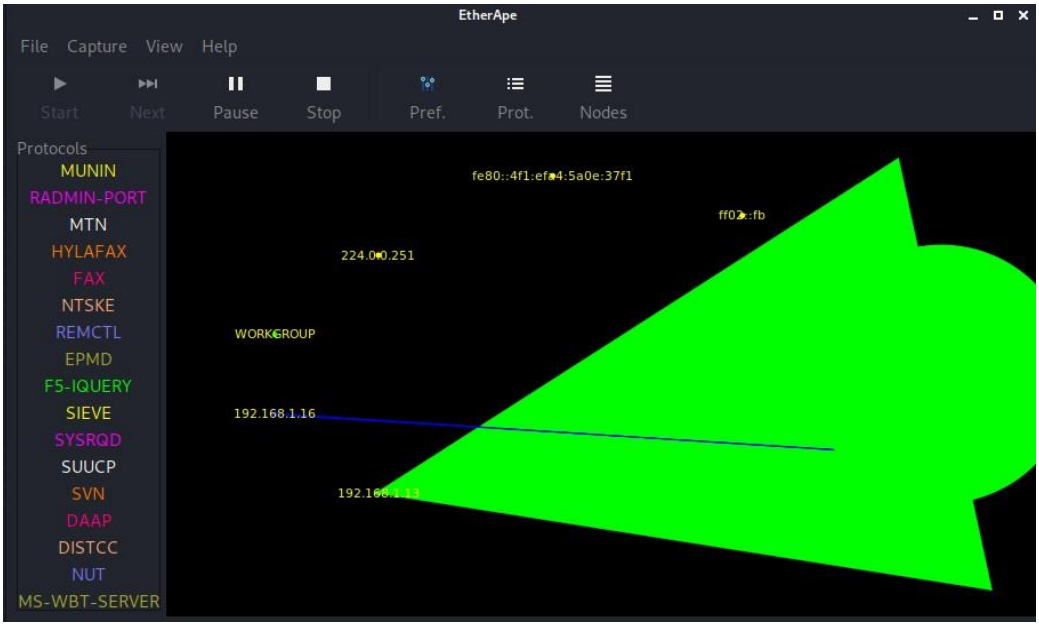
Ejecución del comando hping3 hacia Servidor FreePBX



Con la herramienta EtherApe se observa en la Figura 112 el tráfico constante que se está generando en la red para congestionar el servicio de telefonía.

Figura 112.

Mapa de inundación generado por hping3 sobre la victima



Nota. Autoría propia

Además, se puede observar en la Figura 103 las estadísticas de los paquetes enviados y la gran cantidad de paquetes más de 2 millones por lo que para realizar esto se necesita que la computadora del atacante tenga buenos recursos tanto en software como en hardware.

Figura 113.

Estadísticas de los paquetes con la herramienta hping3

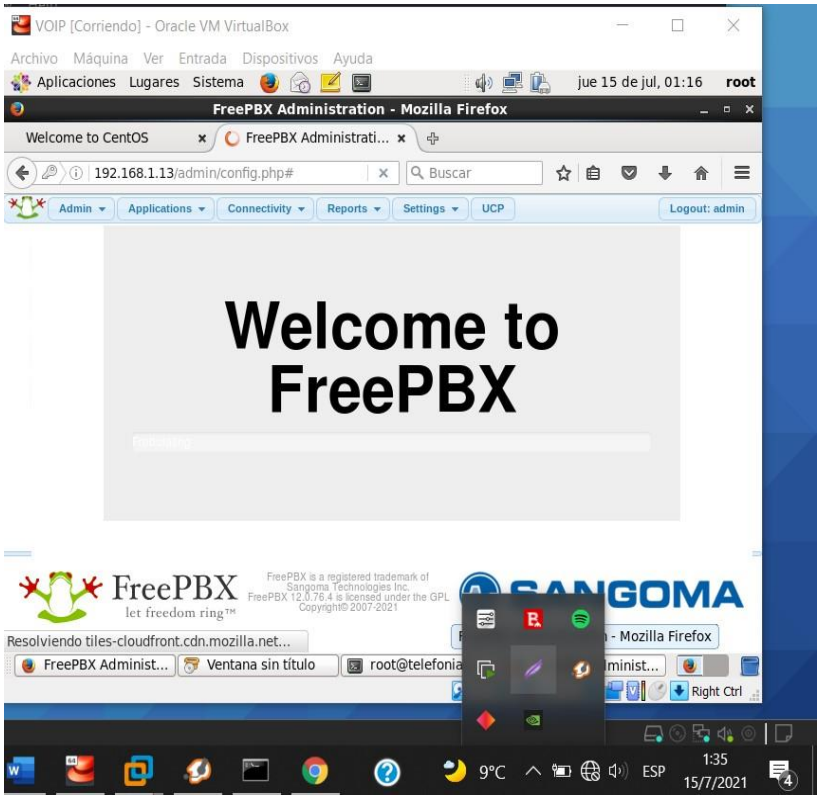
```
--- 192.168.1.13 hping statistic ---
23849874 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~# hping3 -a 8.8.8.8 -p 5060 -S --flood 192.168.1.13
HPING 192.168.1.13 (eth0 192.168.1.13): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Nota. Autoría propia

Finalmente en la Figura 114 se muestra que el servicio de telefonía cae y se demora en ingresar a la plataforma y como se apuntó a los DNS de Google también se observa que hay una desconexión del adaptador de red lo que podría hacer pensar al administrador que el problema es una mala conexión del internet y no un ataque en sí.

Figura 114.

Desconexión en la central telefónica FREEPBX.



Nota. Autoría propia

5.2. Políticas de Seguridad para la Telefonía IP.

Una vez evidenciados los fallos existentes en la red de Telefonía IP, se recomienda ciertos mecanismos de seguridad adecuados, que garantizan la protección de los sistemas de telefonía IP basados en SIP, ante ataques de Denegación de Servicio, específicamente para flooding se recomienda las siguientes políticas de Seguridad.

<table>
<tr><td colspan="2">Empresa de Soluciones Integrales
SINFOTECNIA</td><td>Pág
: 1
Versión 1</td></tr>
<tr><td rowspan="3"> 
</td><td>Políticas de Seguridad de la información</td><td>Fecha:
2021</td></tr>
<tr><td>Elaborado por:
Lucia Guerrón</td><td>Revisado: Ing. Darwin Hernández
Administrador de Red.</td></tr>
<tr><td>Aprobado por: Ing. Esteban Vallejos
Gerente Sinfotecnia</td><td></td></tr>
</table>

a) INTRODUCCIÓN

1.1. Alcance

Este Modelo de Seguridad sobre la Telefonía VoIP tiene como alcance el desarrollo de las 7 etapas de la metodología PTES con el fin de detectar las vulnerabilidades, el nivel de acceso y el grado de seguridad externo e interno, mediante la ejecución de pruebas no maliciosas que no perjudiquen el desempeño normal de la empresa, para de esta forma plantear las medidas preventivas ante las debilidades encontradas; las mismas que están identificadas para así conseguir una mayor seguridad en las comunicaciones.

1.2. Niveles Organizacionales

a) La administración del presente instrumento por parte de Sinfotecnia estará a cargo del Gerente de esta empresa privada o quien haga sus funciones.

b) Administrador de red. - Persona encargada de administrar los recursos de red de la institución. Bajo su administración corresponde la aceptación de las políticas de gestión de red.

2. MARCO NORMATIVO

El presente documento se realizó en base a la Norma NTE INEN-ISO/IEC 27002; la misma que establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos indicados en esta norma brindan una guía general sobre las metas aceptadas comúnmente para la gestión de la seguridad de la información. Cabe recalcar que ningún conjunto de controles puede lograr la seguridad completa y que se deberían implementar acciones adicionales de gestión para monitorear, valorar y mejorar la eficiencia y la eficacia de los controles de la seguridad para apoyar las metas de la organización

3. VIGENCIA

El presente documento como documento de políticas de seguridad entrará en vigencia una vez aprobado por el gerente de Sinfotecnia. Dicho manual debe ser monitoreado, revisado y mejorado, donde sea necesario, para asegurar que se cumplan los objetivos de la seguridad y del negocio de la organización.

4. ESTRUCTURA

- Mejorar el control de los dispositivos de redes.
- Ejecución de las 7 etapas de la Metodología PTES
- Planeación y definición de acuerdos.
- Recopilación de la información.
- Modelado e identificación de amenazas.
- Análisis de las vulnerabilidades
- Explotación de la información encontrada.
- Post Explotación.
- Entrega de Informes

5. TIPO DE PENTESTING

En esta investigación se emplea el testeo de CAJA BLANCA, ya que se tiene la autorización del gerente de la Empresa Sinfotecnia para tener el acceso a las instalaciones, así como a la información que se requiera para la elaboración de estas pruebas de penetración.

6. HERRAMIENTAS

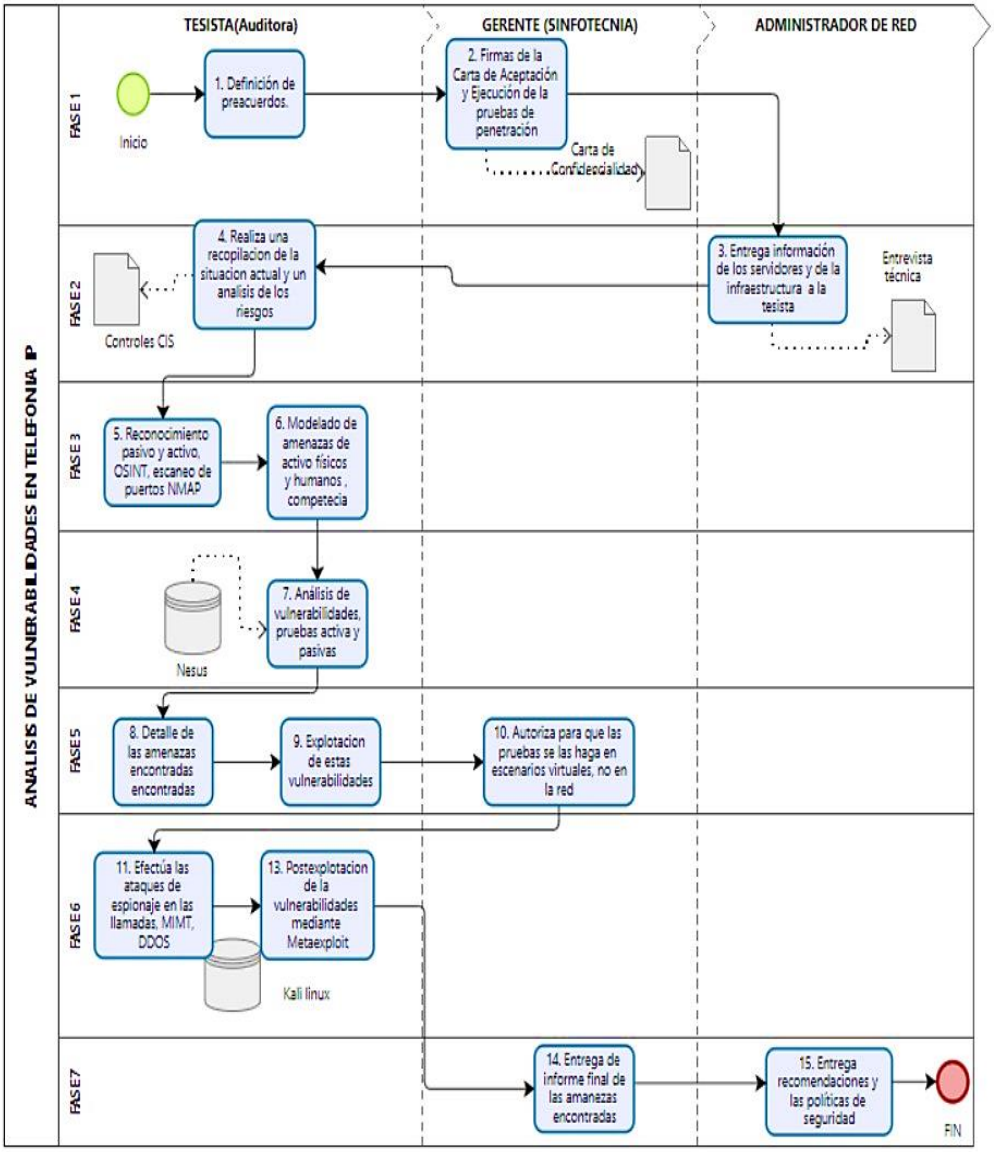
KALI LINUX	WIRESHARK	NESSUS
NMAP		
SVMAP		
METAEXPLOIT		
ETTERCAP		

7. TERMINOLOGÍA

- Malware: programa con intenciones maliciosas que se instala en un sistema operativo.
- Metaexploit: programa muy versátil que engloba muchas disciplinas de la seguridad informática. Muy utilizado por los auditores y atacantes de la seguridad informática hoy en día.
- Payload: pequeño código que utiliza un exploit para aprovechar alguna vulnerabilidad y realizar así acciones maliciosas en el sistema.
- Pentesting: acción de auditar un sistema referente a la seguridad informática
- Plugin: Pequeño programa que se acopla a otro más completo para mejorar y ampliar sus funciones
- Protocolo VoIP: protocolo que utiliza las IP comunes para realizar llamadas a través de internet.
- Protocolos TCP/UDP: convenio de comunicaciones en internet para el intercambio de datos.
- Proxy: Un servidor que ejerce de intermediario entre un sistema e internet con el fin de proteger la dirección IP origen.
- PTES: siglas de Penetration Testing Execution Estándar que reúnen un conjunto de estándares para realizar auditorías de seguridad.
- Shellcode: conjunto de ordenes traducidas a un lenguaje de de bajo nivel (muy básico para el sistema) con el objetivo de ser ejecutado en una pequeña porción de memoria.

8. FLUJOGRAMA DE EJECUCIÓN

Figura 115.
Flujograma de Ejecución



Nota. Autoría propia

Dominio	Gestión de Riesgos en la Telefonía IP	**Destinatario**
Control	Actualización de sistemas	Administrador de Red
Descripción		

3. El administrador de red deberá dar solución al problema en el menor tiempo posible y de acuerdo a las características del problema que se presente, tomando como base el perfil de riesgo de la Tabla 56 y del diagnóstico de la búsqueda y resolución de problemas, se establece un sistema de asignación de riesgos según el estado del servicio:

Tabla 56.

Perfil de Riesgo

Prioridad	***Escala***	***Riesgo***
Extremo	13-15	Riesgo extremo de que los controles de seguridad se vean comprometidos con la posibilidad de que se produzcan pérdidas financieras catastróficas como resultado
Alto	10-12	Alto riesgo de que los controles de seguridad se vean comprometidos con la posibilidad de que ocurran pérdidas significativas como resultado
Elevado	7-9	Riesgo elevado de controles de seguridad comprometidos con la posibilidad de que se produzcan pérdidas materiales como resultado
Moderado	4-6	Riesgo moderado de que los controles de seguridad se vean comprometidos con la posibilidad de que se produzcan pérdidas financieras limitadas como resultado
Bajo	1-3	Riesgo bajo de que los controles de seguridad se vean comprometidos con impactos negativos mensurables como resultado

Nota. Adaptado de (Pentest Standard, 2012).

Valoración de Riesgos:

- Riesgo (Extremo): La solución a las vulnerabilidades debe ser urgente.
- Riesgo (Alto): Se debe dar tratamiento de vulnerabilidades de forma inmediata
- Riesgo (Elevado): El tratamiento de vulnerabilidades debe ser efectivo y oportuno.
- Riesgo (Moderado): El riesgo puede ser controlado
- Riesgo (Bajo): El riesgo puede ser aceptado.

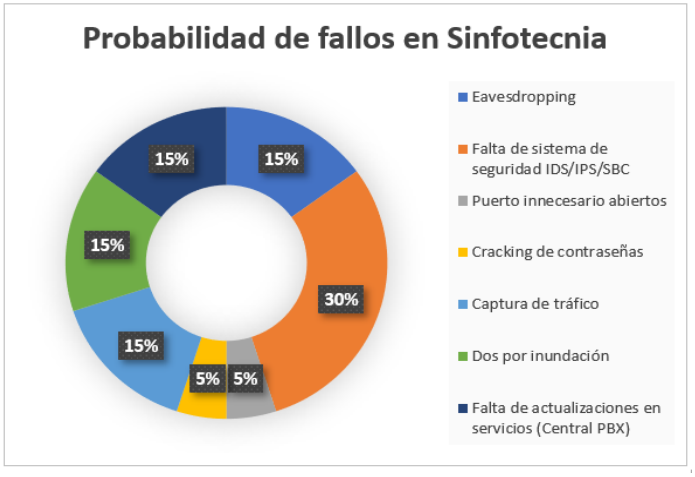
Posibilidad de amenazas:

- Riesgo (Extremo): Mas de 12 veces al año.
- Riesgo (Alto): De 9 a 12 veces al año.
- Riesgo (Elevado): De 6 a 10 veces al año.
- Riesgo (Moderado): De 2 a 6 veces al año.
- Riesgo (Bajo): 1 a 2 veces cada año

Hallazgos generales:

Figura 116.

Probabilidad de fallos en la empresa Sinfotecnia.



Nota. Elaboración propia

Empresa de Soluciones Integrales **SINFOTECNIA**	*Pág*: 8 *Versión* 1
Políticas de Seguridad de la información	Sinfotecnia Evolución Tecnológica

Dominio	Gestión de Seguridad	**Destinatario**
Control	Análisis de sistemas	Administrador de Red

El administrador de la red debe estar al corriente de los nuevos parches y actualizaciones y los aplique en sus sistemas. Es recomendable:

4. Incorporar al sistema organizacional de administración y actualización de parches de seguridad y manejo centralizado de antivirus para todos los equipos y servidores utilizados para la implementación de soluciones VoIP.

5. Habilitar las actualizaciones automáticas de cada aplicación, ya que las mismas cubren nuevos huecos de seguridad que han sido descubiertos por el fabricante.

Dominio	Gestión de Seguridad	**Destinatario**
Control	Configuraciones de usuarios	Administrador de Red
Descripción		

6. No usar nombres por defecto para archivos de configuración
7. Limitar el acceso a la ubicación de los equipos y servidores
8. Cambiar el passwords por defecto de TODOS los equipos y dispositivos que conforman la red VoIP.
9. Utilizar claves seguras para las entidades SIP, y que no se repitan.
10. Usar nombres de usuarios SIP diferentes que sus extensiones.

Empresa de Soluciones Integrales **SINFOTECNIA**	*Pág*: 9 *Nro. Revisión:* 1
Políticas de Seguridad de la información	Sinfotecnia Evolución Tecnológica

Dominio	Gestión de Seguridad	**Destinatario**
Control	Firewall SIP	Administrador de Red
Descripción		

11. El uso de Firewall SIP es una práctica muy eficiente para detectar y mitigar varios ataques a los sistemas de VoIP. Esta tecnología permite examinar todas las señales enviadas al proxy SIP protegiendo las aplicaciones VoIP de ataques específicos al protocolo SIP.
12. Al administrador de red debe configurar reglas de ingreso y salida de paquetes de voz sobre los equipos de la red VoIP para así minimizar el riesgo de accesos indebidos al servidor, así como restringir las redes IP que tendrán acceso a los servicios de telefonía.

Dominio	Gestión de Seguridad	**Destinatario**
Control	Instalación de dispositivos de seguridad	Administrador de Red
Descripción		

13. Se recomienda al administrador de Red usar un SBC (Controlador de Borde de Sesión) en la red VoIP, puesto que un SBC diferencia el tráfico de voz al entrar en la red y trabaja en la capa de aplicación a diferencia de un firewall; cabe indicar que a pesar de que los dos son muy necesarios en una red de datos, el SBC es específicamente para redes Voz sobre IP **(Ver Anexo I)**

Dominio	Gestión de Seguridad	**Destinatario**
Control	Conexiones Seguras en VoIP	Administrador de Red
Descripción		

14. Hay que tener en cuenta que para que una llamada sea segura, se debe emplear TLS para todas las conexiones entre las terminales SIP que participan en la llamada.

- Los extremos al iniciar la comunicación negocian el algoritmo de cifrado que van a ejecutar.
- Se realiza el intercambio de llaves y se acuerda los algoritmos de firma.
- Una vez establecida la comunicación, se emplean los algoritmos tanto de clave simétrica para cifrar como el de firma.

Dominio	Gestión de Seguridad	**Destinatario**
Control	Usuarios Finales	Administrador de Red
Descripción		

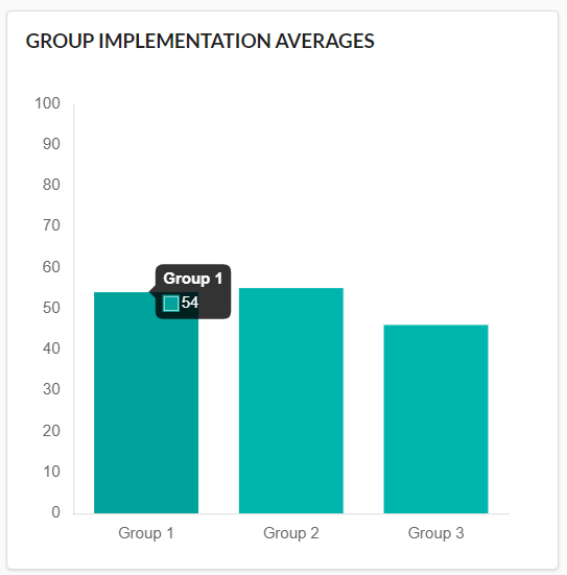
15. Se recomienda desactivar TFTP y Telnet, ya que generalmente los teléfonos SIP hacen solicitudes TFTP para actualizar archivos de configuración y firmware. TFTP es insegura ya que los archivos se envían sin cifrar. También se debe desactivar NAT en las extensiones que no son remotas y como última recomendación configurar contraseñas robustas.

5.3. Análisis Final de Riesgos

En un primer análisis se obtuvo que las salvaguardas definidas en la empresa eran de 25, después de realizar el proceso del Modelo de Seguridad de PTES, se obtiene que los resultados promedios en las salvaguardas de los controles CIS, específicamente para el grupo IG1, subió a 54 como se puede observar en la Figura 117.

Figura 117.

Estado Final de las salvaguardas definidas en la Telefonía IP



Nota. Obtenido de la Herramienta CIS SAT.

Hay que tener en cuenta que el enfoque de esta investigación está orientado a la Seguridad de la Telefonía IP, es así que el cambio más notorio se centra en los controles C03 orientado a *la gestión continua de vulnerabilidades*, pues se propuso un modelo de seguridad para lograr detectar los fallos que podría presentar más y comprometer la disponibilidad del servicio de telefonía como es el caso de las escuchas indebidas, del ataque DoS por inundación y de falta de parches de seguridad en las aplicaciones y comunicaciones.

El control C05 enfocado en *Configuración segura para el hardware y el software de las estaciones de trabajo y servidores* también muestra mejoría pues al realizar este proceso se deja en claro que los programas utilizados en las estaciones de trabajo deben estar actualizados, con contraseñas únicas, no realizar el crackeo de software si no es de fuentes seguras o confiables evitando así el ransomware; además cuando un empleado deja su estación de trabajo debe estar consciente de resguardar la información que almacena en sus dispositivos. En este punto también el administrador de red debe eliminar las cuentas y accesos de las personas que por algún motivo dejen de trabajar en la empresa.

Un cambio también se realiza en el control C09 que trata del *Escaneo y control de puertos de red, protocolos y servicios, y* utilizando herramientas de exploración, sniffer se muestran puertos que no deberían estar abiertos de manera innecesaria si no se les ocupa, así como el cambio de numeración de puertos predeterminados, en el capítulo 4 se planteó un formato para que haya una evidencia cada vez que se haga este tipo de análisis.

El siguiente punto C11 *basado en configuración segura para dispositivos de red*, tales como firewalls, routers y switches también presentan un cambio pues se configuró las reglas para que funcione Fail2Ban un complemento importante en las centrales FreePBX, y una fortaleza que ya tenían la empresa es la segmentación por VLAN que en caso de un ataque ya separa los servidores de información más sensible.

Y finalmente los controles que más evidenciaron un progreso son los C17, C19, C20 debido a constituyen la referencia a las pruebas de pentesting, gestión de incidentes y la concientización de la importancia de la Seguridad en la Telefonía IP en las personas encargadas de la administración de la red. En estos puntos se ejecutaron las distintas etapas del modelo de Seguridad y se planteó formatos de reportes de vulnerabilidades así como la entrega de informes con el detalle de procedimientos ejecutados en cada

evento, pues una debilidad en la telefonía IP si no es atendida oportunamente podría desencadenar en un ataque más intrusivo a la empresa. En la Tabla 57 se muestra estado inicial y final de estos controles que pasaron de una valoración alta a un valoración media y baja en la mayoría de los controles.

Tabla 57.

Estado inicial y final de los controles CIS.

Controles	Estado Inicial	Estado Final
C01. Inventario y control de activos de hardware		
C02. Inventario y control de activos de software		
C03. Gestión continua de vulnerabilidades		
C04. Uso controlado de los privilegios administrativos		
C05.Configuración segura para el hardware y el software de las estaciones de trabajo y servidores		
C06.Mantenimiento, monitoreo, y análisis de logs de auditoría		
C07. Protección de correo electrónico y navegador web		
C08. Defensas contra malware		
C09. Limitación y control de puertos de red, protocolos y servicios		
C10. Funciones de recuperación de datos		
C11.Configuración segura para dispositivos de red, tales como firewalls, routers y switches		
C12. Protección perimetral		
C13. Protección de datos		
C14. Control de acceso basado en la necesidad de saber		
C15. Control de acceso inalámbrico		
C16. Monitoreo y control de cuentas		
C17. Implementar un programa de concienciación y capacitación en seguridad		
C18. Seguridad del software de aplicación	No considerado	
C19. Respuesta y gestión de incidentes		
C20. Pruebas de penetración y ejercicios de equipo rojo		

Nota. Elaboración propia

Algunos de estos controles antes de ser analizados no tenían ni el estado de definidos actualmente estos controles y subcontroles ya fueron considerados como mejoras en las salvaguardas y la descripción del estado de cada control queda descrita en la Tabla 58.

Tabla 58.

Descripción actual de los controles CIS

Controles	**Estado Control**
C01. Inventario y control de activos de hardware	Definido y aprobado
C02. Inventario y control de activos de software	Definido y aprobado
C03. Gestión continua de vulnerabilidades	Implementado y reportado
C04. Uso controlado de los privilegios administrativos	Definido y aprobado
C05.Configuración segura para el hardware y el software de las estaciones de trabajo y servidores	Definido y reportado
C06.Mantenimiento, monitoreo, y análisis de logs de auditoría	Definido y aprobado
C07. Protección de correo electrónico y navegador web	Definido y aprobado
C08. Defensas contra malware	Definido y aprobado
C09. Limitación y control de puertos de red, protocolos y servicios	Implementado y reportado
C10. Funciones de recuperación de datos	Definido parcialmente
C11.Configuración segura para dispositivos de red, tales como firewalls, routers y switches	Definido y reportado
C12. Protección perimetral	Definido parcialmente
C13. Protección de datos	Definido parcialmente
C14. Control de acceso basado en la necesidad de saber	Definido y aprobado
C15. Control de acceso inalámbrico	Definido e implementado
C16. Monitoreo y control de cuentas	Definido y aprobado
C17. Implementar un programa de concienciación y capacitación en seguridad	Definido e implementado
C18. Seguridad del software de aplicación	No considerado
C19. Respuesta y gestión de incidentes	Implementado y reportado
C20. Pruebas de penetración y ejercicios de equipo rojo	Implementado y reportado

Nota. Elaboración propia

CONCLUSIONES

Una vez terminado este proyecto de investigación sobre la red de Telefonía IP de la empresa Sinfotecnia, se tiene las siguientes conclusiones:

- Se estableció un modelo de seguridad propuesto con 4 etapas denominado Model Security- Tel, el cual está basado en la metodología PTES y orientado a proteger los servicios de la Telefonía IP contra los diferentes ataques, para que el administrador de red pueda adoptar y aplicar los mecanismos más idóneos de seguridad según los parámetros requeridos en la empresa Sinfotecnia.

- Se realizó el análisis y el levantamiento de información de la red de Telefonía IP en la empresa Sinfotecnia, y en la primera inspección se observó que la versión de Sistema Operativo y de la central Free PBX/ Asterisk se encuentra con una versión bastante desactualizada por falta de parches de seguridad.

- El uso de herramientas informáticas facilita la tarea del investigador para determinar las vulnerabilidades informáticas dentro de una empresa, las empleadas en esta investigación fueron: CIS SAT Pro, Kali Linux con sus distribuciones y Nessus logrando así encontrar que el servidor de comunicaciones VoIP presentaba vulnerabilidades con un alto riesgo de gravedad, como son las escuchas indebidas en la red y denegaciones de Servicio.

- Durante la ejecución de las etapas del Modelo de seguridad y el testing de vulnerabilidades encontradas en las comunicaciones de la Telefonía IP, se demostró con máquinas virtuales que existen amenazas de seguridad, causadas

por contar con las configuraciones por defecto, puertos innecesarios abiertos en el servidor los cuales mostraban los servicios que se están corriendo en cada uno de ellos, estas vulnerabilidades se corrigieron con la instalación de la herramienta fail2ban y asegurando el puerto SSH del servidor.

- El análisis de riesgo inicial de la empresa Sinfotecnia se lo realizó basándose en los controles CIS con un resultado inicial de 25 salvaguardas definidas en estado de riesgo Alto y Considerable; luego de realizar el análisis de riesgo final se obtuvo un resultado de 54 salvaguardas con un riesgo disminuido a nivel Medio y Bajo.

- Con las medidas de seguridad propuestas se logró que la empresa considere la importancia de sus comunicaciones telefónicas creando conciencia en sus usuarios de lo importante que es el manejo de la información, evitando la proliferación y el fácil acceso en redes basadas en Internet.

RECOMENDACIONES

- Se recomienda instalar un controlador de borde de sesión en los sistemas de VoIP para reforzar, la encriptación en las comunicaciones y cuya implementación sea fácil de implementar, sin necesidad de hacer cambios en la red.
- Realizar de manera periódica una evaluación de las medidas de seguridad de la red de VoIP o en si una auditoría de sistemas por lo menos dos veces al año.
- Usar estrictamente conexiones SSH, para la administración y configuración de los equipos.
- Obtener copias de seguridad cada vez que se realicen cambios en los servidores, donde impliquen la configuración de políticas.
- Cambiar las configuraciones por defecto por ser una potencial amenaza para la seguridad, así como cambiar la contraseña de equipos y servidores, cuando se ha identificado algunos accesos no autorizados.

REFERENCIAS

3CX. (2010). *VoipForo*. Obtenido de IAX - Inter-Asterisk eXchange protocol: http://www.voipforo.com/IAX/IAX-frames.php

Arias, R., & Arias, I. (2013). *Users.* Obtenido de Técnico en Redes & Seguridad: https://www.academia.edu/38159891/Técnico_en_Redes_and_Seguridad_5._Asterisk_USERS_FREELIBROS.ORG

Atelis PLC. (2015). *Slide Player*. Obtenido de VoIP and Asterisk: https://slideplayer.com/slide/5219738/

Barbéran, Javier. (2011). *DOCPLAYER.* Obtenido de Implantación de un sistema VoIP basado en Asterisk: http://docplayer.es/802190-Implantacion-de-un-sistema-voip-basado-en-asterisk.html

Beggs, R. (Junio de 2014). *Mastering Kali Linux for Advanced Penetration Testing.* Obtenido de https://oiipdf.com/mastering-kali-linux-for-advanced-penetration-testing

Centro de Seguridad de Internet. (2020). *Centro de Seguridad de Internet*. Obtenido de Herramientas de Ciberseguridad: https://csat.cisecurity.org/

Chaudhary, D., & Falakbanu, M. (2016). *IJSRD.* Obtenido de Técnicas de Testeo: A Comparative Study of White Box, Black Box andGrey Box Testing

CIS CSAT Pro. (2018). *Guia de Usuario CSAT Pro* . Obtenido de Puntuación: https://csat.readthedocs.io/en/stable/source/csat_pro_user_guide/#scoring

CISCO. (25 de Septiembre de 2014). *CISCO*. Obtenido de Introducción de Gatekeepers para H.323: https://www.cisco.com/c/es_mx/support/docs/voice/h323/5244-understand-gatekeepers.html

Cisco. (s.f.). *Cisco*. Obtenido de http://www.cisco.com/c/en/us/products/routers/881-integrated-services-router-isr/index.html

Colombia Systems. (s.f.). *Colombia Systems*. Obtenido de Tarjetas PCI Digium: http://www.colombiasystems.com/-/tarjeta-digium-aex410/

DocShare. (Enero de 2017). *docshare.tips.* Obtenido de Comandos Nmap: http://docshare.tips/comandos-nmap_5868135bb6d87f26678b45e4.html

Elastix Tech. (s.f.). Obtenido de Aprenda Telefonía IP con Asterisk: http://elastixtech.com/protocolo-iax/

Emilse, E. (2014). *Timetoast*. Obtenido de Evolución de las telecomunicaciones: https://www.timetoast.com/timelines/evolucion-de-las-telecomunicaciones--3

España, M. C. (2003). *Servicios Avanzados de Telecomunicación.* Madrid: Díaz de Santos, S.A.

Gómez, J. (2015). Obtenido de UGR CyberSecurity Group: http://ucys.ugr.es/download/taller1/Taller1_Intro_hacking.pdf

Gómez, J., & Gil, F. (2008). *VoIP y Asterisk* . Alfaría: Alfaomega.

González, P., Sanchéz, G., & José, S. (2015). *oxWORD.* Obtenido de Pentesting con Kali 2.0: http://www.intercambiosvirtuales.org/libros-manuales/pentesting-con-kali

Guitiérrez, R. (2015). *IT Docs.* Obtenido de Seguridad en VoIP: Ataques, Amenazas y Riesgos: http://www.it-docs.net/ddata/896.pdf

INCIBE. (s.f.). *Instituto Nacional de Ciberseguridad*. Obtenido de Herramienta de autodiagnóstico : https://adl.incibe.es/questions.php

Infopulse. (3 de Febrero de 2019). *Infopulse*. Obtenido de Guide to Modern Penetration Testing : https://medium.com/@infopulseglobal_9037/guide-to-modern-penetration-testing-part-2-fifty-shades-of-grey-box-95198b8e34c3

Jesús, G. (2009). Obtenido de Universidad de Córdova: http://www.uco.es/~i62gicaj/RTP.pdf

Jiménez, C. (5 de Junio de 2016). *Seguridad en redes y sistemas: Técnicas y conceptos sobre hacking y pentesting.* Barcelona, España: Universidad Abierta de Cataluña. Obtenido de Seguridad en redes y sistemas: Técnicas y conceptos sobre hacking y pentesting: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/52944/9/cjmenezTFG0616memoria.pdf

José, H., & Roldán, D. (2006). *Tecnología VoIP y Telefonía IP*. España: Alfaomega.

Kennedy, D. (s.f.). Obtenido de SecManiac: http://www.trustedsec.com/files/Changing_an_Industry_NEOISF.pdf

López, A. (12 de Diciembre de 2009). Obtenido de Slideshare: http://es.slideshare.net/adrikr73/rtp-realtime-transport-protocol

ManageEngine. (2020). *ManageEngine*. Obtenido de ¿Qué son y cómo implementar los Controles de Seguridad Crítica CIS?: https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

Management Solutions. (2006). *Management Solutions.* Obtenido de VoIP: Convergencia y comoditización: https://www.managementsolutions.com/sites/default/files/publicaciones/esp/VOIP-convergencia.pdf

Medioroz, F. (2014). *SlideShare.* Obtenido de Telefonía IP: https://es.slideshare.net/fernandomendioroz/telefona-ip-sip-diameter-rtprtpc

Muñoz, M. (2008). *Universidad Carlos III de Madrid.* Obtenido de Introducción (recordatorio) a RTP y RTCP: http://www.it.uc3m.es/mario/sim/07_Intro_RTP.pdf

noteboox.de. (s.f.). *noteboox.de*. Obtenido de HP Proliant: https://noteboox.de/HP-ProLiant-ML110-G6-506667-421_1

Pedraza, H. (14 de Noviembre de 2014). Obtenido de Wordpress: https://hectorpedraza10.wordpress.com/2014/11/21/fases-del-haking-etico/

Pentest Standard. (30 de Abril de 2012). *Penetration Testing Execution Standard*. Obtenido de http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

Pérez, M. (Febrero de 2012). Obtenido de Scribd: http://www.scribd.com/doc/98081446/Metodologias-mas-usadas-en-pentesting-Estudio-comparativo #scribd

Pignanelli, I. (2012). Obtenido de Nachos Informatica: http://nachoseginformatica.blogspot.com/2012/11/hackercrackerlamer.html

Rico, J. (25 de Julio de 2013). Obtenido de Corporación Universitaria Republicana: http://urepublicana.edu.co/ingenieria/wp-content/uploads/2014/04/EstadoInseguridadVoIP.pdf

Suárez, G., & Quispe, R. (2011). *Universidad Rey Juan Carlos.* Obtenido de Voz sobre IP y Telefonía sobre IP.: https://eciencia.urjc.es/bitstream/handle/10115/5939/vozsobreip.pdf?sequence=1

Yunk, K. (29 de Marzo de 2019). *8x8*. Obtenido de The Ultimate Guide to VoIP Advantages and Disadvantages: https://www.8x8.com/blog/voip-advantages-disadvantages

ANEXOS

ANEXO A: Carta de Autorización.

Sinfotecnia®
Evolución Tecnológica

Ibarra, 02 de junio del 2021

CERTIFICADO

A nombre de **SINFOTECNIA Empresa de Soluciones Integrales**, yo **KLEIMER ESTEBAN VALLEJOS GARZÓN** Gerente Propietario, avalo que la **Srta. GUERRÓN SUBÍA LUCÍA ISABEL** con cédula Nro. 1003440698, estudiante de la Universidad Técnica del Norte de la Facultad de Ingeniería en Ciencias Aplicadas quien actualmente esta realizando el Curso de Actualización de Conocimientos de la Carrera de Electrónica y Redes de Comunicación tendrá acceso a la infraestructura así como a la información que requiera para la continuación de su proyecto de tesis (MODELO DE SEGURIDAD SOBRE LA *TELEFONÍA IP/OPEN SOURCE EN BASE A LA METODOLOGÍA PTES EN LA EMPRESA SINFOTECNIA*), contando con mi apoyo y autorización para el desarrollo del mismo.

Se expide el presente Certificado, para los fines que se considere conveniente.

Atentamente.

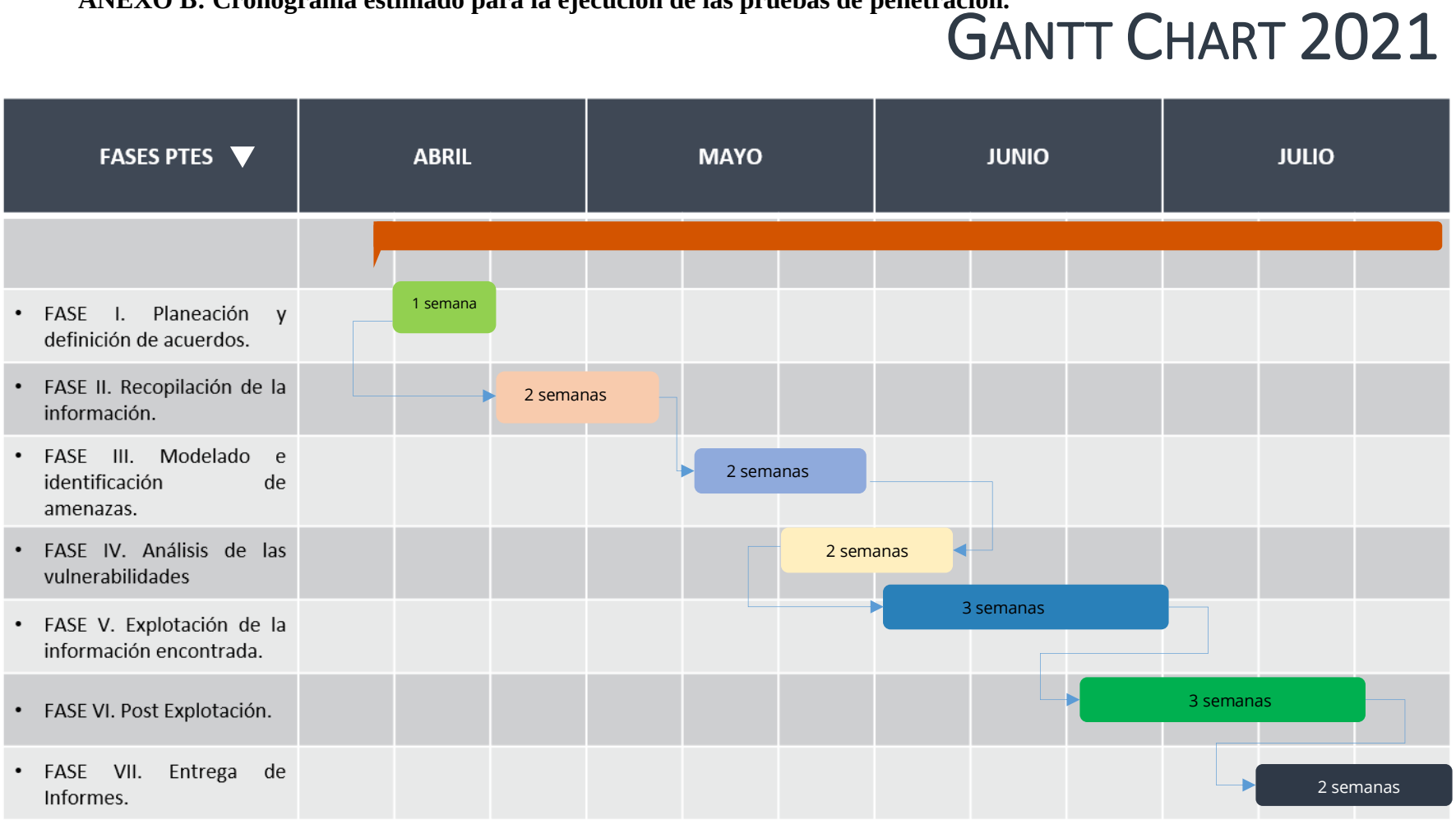
Sinfotecnia
R.U.C. 1002167003001

Ing. Esteban Vallejos
SINFOTECNIA

MATRIZ IBARRA: Dr. Marco Nicolalde 4-22 y Brasil
Teléfono: 062 957 127 ext. 101 / 062 953 686
AMBATO: Av. Los Shyris 2239 y Luís Cordero / Teléfono: 032 850 037
QUITO: Gaspar de Villarroel y 6 de Diciembre Edif. Parque Real, Torre Cipress 5, Dpto. 41 Teléfono: 023 360 583
www.Sinfotecnia.com

Infraestructura para Centros de Datos
Cableado Estructurado
Redes y Conectividad
Soluciones de Telefonía IP
Servidores Almacenamiento
Servicios TIC

ANEXO B: Cronograma estimado para la ejecución de las pruebas de penetración.



ANEXO C: Acuerdo de Confidencialidad y de No Divulgación de la Información

Sinfotecnia®
Evolución Tecnológica

ANEXO C: Acuerdo de Confidencialidad y de No Divulgación de la Información

Soluciones integrales en redes, seguridades y comunicaciones
Sinfotecnia

CARTA DE ACEPTACIÓN Y COMPROMISO PARA LA EJECUCIÓN DEL MODELO DE SEGURIDAD EN LA EMPRESA SINFOTECNIA

En la ciudad de Ibarra, a los 02 días del mes de junio del dos mil veintiuno comparece, por una parte, el señor Ingeniero **Esteban Vallejos** en su calidad de **Gerente Propietario** de la **Empresa Sinfotecnia** y la Srta. **Lucía Isabel Guerrón Subía** con **CI: 1003440698**, tesista y estudiante de la Carrera de **Ingeniería Electrónica y Redes de Comunicación**, quienes comprometen al cumplimiento de las siguientes cláusulas:

PRIMERA. - ANTECEDENTES.

1. **La Empresa Sinfotecnia**, es una empresa de Soluciones Integrales en el ámbito de las Telecomunicaciones, que surgió como una pequeña empresa en el año 2004 y que a través de estos años se ha ido consolidando como una empresa reconocida tanto en la provincia de Imbabura como en el norte del país y entre los principales productos y servicios que ofrece a empresas públicas y/o privadas se encuentran los siguientes: cableado estructurado, equipos de networking, desarrollo e implementación de redes informática, redes eléctricas, redes de comunicación, redes de seguridad, mantenimiento y asesoría técnica.
2. Los estudiantes de la Carrera de **Ingeniería Electrónica y Redes de Comunicación** de la **Universidad Técnica del Norte**, dentro de los requisitos establecidos en el Reglamento de Régimen Académico, para la obtención de su titulación, deben cumplir con el cronograma establecido dentro de un lapso de 18 meses, y en función de que los sectores sociales, productivos y culturales guarden estrecha relación con las Instituciones de Educación Superior, a fin de establecer la cooperación interinstitucional.
3. **Sinfotecnia** cuya matriz se encuentra ubicada en la ciudad de Ibarra, tiene la necesidad de mejorar la seguridad de sus comunicaciones entre sus distintas oficinas y sucursales de manera que se pueda mitigar los ataques e infiltraciones (escaneo, obtención de acceso) que se registraron en el presente año, lo que podría desencadenar en incidentes de poca o gran magnitud tanto para los clientes como para la empresa en general.

SEGUNDA OBJETO DE LA CARTA COMPROMISO:

2.01.- El presente documento establece el compromiso de las partes a fin de que la Srta. Lucía Isabel Guerrón Subía, desarrolle su proyecto de tesis cuyo tema es **"MODELO DE SEGURIDAD SOBRE LA TELEFONÍA IP/ OPEN SOURCE EN BASE A LA METODOLOGÍA PTES EN LA EMPRESA SINFOTECNIA"**

2.02.- De conformidad a lo descrito en este documento, mediante el cual el Ing. Esteban Vallejos, Gerente Propietario pone en conocimiento del Ing. Darwin Hernández, Administrador Técnico de la Empresa las tareas que realizará la Tesista, las mismas que se definen a continuación:

- Mejorar el control de los dispositivos de redes.
- Ejecución de las 7 etapas de la Metodología PTES

MATRIZ IBARRA: Dr. Marco Nicolalde 4-22 y Brasil
Teléfono: 062 957 127 ext. 101 / 062 953 686
AMBATO: Av. Los Shyris 2239 y Luis Cordero / Teléfono: 032 850 037
QUITO: Gaspar de Villaroel y 6 de Diciembre Edif. Parque Real, Torre Cipress 5, Dpto. 41 Teléfono: 023 360 583
www.Sinfotecnia.com

Sinfotecnia®
Evolución Tecnológica

- Planeación y definición de acuerdos.
- Recopilación de la información.
- Modelado e identificación de amenazas.
- Análisis de las vulnerabilidades
- Explotación de la información encontrada.
- Post Explotación.
- Entrega de Informes

TERCERA. - COMPROMISOS DE LAS PARTES:

- **La empresa.** se compromete a:

1- Brindar las facilidades necesarias durante la ejecución de la Tesis Previa a la Obtención al título Profesional y definir las actividades administrativas o comerciales que tienen que realizar los estudiantes en la Institución

- La Facultad **de Ingeniería en Electrónica y Redes de Comunicación** se compromete a:

1- Dar el respaldo y aval para realizar y culminar la tesis Sinfotecnia.

- El **estudiante** se compromete a:

1- Entregar el proyecto de investigación con las respectivas pruebas y sugerencias, aportando con su labor al beneficio de Sinfotecnia.

CUARTA DERECHOS DE PROPIEDAD: De acuerdo a lo que determina la Ley de Propiedad Intelectual, los derechos de autor le corresponden de manera igualitaria a la Universidad Técnica del Norte y a Sinfotecnia, debiendo existir autorización previa de los autores para la difusión y/o publicación del contenido de la obra en forma total o parcial.

CONDICIONES DE REVISIÓN. - De existir alguna revisión de las condiciones establecida en el presente instrumento se lo hará conocer por escrito a fin de ser aprobada por las partes.

ADMINISTRADOR. -

La administración del presente instrumento por parte de Sinfotecnia estará a cargo del Ing. Esteban Vallejos Gerente de esta empresa privada o quien haga sus funciones.

ACEPTACIÓN

Las partes aceptan cada una de las consideraciones que anteceden a las que expresamente se someten.

Para constancia de lo actuado, las partes suscriben el presente documento, en dos ejemplares del mismo formato, en Ibarra, al 02 del mes de junio del 2021.

Sinfotecnia
R.U.C 1002167003001

Lucia Guerrón
ESTUDIANTE U.T.N

Ing. Esteban Vallejos
Gerente de Sinfotecnia.

ANEXO D: Entrevista realizada en la Empresa al Administrador de la red de datos.

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

Entrevista Técnica sobre el Servicio de VoIP

Empresa: *Sinfotecnia*

Fecha: 25 de mayo del 2021

Indicación: El siguiente cuestionario está dirigido al Administrador de Red de esta empresa; cuya opinión contribuirá el desarrollo de esta investigación.

ÍTEM	SI	NO	Descripción
1. ¿En la empresa se aplican políticas de seguridad informática?		x	-
2. Anteriormente se ha efectuado alguna auditoria de seguridad en la red.		x	-
3. La Empresa tiene instalada una solución de VoIP	x		Free PBX
4. ¿La Empresa posee Firewall Empresarial?		x	-
5. Los servidores de VoIP tienen protección física contra el manejo no autorizado de usuarios.		x	-
6. La red de VoIP ha sido víctima de ataques tanto a la central como a sus terminales.	x		Intercepción de llamadas
7. Tiene implementados protocolos de seguridad en el servicio de VoIP		x	-
8. La configuración de puertos la realiza utilizando los puertos estándares y por defecto	x		

ÍTEM	1	2	3	4	5	6	7	8	9	10
9. De acuerdo a su experiencia, ¿Con qué frecuencia almacena y respalda la información de los servidores?										
• VoIP						x				
• WEB							x			
• DNS					x					
• Base de Datos							x			
• FTP						x				
10. ¿Con que frecuencia cambia el password de los equipos y dispositivos que conforman la red VoIP?										
• Central PBX-IP						x				
• Extensiones						x				
• Cuentas de usuario							x			
11. ¿Qué medida de seguridad usted considera que protegería de mejor manera la red de VoIP?										
• IDS/ Sistema de detección De intrusos							x			
• Firewall									x	
• Políticas de seguridad								x		
• Antivirus							x			
• Cifrado en las llamadas								x		
• SCB Controlador de borde									x	
12. De acuerdo a su experiencia, ¿Con qué metodología de hacking ético esta familiarizado?										
• OSSTMM							x			
• OWASP					x					
• PTES						x				
• NIST				x						

ANEXO E. Herramienta de Diagnostico de Riesgos en PYMES

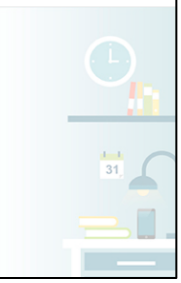
Dependencia Tecnológica

¿Qué tecnologías utiliza en su empresa?

- [ ] Correo electrónico
- [ ] Página web
- [x] Servidor(es) propio(s)
- [ ] Teletrabajo
- [x] Dispositivos móviles (tablet / smartphone / portátiles) con información de empresa

¿Cómo mantiene sus sistemas informáticos al día?

- (●) Tratamos de mantenerlos nosotros mismos como podemos
- ( ) Nos los mantiene un amigo
- ( ) Tenemos informático en plantilla
- ( ) Subcontratamos el mantenimiento informático



¿Tiene algún sistema de protección en sus ordenadores?, y ¿lo utiliza?

- ( ) No lo sé
- ( ) No, ninguno
- ( ) Todos los equipos tienen un antivirus instalado
- (●) Además de los antivirus tenemos un cortafuegos implantado en la empresa
- ( ) Además de antivirus y cortafuegos, ciframos discos y equipos

¿Ha formado recientemente a sus empleados en ciberseguridad?

- ( ) Considero que no es necesario
- ( ) Les dimos información para leer
- (●) Recibieron una charla
- ( ) Fueron a un curso de unos días
- ( ) Al contratar empleados requerimos que hayan recibido algún cursillo

¿Controla el acceso a sus dependencias?

- [ ] No, el acceso es libre
- [ ] Usamos tarjetas de acceso / llaves
- [ ] Tenemos elementos físicos que bloquean la entrada (por ejemplo, tornos o puertas con control de acceso); solo se permite el acceso identificado
- [x] Tenemos cámaras de seguridad
- [ ] Tenemos un guardia de seguridad que controla los accesos

¿Tiene definida algún tipo de política de gestión de contraseñas?

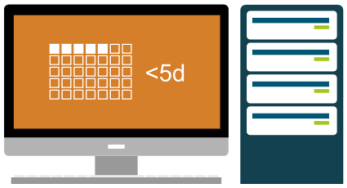
- ( ) No
- (•) Sí, el usuario escoge su contraseña
- ( ) Nuestro servidor central nos obliga a cambiar la contraseña cada cierto tiempo
- ( ) Sí, tenemos una política de gestión de contraseñas, bien definida y de obligado cumplimiento

¿Tiene presencia su empresa en las redes sociales?

- ( ) Sí, tenemos una cuenta de Twitter o Facebook... creo
- (•) Tenemos cuenta en un par de redes sociales, pero las actualizamos sólo cuando hay algo importante
- ( ) Tenemos presencia en varias redes sociales y una persona que las mantiene actualizadas (Community Manager)
- ( ) No, en ninguna

¿Cuánto tiempo podría estar su empresa con sus sistemas caídos sin que las pérdidas sean considerables?

- ( ) Menos de 4 horas
- ( ) Más de 4 horas pero menos de un día
- (•) Entre 1 y 5 días
- ( ) Más de 5 días, no es fundamental para mi actividad o tengo prevista una alternativa



¿Con qué frecuencia realiza copias de seguridad de sus sistemas?

Cuando me acuerdo | Nunca / No lo sé | Una vez al mes | Cada semana | Todos los días

¿Se realizan conexiones remotas a sus sistemas?

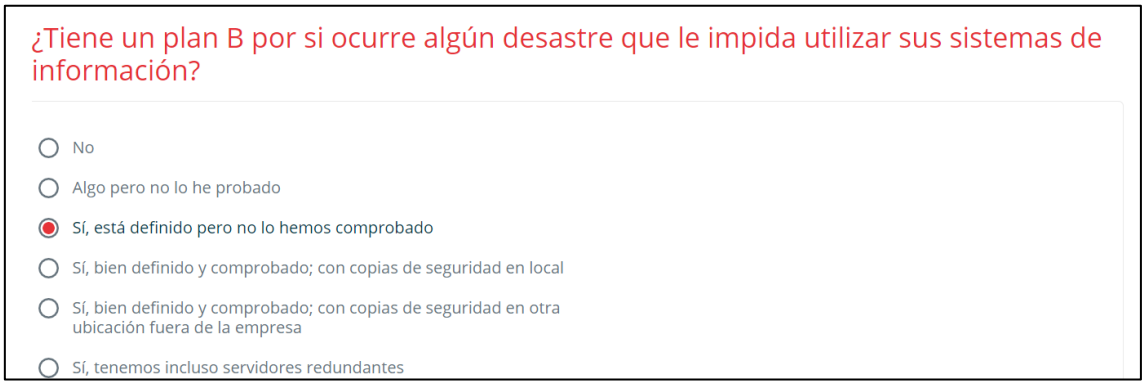
- ○ Empleados y clientes a través de la página web
- ○ Los empleados accediendo a través de una aplicación web / intranet
- ● Solo yo, de forma segura
- ○ Los empleados pueden acceder a aplicaciones internas en remoto y usar escritorio remoto
- ○ No, nunca

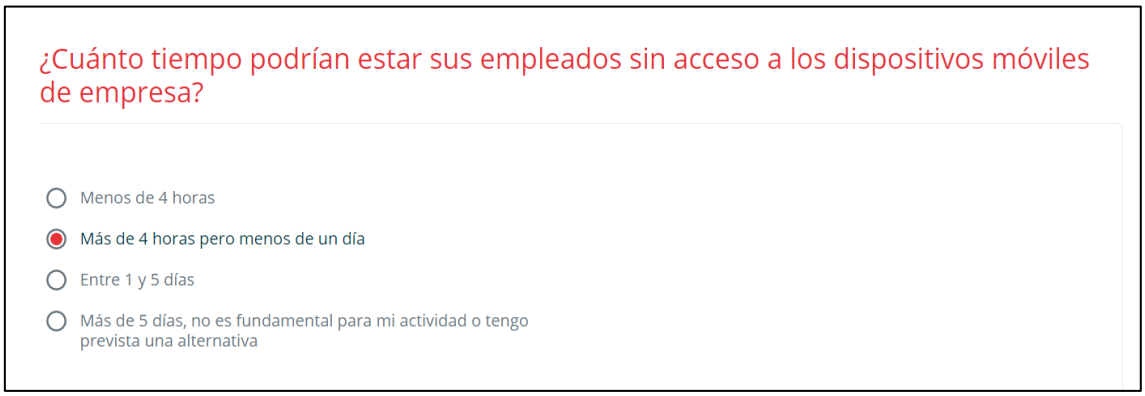
¿Quién tiene privilegios para administrar las aplicaciones internas de la empresa?

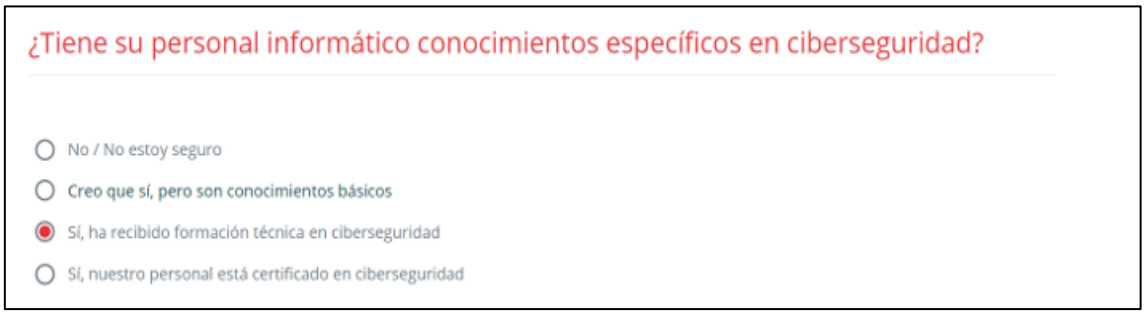
- ○ Todos los usuarios
- ○ Algunos usuarios autorizados
- ○ Solo yo
- ● Nuestro informático en plantilla
- ○ La empresa de mantenimiento informático que tenemos contratada

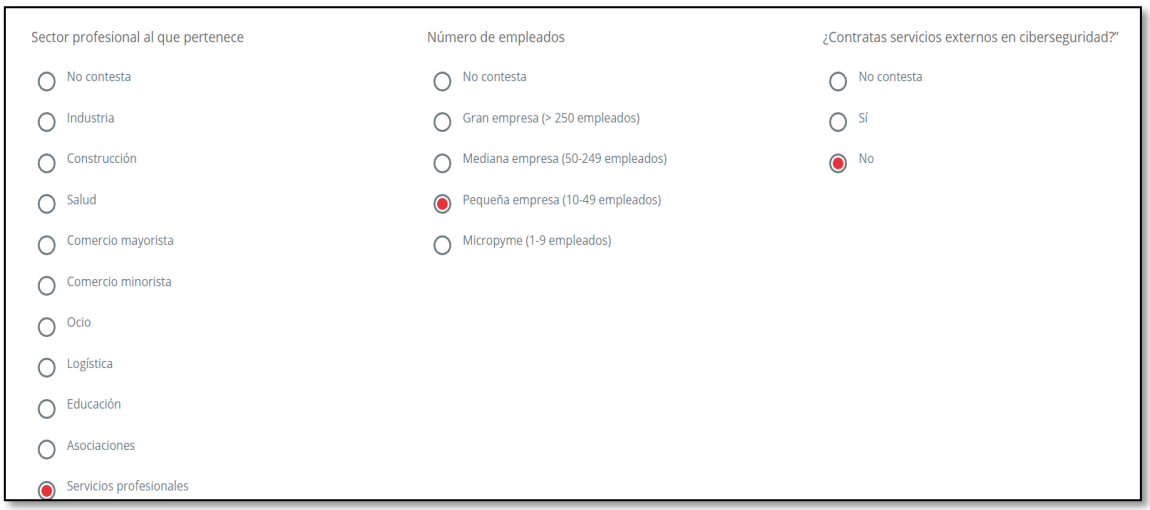
¿Dónde se encuentran los servidores y routers de su organización?

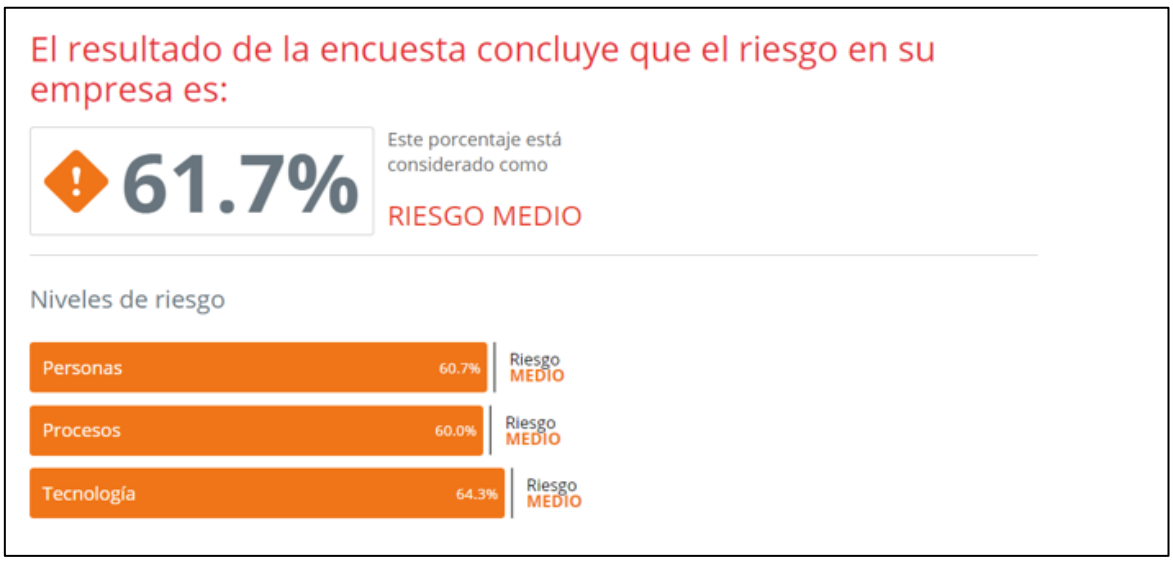
- ○ Están en una zona de paso
- ● En un cuarto compartido
- ○ En un espacio con acceso restringido
- ○ En las instalaciones del proveedor


¿Tiene un plan B por si ocurre algún desastre que le impida utilizar sus sistemas de información?
No
Algo pero no lo he probado
Sí, está definido pero no lo hemos comprobado
Sí, bien definido y comprobado; con copias de seguridad en local
Sí, bien definido y comprobado; con copias de seguridad en otra ubicación fuera de la empresa
Sí, tenemos incluso servidores redundantes


¿Cuánto tiempo podrían estar sus empleados sin acceso a los dispositivos móviles de empresa?
Menos de 4 horas
Más de 4 horas pero menos de un día
Entre 1 y 5 días
Más de 5 días, no es fundamental para mi actividad o tengo prevista una alternativa


¿Tiene su personal informático conocimientos específicos en ciberseguridad?
No / No estoy seguro
Creo que sí, pero son conocimientos básicos
Sí, ha recibido formación técnica en ciberseguridad
Sí, nuestro personal está certificado en ciberseguridad


Sector profesional al que pertenece
No contesta
Industria
Construcción
Salud
Comercio mayorista
Comercio minorista
Ocio
Logística
Educación
Asociaciones
Servicios profesionales
Número de empleados
No contesta
Gran empresa (> 250 empleados)
Mediana empresa (50-249 empleados)
Pequeña empresa (10-49 empleados)
Micropyme (1-9 empleados)
¿Contratas servicios externos en ciberseguridad?"
No contesta
Sí
No

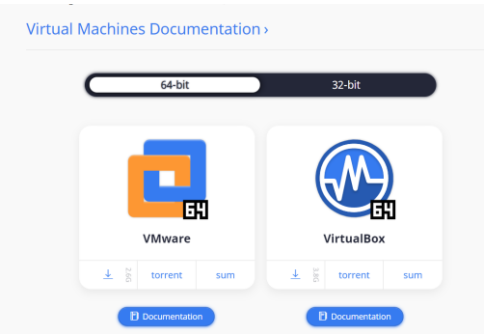


Resumen del diagnóstico

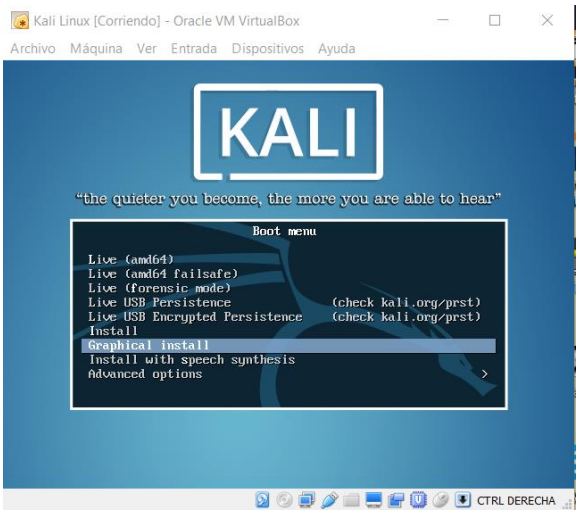
El nivel de seguridad es adecuado pero mejorable. Ya es consciente de que sus empleados son uno de los elementos en los que más tiene que invertir en ciberseguridad y tiene algunas medidas. No obstante, aún le falta hacer un esfuerzo para organizar y controlar mejor algunos aspectos (INCIBE, s.f.).

ANEXO F. Instalación de la herramienta Kali Linux

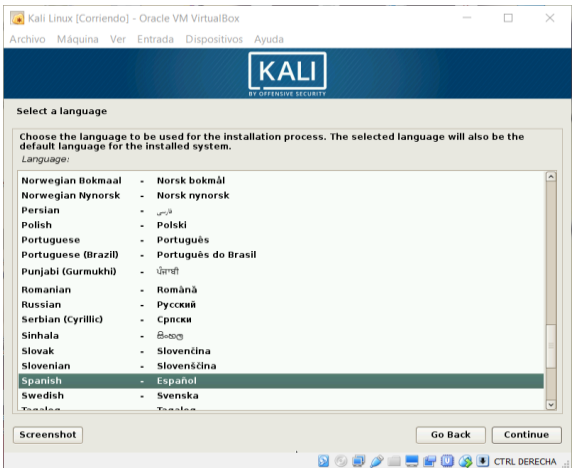
1. Instalación de Kali Linux en una máquina virtual. Descargar y seleccionar la imagen ISO que corresponde a la versión 2021.2 de Kali.



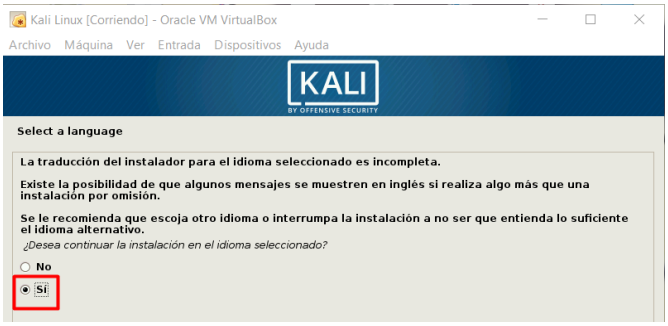
2. Seleccionar el modo de instalación gráfico.



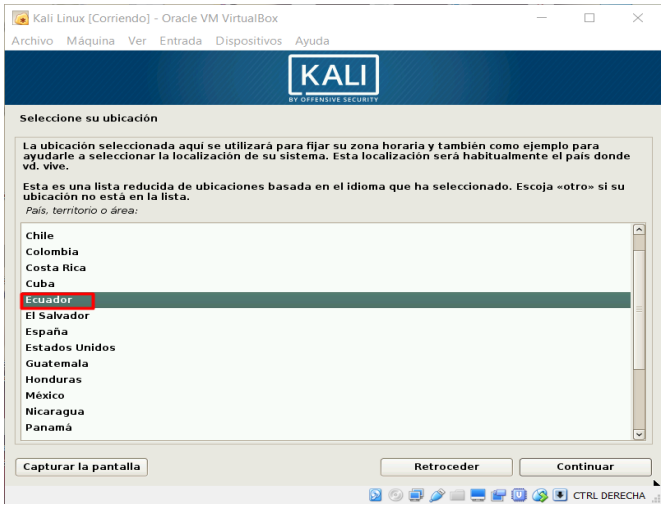
3. Seccionar el idioma para el proceso de instalación.



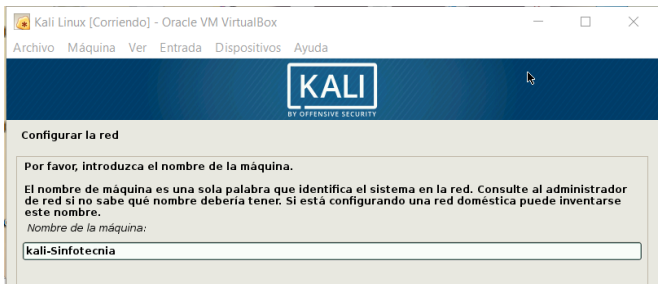
4. Marcar la opción SI para continuar con la instalación.



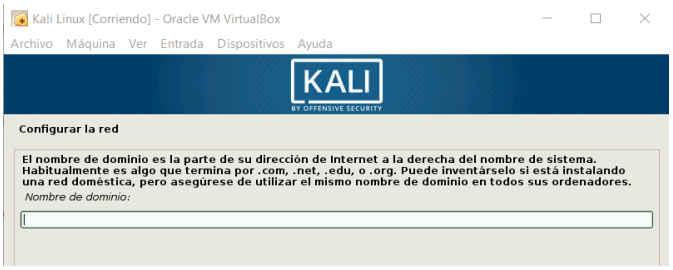
5. Buscar el país de residencia y click en continuar.



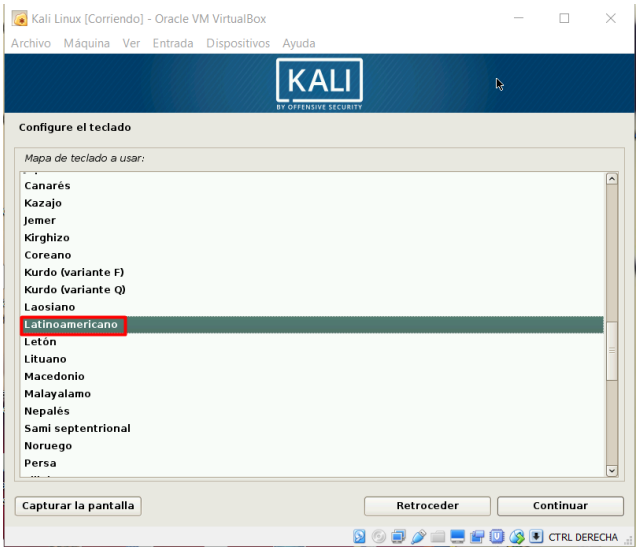
6. Ingresar un nombre para la máquina de Kali Linux.



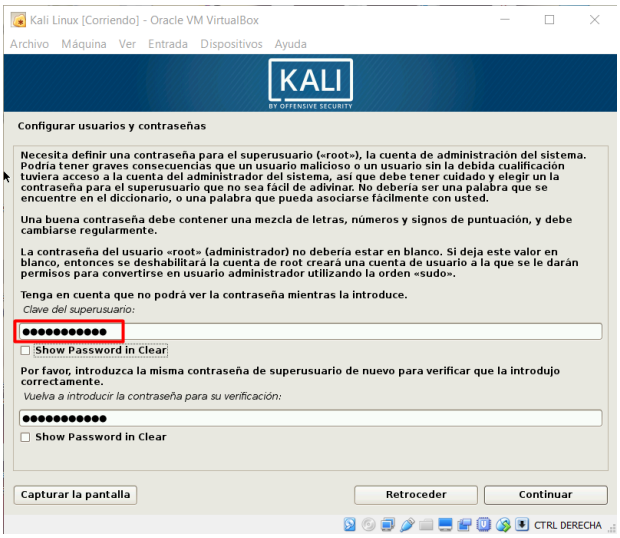
7. Escribir un dominio si se quiere meter este equipo dentro de la red, sino dejarlo en blanco.



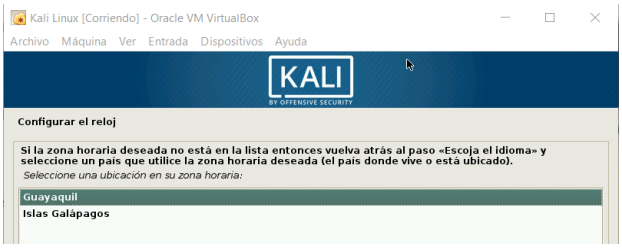
8. Elegir el lenguaje del teclado y continuar con la instalación.



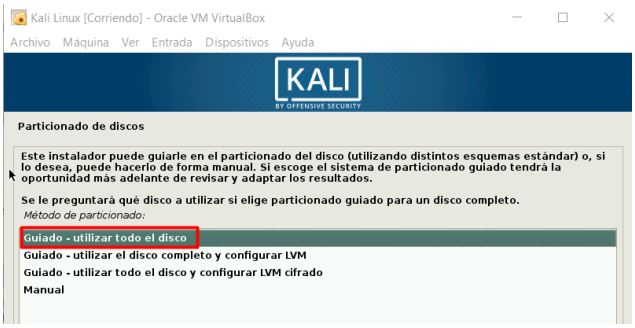
9. Ingresar una contraseña para Super Root y volver a escribirla para confirmarla.



10. Escoger la ubicación para sincronizar la hora horaria del sistema.



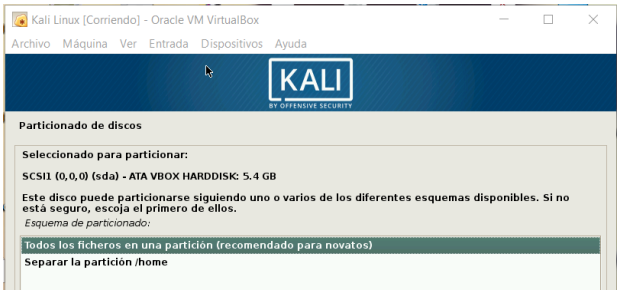
11. En esta ventana de partición de discos, marcar la opción Guiado y con la opción de usar todo el disco.



12. Escoger el controlador del disco en este caso solo se tiene uno en este equipo.

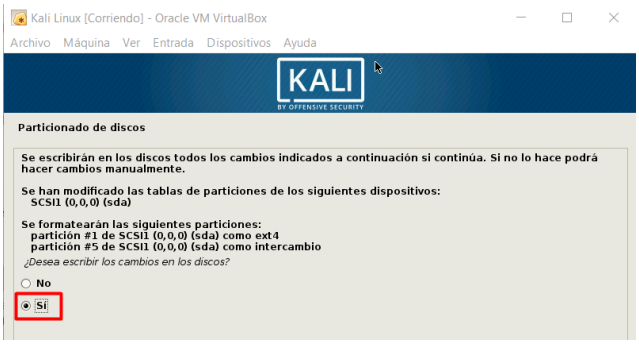
13. En este caso como solo se va a utilizar una partición, dejar en la opción por defecto -

    ➔Todos los ficheros en una partición



14. Dar click en la opción ➔ Finalizar el particionado y escribir los cambios en el disco.

15. Confirmar que se desea realizar esos cambios en el disco para continuar con la instalación del sistema.

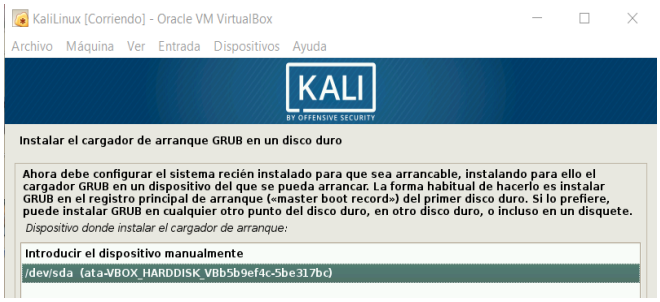


16. Esperar que se complete la instalación del sistema.

17. En esta ventana escoger la opción NO porque no deseamos en este momento la réplica en la red.

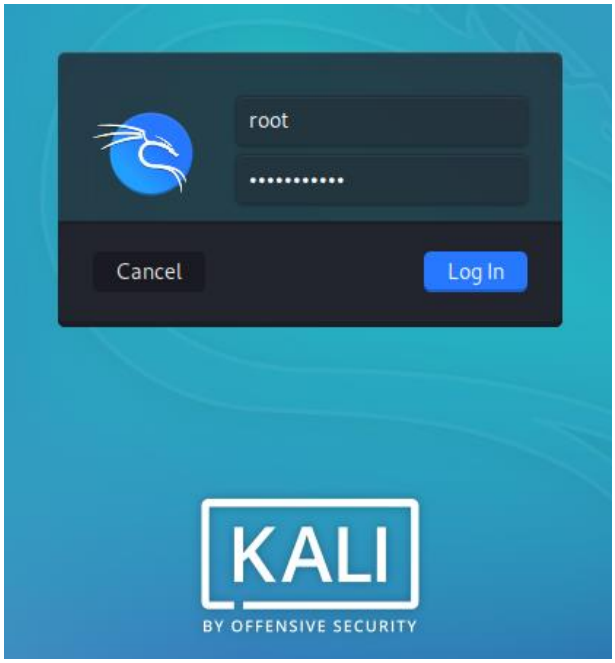
18. En este paso es importante seleccionar la opción SI ya que este cargador de arranque GRUB, permite el arranque en el registro principal.

19. Dejar la opción por defecto y click en continuar para finalizar la instalación.



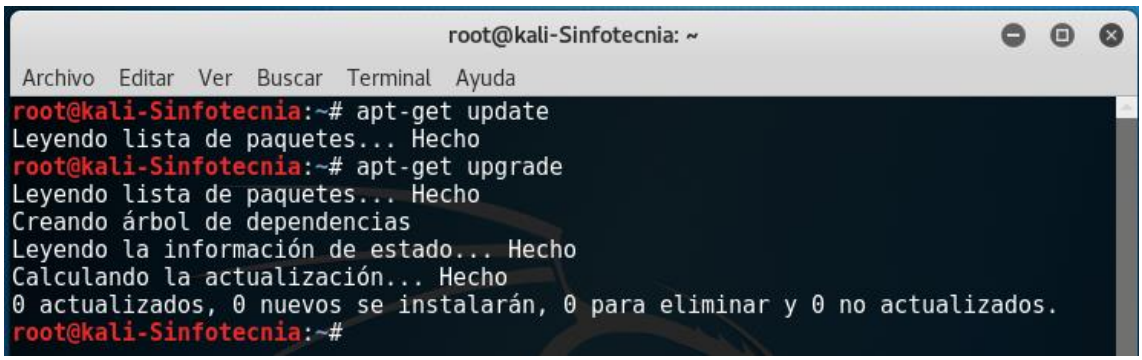
20. Esperar que finalice la instalación y cuando se haya completado aparecerá el siguiente mensaje.

21. La máquina Kali Linux se reiniciará y pedirá ingresar el usuario, que por defecto es Root y a continuación escribir la contraseña de super usuario que se ingresó en el proceso de instalación ➔ Iniciar Sesión.



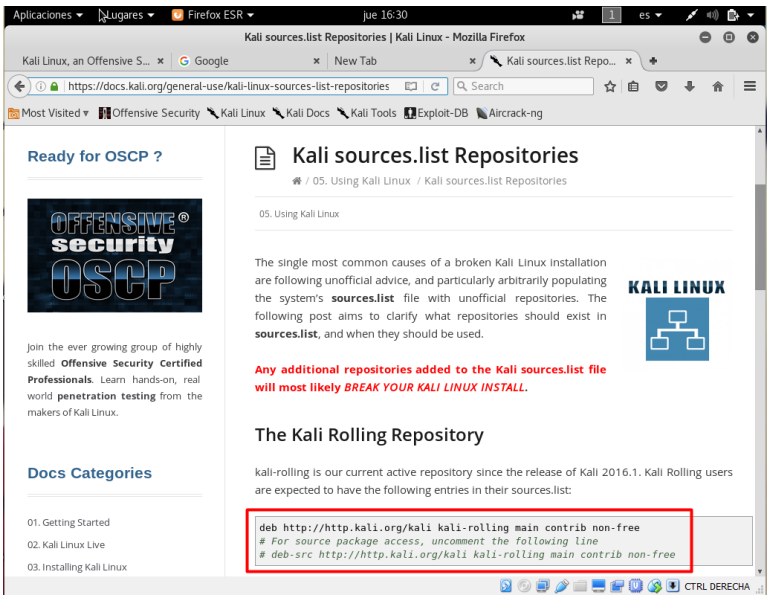
22. Así se observa el entorno de Kali Linux, ya que instalado en la máquina virtual.

23. Al actualizar por primera vez los ficheros de los repositorios, no se efectuará ningún cambio por los q es necesario editar las fuentes de actualización.



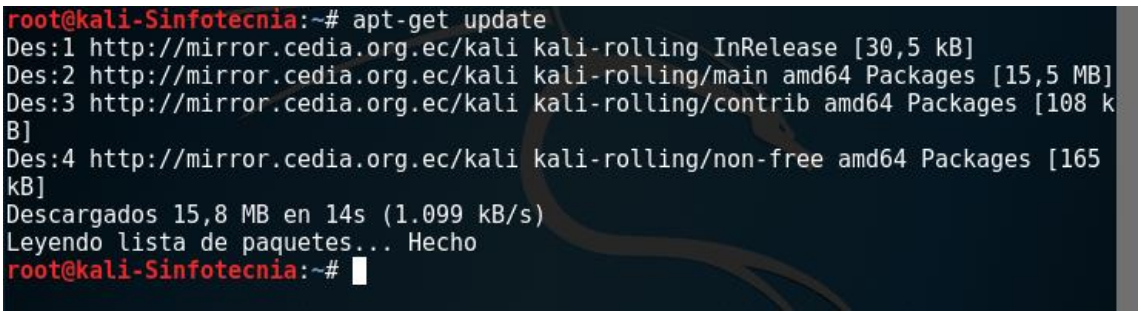
23. Para esto se debe editar el fichero con las listas de las fuentes de los repositorios.

24. Buscar en la página oficial de Kali Linux los documentos oficiales de los repositorios y copiar las instrucciones.



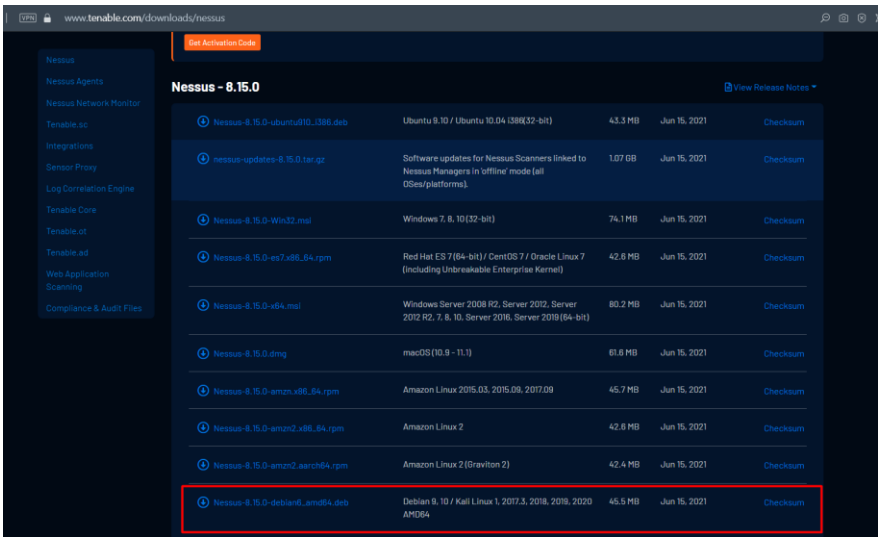
25. Al instalar Kali por defecto este no trae los repositorios necesarios para instalar ciertas aplicaciones, para lograr obtenerlas debemos agregar manualmente estos datos:

26. Una vez hecho esto ya está listo para actualizarse los ficheros update y upgrade.



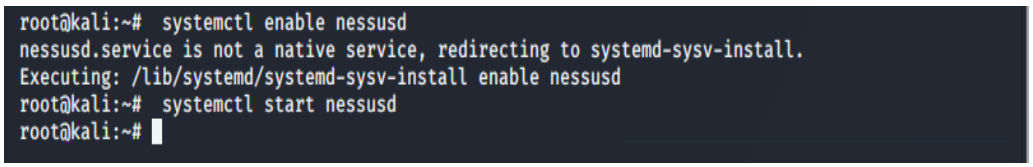
ANEXO G. Instalación del escáner de vulnerabilidades Nessus.

1. Descargar el software Nessus desde su página web, escogiendo el sistema operativo en el q se desea instalar: https://www.tenable.com/downloads/nessus

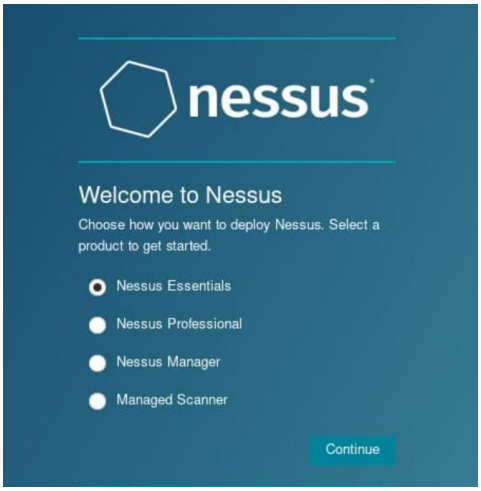


2. Una vez descargado el paquete se procede a descomprimirlo y ejecutarlo en Kali Linux con el siguiente comando:

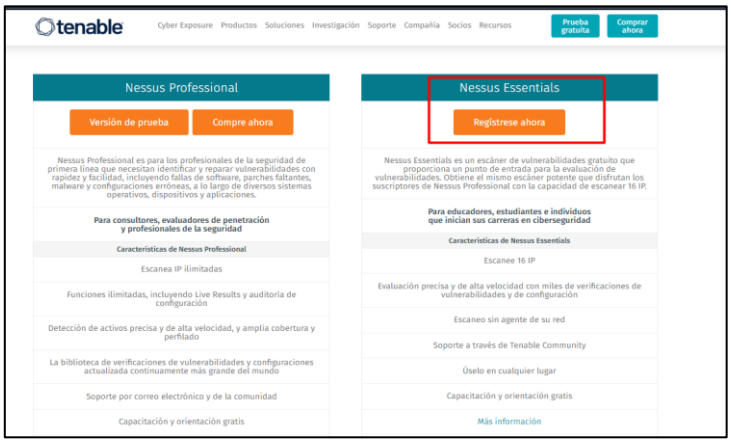
3. Para que el servicio este disponible cada vez que se inicie la máquina virtual, se ingresa las siguientes instrucciones:



4. A continuación, se debe ingresar en el navegador https://kali:8834/ para proceder con la configuración de la cuenta de administrador, en este caso se escogió Nessus Essencials.



5. En esta ventana es necesario registrarse y crear la cuenta con el nombre de usuario, su contraseña y el correo electrónico.

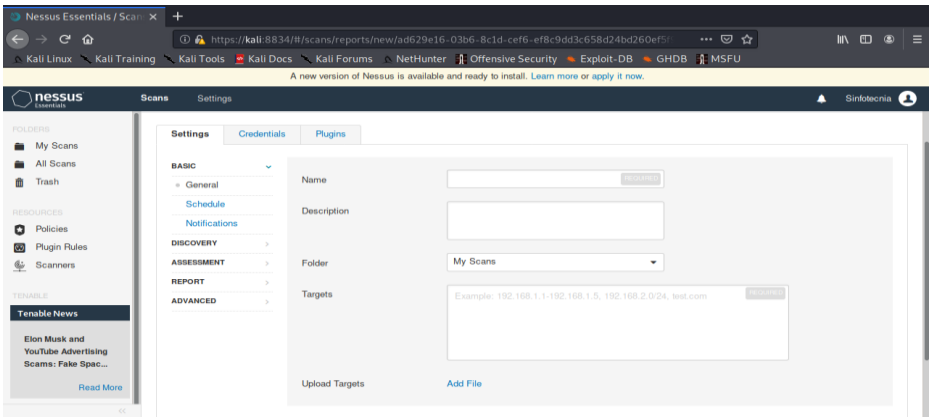


6. Como ya se hizo el registro en la página oficial de Nessus, se da click en Saltar esta opción.

7. Luego se debe ingresar la información q llegó a nuestro correo personal y así el producto quedar activado por un tiempo temporal.

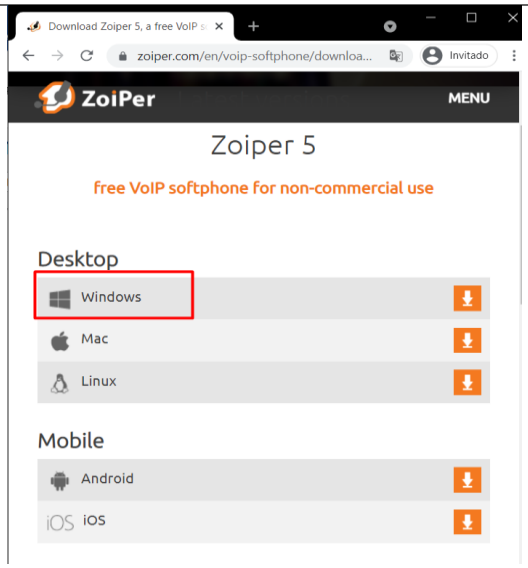
8. Completado todo lo anterior, es necesario esperar que se instalen todos los pluggins y así Nessus está listo para realizar el escaneo según las necesidades del administrador u auditor.

9. En la pestaña Nuevo Escaneo, se puede seleccionar las diferentes plantillas con las que cuenta Nessus, en esta auditoria se utilizó la opción de Escaneo avanzado para analizar una red en específico.



ANEXO H. Instalación de softphone Zoiper

1. Zoiper es una aplicación disponible tanto para PC como para dispositivos móviles. Descargar el software haciendo desde el siguiente link: **http://www.zoiper.com ➔ Download**



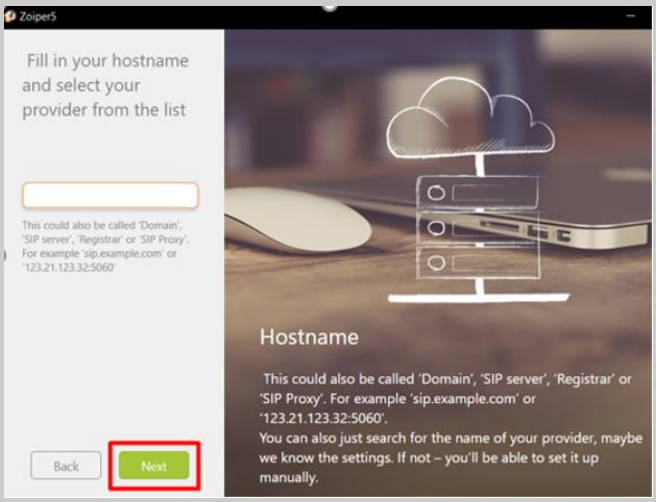
2. Seleccionar la opción de Instalar y aceptar los permisos de la aplicación, escoger 34 o 62 dependiendo del sistema dar click en Siguiente para terminar con la instalación de la app.

3. Una vez descargado se tiene la siguiente pantalla, en la cual se debe configurar la cuenta asignada en la central IP PBX y su contraseña.

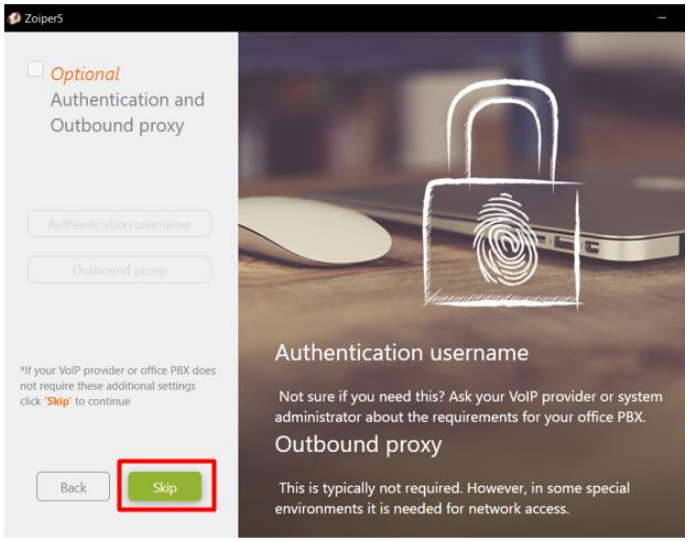
- ✓ # Extensión
- ✓ Dirección IP del Servidor
- ✓ Puesto SIP ➔ 5060

Ej➔ 105@192.168.1.14:5060

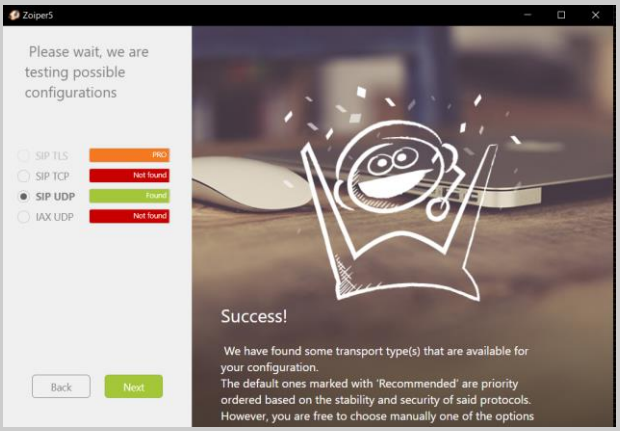
4. También da la opción de asignar el dominio del servidor IP PBX o de algún proveedor de VoIP. Como ya se encuentra asignado, dar click en **Next.**



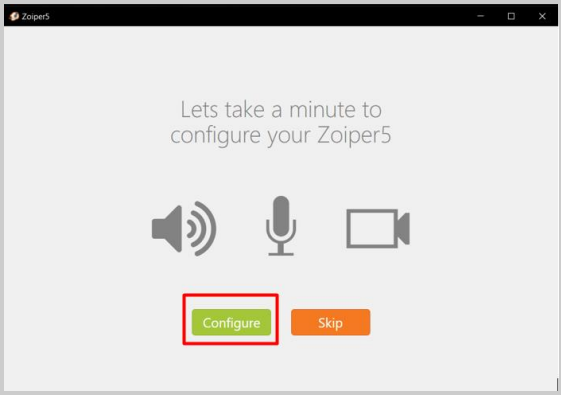
5. A continuación, muestra la siguiente pantalla en la cual da la opción de autenticación y de asignar un proxy saliente, dar click en **Skip** para omitir este paso**.**



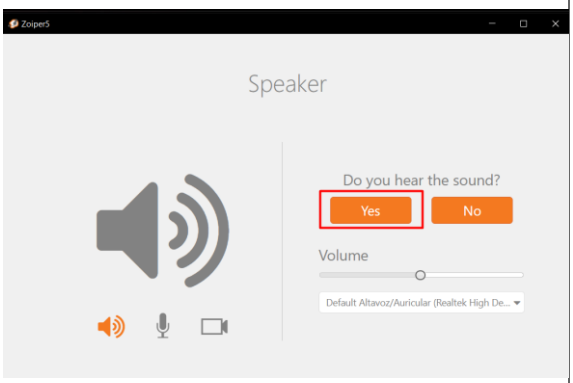
6. Esperar a que se realice la configuración del puerto y se active y dar click en **Next.**



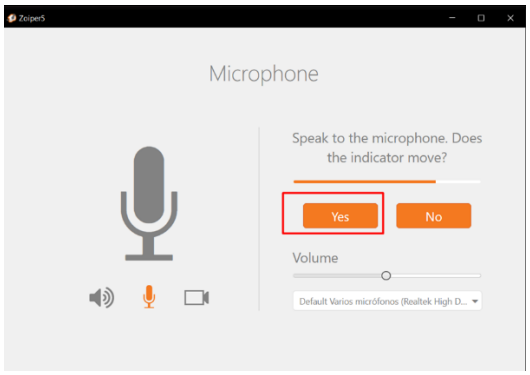
7. Una vez habilitada la configuración, la aplicación permite comprobar el sonido, la voz y el video para ejecutar esas pruebas dar click en **Configure**.



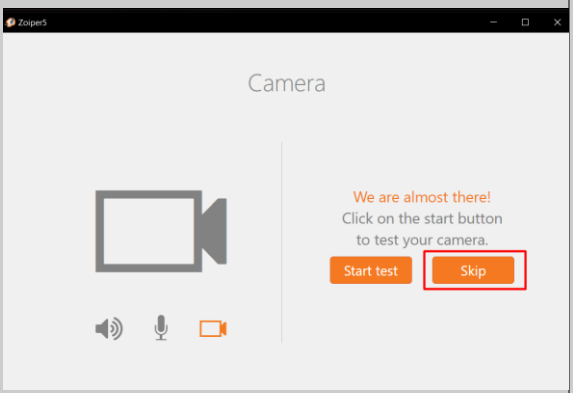
8. Se realiza la comprobación del timbre y del volumen.



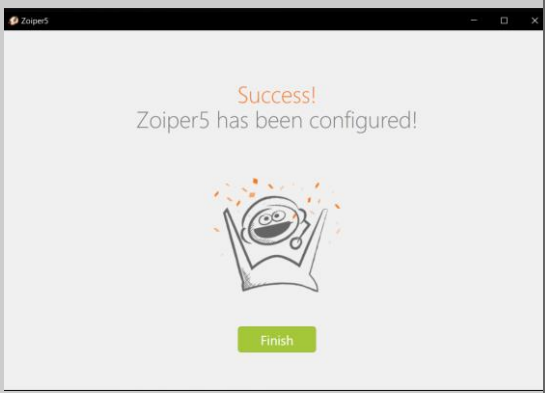
9. Además, se realiza la comprobación del micrófono y que funcione correctamente.

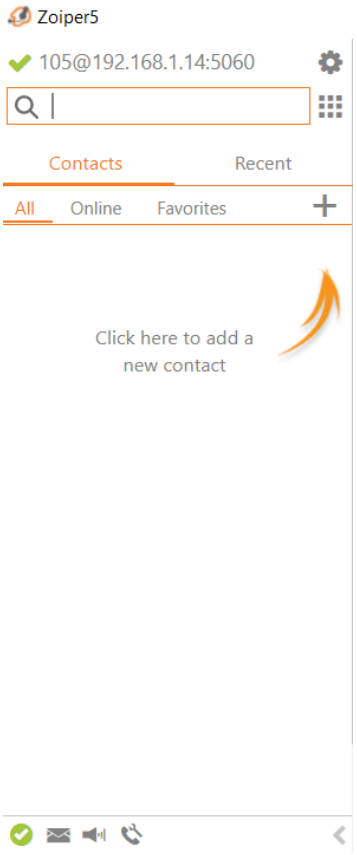
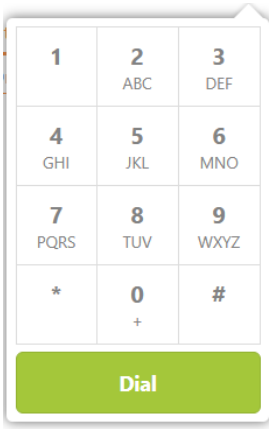


10. En este caso la configuración de la cámara no se realiza el test porque se efectuará solo llamadas de voz.



11. Finalmente muestra que el Zoiper fue configurado exitosamente.



12. Se observa que la cuenta esta registrada y activada. 	13. Finalmente, ya se puede utilizar Zoiper y realizar las llamadas entre los usuarios registrados. 

ANEXO I. Equipo de Borde SBC (Propuesta)

AudioCodes Session Border Controllers

DATASHEET

Mediant™ 500L

Hybrid SBC and Media Gateway

The AudioCodes **Mediant 500L enterprise session border controller (E-SBC)** and media gateway is a compact, high performance VoIP connectivity solution for small enterprises and branch office locations.

Scaling up to 60 concurrent sessions, the Mediant 500L connects IP-PBXs to any SIP trunking service provider and offers superior performance in connecting any SIP to SIP environment.

In addition, the Mediant 500L supports up to 8 voice channels to enable versatile connectivity between TDM and VoIP networks, such as connecting legacy TDM PBX systems to IP networks and IP-PBXs to the PSTN.

60 SBC Sessions | 8 TDM Sessions | Branch Survivability

Comprehensive interoperability
Proven interoperability with SIP trunks, SIP platforms and IP cloud services

Hybrid functionality
True hybrid SBC and gateway platform for gradual migration, low CAPEX and reduced space and power footprints

Enhanced security
Robust perimeter defense against cyber, DoS and DDoS attacks, as well as eavesdropping, fraud and service theft

Superior voice quality
Advanced capabilities for optimizing and monitoring voice service quality

High resiliency
Local branch survivability and PSTN fallback with E911

audiocodes

AudioCodes Session Border Controllers

DATASHEET

Mediant™ 500L

Specifications

Capacities			
Max. Signaling	60	**Max. RTP/SRTP Sessions**	60
Max. Registered Users	200		
Telephony Interfaces			
Digital	1-4 BRI ports, network S/T interfaces, NT or TE termination		
Analog	Up to 4 FXS and 4 FXO ports		
Network Interfaces			
Ethernet	4 GE interfaces configured in 1+1 redundancy or as individual ports		
Security			
Access Control	DoS/DDoS line rate protection, bandwidth throttling, dynamic blacklisting (Intrusion Detection System)		
VoIP Firewall	RTP pinhole management, rogue RTP detection and prevention, SIP message policy, advanced RTP latching		
Encryption/Authentication	TLS, SRTP, HTTPS, SSH, client/server SIP Digest authentication, RADIUS Digest		
Privacy	Topology hiding, user privacy		
Traffic Separation	VLAN/physical interface separation for multiple media, control and OAMP interfaces		
Interoperability			
SIP B2BUA	Full SIP transparency, mature and broadly deployed SIP stack, stateful proxy mode		
SIP Interworking	3xx redirect, REFER, PRACK, session timer, early media, call hold, delayed offer and more		
Registration and Authentication	SIP Registrar, registration on behalf of users/servers, SIP Digest access authentication		
Transport Mediation	Mediation between SIP over UDP/TCP/TLS, IPv4/IPv6, RTP/SRTP (SDES)		
Header Manipulation	Add/modify/delete SIP headers and message body using simple WireShark-like language with powerful capabilities such as variables and utility functions		
Number Manipulations	Ingress and egress digit manipulation		
SIP Interworking	3xx redirect, REFER, PRACK, session timer, early media, call hold, delayed offer		
Signal Conversion	DTMF/RFC 2833/SIP, T.38 fax, T.38 V3, packet-time conversion		
NAT	Local and far-end NAT traversal for support of remote workers		
Voice Quality and SLA			
Call Admission Control	Limit number and rate of concurrent sessions and registers per peer for inbound and outbound directions		
Packet Marking	802.1p/Q VLAN tagging, DiffServ, TOS		
Standalone Survivability	Maintains local calls in the event of WAN failure		
Voice Monitoring and Enhancement	Transrating, RTCP-XR, acoustic echo cancellation, replacing voice profile due to impairment detection, fixed and dynamic voice gain control, packet loss concealment, dynamic programmable jitter buffer, silence suppression/comfort noise generation, RTP redundancy, broken connection detection		
Direct Media	Hair-pinning (no media anchoring) of local calls to avoid unnecessary media delays and bandwidth consumption		
Test Agent	Ability to remotely verify connectivity, voice quality and SIP message flow between SIP UAs		
SIP Routing			
Routing Criteria	Incoming SIP trunk, DID ranges, host names, any SIP headers, codecs, QoE, bandwidth		
Querying External Databases	Routing based on customized queries of ENUM, LDAP, HTTP server (REST API)		
Route To	Configured SIP peers, registered users, IP address, request URI		
Advanced Routing Features	Alternative routes, load balancing, least-cost routing, call forking, E911 emergency call detection and prioritization		
SIPREC	IETF standard SIP recording interface		
Management			
OAM&P	Browser-based GUI, CLI, SNMP, INI Configuration file, REST API, EMS		
Physical/Environmental			
Dimensions	51 x 296 x 160 mm (2 x 11.65 x 6.3 in.) (HxWxD)		
Weight	670g		
Mounting	Desktop		
Power	Single universal AC power supply 100-240V, 50-60 Hz, 12V/3A or 12V/5A		
Environmental	Operational: 5 to 40° C (41 to 104°F); Storage: -25 to 85°C (-13 to 185°F) Relative Humidity: 10 to 90% non-condensing		

Sinfotecnia®
Evolución Tecnológica

Ibarra, 06 de octubre del 2021

La Empresa SINFOTECNIA – Soluciones Integrales por medio de la presente:

CONSTANCIA DE CULMINACION

Que la Srta. **Lucía Isabel Guerrón Subía** con cédula de identidad **1003440698** estudiante de la Carrera de Ingeniería en Electrónica y Redes de Comunicación de la Universidad Técnica del Norte realizó el tema de tesis: *MODELO DE SEGURIDAD SOBRE LA TELEFONÍA IP/ OPEN SOURCE EN BASE A LA METODOLOGÍA PTES EN LA EMPRESA SINFOTECNIA* y cumplió con todos los acuerdos y procedimientos establecidos por la gerencia de la empresa para el desarrollo de su trabajo de grado entregando la propuesta del Modelo de Seguridad a la empresa, la misma que sirva como referencia para realizar pruebas de penetración internas y verificar el estado de la red.

En constancia se expide el presente certificado, para los fines que la interesada lo considere conveniente.

Atentamente,

Sinfotecnia
R.U.C. 1002167003001

.....

Ing. Esteban Vallejos

Gerente General

MATRIZ IBARRA: Dr. Marco Nicolalde 4-22 y Brasil
Teléfono: 062 957 127 ext. 101 / 062 953 686
AMBATO: Av. Los Shyris 2239 y Luis Cordero / Teléfono: 032 850 037
QUITO: Gaspar de Villarroel y 6 de Diciembre Edif. Parque Real, Torre Cipress 5, Dpto. 41 Teléfono: 023 360 583
www.Sinfotecnia.com

ANEXO J. Acta de entrega del Informe Técnico.

ANEXO J. Acta de entrega del Informe Técnico.

Ibarra, 06 de octubre del 2021

Señor.
Ing. Esteban Vallejos
GERENTE SINFOTECNIA

De mis consideraciones:
Yo, LUCÍA ISABEL GUERRÓN SUBÍA estudiante de la Carrera de Ingeniería en Electrónica y Redes de Comunicación, en calidad de autora del proyecto de titulación " MODELO DE SEGURIDAD SOBRE LA TELEFONÍA IP/ OPEN SOURCE EN BASE A LA METODOLOGÍA PTES EN LA EMPRESA SINFOTECNIA", me permito hacer la entrega de los informes y políticas de seguridad sugeridas en base a las vulnerabilidades encontradas en el servicio de VoIP, con el propósito de que esta información sea socializada al administrador de red y empleados de esta empresa, para que de esta manera sea revisada y puesta en práctica.

Atentamente,

Lucía Isabel Guerrón Subía
Estudiante UTN
C.I: 1003440698

Sinfotecnia
R.U.C 1002167003001

Recibido