UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Análisis de la seguridad VoIP en la telefonía IP

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTORES:

Alvarez Nuñez, Cristhian Enmanuel (orcid.org/0000-0002-9216-6184)

De La Cruz Garcia, Julian Jesus (orcid.org/0000-0003-4598-0527)

ASESOR:

Mgtr. Tavara Ramos, Anthony Paul (orcid.org/0000-0002-4159-930X)

LÍNEA DE INVESTIGACIÓN:

Infraestructura y Servicios De Redes y Comunicaciones.

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Fortalecimiento de la democracia, liderazgo y ciudadanía.

PIURA – PERÚ

2023

Dedicatoria

La presente investigación se la dedicamos a nuestras familias por ser nuestro principal soporte, por fortalecernos y también a nuestros padres que cada día nos dan el apoyo incondicional, las fuerzas que necesitamos para que sigamos adelante y poder cumplir nuestro sueño de llegar a ser buenos profesionales.

Agradecimiento

A Dios nuestro padre celestial, por sobre todas las cosas, en la cual nos brinda buena salud, asimismo permitiéndonos alcanzar las metas propuestas y también agradecemos a nuestro asesor brindándonos las lecciones y orientaciones durante el desarrollo de la investigación propuesta.

Declaratoria de autenticidad del asesor

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, TAVARA RAMOS ANTHONY PAUL, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - PIURA, asesor de Tesis titulada: "Análisis de la seguridad VoIP en la telefonía IP", cuyos autores son DE LA CRUZ GARCIA JULIAN JESUS, ALVAREZ NUÑEZ CRISTHIAN ENMANUEL, constato que la investigación tiene un índice de similitud de 13.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

PIURA, 26 de Junio del 2023

Apellidos y Nombres del Asesor:	Firma
TAVARA RAMOS ANTHONY PAUL **DNI:** 40784283 **ORCID:** 0000-0002-4159-930X	Firmado electrónicamente por: ATAVARAR el 07-07-2023 14:31:20

Código documento Trilce: TRI - 0551659

INVESTIGA UCV

Figura 1. Declaratoria de autenticidad del asesor

Declaratoria de originalidad de los autores

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Originalidad de los Autores

Nosotros, DE LA CRUZ GARCIA JULIAN JESUS, ALVAREZ NUÑEZ CRISTHIAN ENMANUEL estudiantes de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - PIURA, declaramos bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Análisis de la seguridad VoIP en la telefonía IP", es de nuestra autoría, por lo tanto, declaramos que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. Hemos mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

En tal sentido asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de la información aportada, por lo cual nos sometemos a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

Nombres y Apellidos	Firma
CRISTHIAN ENMANUEL ALVAREZ NUÑEZ **DNI:** 70868512 **ORCID:** 0000-0002-9216-6184	Firmado electrónicamente por: CRALVAREZN el 26-06-2023 16:03:51
JULIAN JESUS DE LA CRUZ GARCIA **DNI:** 71501601 **ORCID:** 0000-0003-4598-0527	Firmado electrónicamente por: JCRUZGA11 el 26-06-2023 15:58:50

Código documento Trilce: TRI - 0551656

INVESTIGA UCV

Figura 2. Declaratoria de originalidad de los autores

Índice de contenidos

Índice de tablas

Índice de figuras

Resumen

La tecnología en los últimos años avanzó a pasos agigantados. Las empresas se han visto en la obligación de implementar tecnología en cada una de sus áreas. Muchas empresas tienen implementado un servicio de telefonía IP con tecnología VoIP, pero esta tecnología presenta vulneraciones lo cual puede traer consecuencias leves o críticas en las empresas. La presente Investigación tiene por objetivo determinar las características de la seguridad VoIP. El proyecto de investigación fue de tipo aplicada, el nivel de la investigación fue descriptivo. La investigación tuvo los siguientes resultados: según el escaneo a la VoIP, las vulnerabilidades se pueden dividir por nivel de riesgo o de impacto, este nivel se determinó según el software Nessus que trabaja con sistema de puntuación CVSS, también la investigación tuvo como resultados la cantidad de vulneraciones por escenario presentado, el cual indicó vulnerabilidades altas en cada una de ellas, por último se obtuvo las soluciones que se deberían realizar para contrarrestar estas vulnerabilidades. Todos estos resultados se lograron gracias a las simulaciones realizadas. La investigación demostró que se pudo escanear e identificar vulnerabilidades, de la misma manera se pudo plantear una serie de pasos para mejorar el nivel de seguridad.

Palabras clave: Protección de datos, Gestión de riesgos, Red de Telecomunicaciones.

Abstract

Technology has advanced by leaps and bounds in recent years. Companies have been forced to implement technology in each of their areas. Many companies have implemented an IP telephony service with VoIP technology, but this technology presents vulnerabilities which can have minor or critical consequences in companies. The objective of this research is to determine the characteristics of VoIP security. The research project was of applied type, the research level was descriptive. The research had the following results: according to the scanning of VoIP, vulnerabilities can be divided by level of risk or impact, this level was determined according to the Nessus software that works with CVSS scoring system, also the research had as results the number of vulnerabilities per scenario presented, which indicated high vulnerabilities in each of them, finally it was obtained the solutions that should be performed to counteract these vulnerabilities. All these results were achieved thanks to the simulations performed. The research showed that it was possible to scan and identify vulnerabilities, in the same way it was possible to propose a series of steps to improve the security level.

Keywords: Data Protection, Risk management, Telecommunications networks

I. INTRODUCCIÓN

Internet al pasar de los años se ha convertido en un servicio de mucha importancia y necesidad para la mayoría de personas y sobre todo de las empresas, gracias a internet se ha logrado implementar la telefonía IP (Protocolo de telefonía por Internet), un servicio que se ha convertido de suma importancia para muchas empresas ya que este servicio es de fácil acceso y uso. Dentro de la telefonía IP encontramos la VoIP. La estructura del servicio telefonía IP depende de esta tecnología para lograr su objetivo.(Olano Díaz y Sánchez Aguilar 2017)

Según lo investigado en artículos y tesis, determina que la telefonía es de mucha ayuda para las empresas y para usuarios también, pero es en la VoIP donde surge el problema de la telefonía IP, ya que se ha visto afectada en su seguridad y es vulnerada por los ciberdelincuentes, ocasionando malestar y disconformidad en el usuario. De la identificación de la teoría, SPAM, es un elemento que en esta investigación se busca determinar si sigue siendo un peligro para las empresas y/o usuarios. (Azrour et al. 2019)

SPIT o SPAM de VoIP se ha vuelto uno de los principales problemas para la telefonía IP, los ciberdelincuentes utilizan esta vía para poder realizar llamadas no deseadas utilizando la tecnología VoIP, también logran bloquear diferentes llamadas desviándose a otro destino generando que lo clientes se incomoden y ya no quiera volver a llamar a la empresa, lo que está generando una pérdida de clientes a las empresas.(Kamas y Aydin 2017)

La motivación de este proyecto se dio a partir del aumento de robos que se viene generando a través de la telefonía IP. Surgió la necesidad de investigar más a fondo este problema que viene causando grandes pérdidas en las empresas, ayudando así a la ciencia en futuras investigaciones. La telefonía IP pasó de ser un beneficio a ser un problema. Por lo expuesto anteriormente, nos preguntamos ¿De qué manera influye la seguridad de la VoIP a la telefonía IP?

El proyecto de investigación se justificó académicamente ya que se utilizaron conceptos y teorías científicas actuales con la finalidad de desarrollar el análisis

de la seguridad VoIP en la telefonía IP. La justificación social se dio porque el análisis que se desarrolló servirá como apoyo para futuras investigaciones, de la misma manera servirá para mejorar los servicios de la telefonía IP. La justificación metodológica se dispone debido a que esta investigación analizó los distintos escenarios en los que la seguridad VoIP puede ser vulnerada. Por último, la justificación práctica se obtuvo por el desarrollo del análisis de la seguridad VoIP en la telefonía IP.

La presente investigación tuvo como objetivo general identificar las características de la seguridad VoIP, también tuvo 3 objetivos específicos, el primero fue determinar las características de seguridad según la protección VoIP, el segundo fue determinar el nivel de seguridad según el control de acceso VoIP y por último determinar el nivel de seguridad según la disponibilidad VoIP.

.

II. MARCO TEÓRICO

En Indonesia, Adhilaksono y Setiawan (2022) descubrieron que, con respecto a las métricas de calidad de la experiencia, unas de las más escogidas es la puntuación media de la opinión, la evaluación perceptiva de la calidad del habla y la relación señal-ruido máxima. Durante este estudió se revisaron 38 artículos en la cual están relacionados con las métricas de calidad de VoIP. Asimismo, realizó una búsqueda con la consulta de métricas de calidad de SIP y SIP sobre WebSocket en Google Scholar y además se consiguió 277 resultados en el mes de abril del 2021. De estos 277 resultados, se alcanzaron nueve artículos más relevantes que hablan de WebRTC y ocho artículos más relevantes que hablan de SIP. Sólo se analizaron los artículos que hablan de la calidad, no de la implementación, el despliegue o la arquitectura de la VoIP. Se realizó una búsqueda adicional para encontrar más artículos relevantes en Google Scholar con la siguiente consulta de búsqueda: rendimiento de VoIP SIP, evaluación del rendimiento de SIP, evaluación del rendimiento de SIP sobre WebSocket, estudio de VoIP, estudio del rendimiento de la aplicación de VoIP, métricas de calidad de SIP y métricas de calidad de las aplicaciones de VoIP. En este artículo se concluyó que todavía hay un pequeño número de estudios sobre la apreciación de la calidad de SIP. Esto se debe a que WebRTC es más sencillo de implementar que SIP, por lo que hay más gente que habla de WebRTC. (Adhilaksono, Setiawan 2022)

Llorens (2022) En su investigación para fin de grado titulada “Análisis e investigación en ataques de vulnerabilidades con Nessus.", tuvo como objetivo dar a conocer más sobre la herramienta Nessus, los usos, las fases de testeo y como gestionar las vulnerabilidades encontradas por el software. Para poder realizar su investigación trabajo con distintos escenarios en cuales aplicó escaneos. El concluye que en un ámbito real se debería realizar un escaneo a todos los equipos de la empresa, dividiendo por grupos con la finalidad que no se alargue el tiempo de escaneo. Teniendo los resultados de escaneo es necesario darle solución para no tener riesgos en la información. Él también nos dice que Nessus puede ser utilizado por

atacantes cibernéticos, ellos con las vulnerabilidades encontradas podrían buscar la forma de atacar y robar información.(Llorens Muñoz 2022)

Espinoza (2020) En su investigación para fin de grado titulada “Implementación de Ethical Hacking para Mejorar la Gestión de Riesgos en los Sistemas Informáticos de la Municipalidad Provincial de Moyobamba” Su objetivo era tomar conciencia de los riesgos potenciales y sus posibles repercusiones. Reconocimiento, Escaneo, Enumeración, Análisis de Vulnerabilidad, Hackeo de Sistemas y Escalamiento de Privilegios fueron las principales fases de la metodología utilizada para el hackeo ético. Después de realizar su investigación, llega a la conclusión de que ahora hay 35 vulnerabilidades y 10 amenazas, lo que representa un aumento en la cantidad de riesgos identificados. La búsqueda de vulnerabilidades en los sistemas informáticos se hizo mucho más fácil con el uso de OpenVas y el escáner de vulnerabilidades Nessus. Por otro lado, la encuesta y las preguntas ayudaron a identificar riesgos que habrían tenido un impacto negativo significativo en el Municipio.(Espinoza Araujo 2020)

En Agadir, Azrour, Farhaouia, Ouanana, Guezzaz (2019) En su investigación, dan más detalles sobre los enfoques para detectar SPIT. Presentaron un enfoque que se basa en el cálculo del valor de seis características. En su trabajo, utilizamos el algoritmo K-Means para agrupar las llamadas como spammer o no spammer. El resultado de la investigación es experimental muestra que nuestro enfoque propuesto puede alcanzar una tasa de verdaderos positivos de entre el 83,3% y el 99,23%, dependiendo del número de SPIT en la red. Se concluye una propuesta de un nuevo enfoque para detectar las llamadas de spammer basado en el algoritmo K-Means. Se calculan seis características de cada llamante utilizando el método propuesto. La información de las personas que llaman y de las llamadas se extrae de la base de datos de registros detallados de llamadas. (Azrour et al. 2019)

En Lambayeque, Olano y Sánchez (2017) En su investigación han usado una red muy amplia en la red IP, asimismo una comunicación por cable para transferir video y audio digital. También aprovecho la ciencia aplicada sobre

la alimentación a través de Ethernet, les ha permitido usar una red para transferir la alimentación a la mayoría de los equipos en su establecimiento de la Municipalidad Distrital de La Victoria. Su objetivo general de su investigación es distinguir los tipos de servidores e instrumentos utilizados en bajo plataforma Linux de acuerdo a los requerimientos. En su investigación se concluye que el servidor lo han aplicado en Linux y el software Elastix que les ha permitido organizar sus recursos integrando Fax, Mail, PBX, Mensajería instantánea, siendo un instrumento indispensable en la implementación de su proyecto. (Olano Díaz, Sánchez Aguilar 2017)

En Guayaquil, Franco (2019) Ha examinado las vulnerabilidades de los sistemas de VoIP como parte de su investigación, efectuando pruebas de pentesting basadas en hacking ético, aplicado simulaciones definidas que les permitió llevar a cabo las pruebas requeridas, fue presentada para optar el grado de título profesional de ingeniero en Networking y telecomunicaciones en la Universidad de Guayaquil. Aplicado en la ciudad de Guayaquil, tuvo como objetivo analizar las vulnerabilidades de la seguridad en sistemas de VoIP, utilizando herramientas de hacking ético. Su investigación es de campo en la cual han recopilado información mediante una encuesta, entrevistas a profesionales involucrados y con conocimientos de las vulnerabilidades que se pueden presentar en los sistemas VoIP. Como resultado, se garantizó la disponibilidad, confidencialidad e integridad de la comunicación gracias a la prueba de análisis de vulnerabilidades realizada en la central telefónica VoIP. (Franco Romero 2019)

Eche y Lizano (2023) En su investigación ha desarrollado un sistema de seguridad de información para restablecer la gestión de riesgos de Tecnología de Información realizado en la Municipalidad de Sechura, ha sido presentado para obtener el título profesional de ingeniero de sistemas en la Universidad César Vallejo. La metodología Zero Security, que consta de seis fases: Reconocer, Escanear, Enumerar, Analizar, Explotar y Reportar, se implementó en Piura con la intención de mejorar la gestión de riesgos TI en el municipio de Sechura. Su investigación concluye en reconocer las

vulnerabilidades y amenazas dando el mejoramiento del objetivo general. (Eche Pingo y Lizano Mendoza 2023)

Cotto (2019) En su investigación ha realizado un estudio sobre las medidas y protocolos de seguridad en las redes informáticas del UPC de la Parroquia Barreiro, fue presentada para optar el grado de título profesional de ingeniería de sistemas en la Universidad técnica de Babahoyo. Aplicado en Ecuador, tuvo como objetivo la identificación de medidas y protocolos de seguridad para una buena gestión de la información en el UPC de Barreiro. En su estudio de caso usa como metodología la investigación cualitativa. En su investigación se concluye realizar un escaneo en la red, ayudando a conocer si existen vulnerabilidades y asimismo reducir el nivel de riesgos de seguridad que se pueden presentar. (Cotto Soliz 2019)

En Bogotá, Bolaños, Cruz y Reyes (2018) en su investigación titulada “Identificación y propuesta de una solución de mejora a las vulnerabilidades informáticas de la red y del ambiente de servidores de preproducción de la entidad KERALTY”, tuvo como objetivo identificar las vulnerabilidades y dar solución a ellas para las mejoras informáticas de la empresa en estudio. Ellos utilizan el software Nessus para poder hallar las vulnerabilidades, este un análisis se realizó a 14 servidores de 178. Con el análisis realizado lograron encontrar las soluciones a las vulnerabilidades con lo cual se pudo mejorar la seguridad de los servidores. Ellos concluyen que al realizar esta mejora fortalecen la seguridad, además se logró mejorar el proceso para gestionar las vulnerabilidades. Por último, la empresa en estudio solicitó su apoyo para realizar diagnósticos de manera periódica.(Bolaños González, Cruz Cuellar y Reyes Peñaloza 2018)

Hernandez (2016) Es un software para escanear en busca de vulnerabilidades. Nessus y Nessusd son sus dos partes constituyentes. El daemon de Nessus, conocido como "Nessusd", está a cargo de ejecutar el análisis en el sistema de destino, y "nessus" es el cliente basado en la consola gráfica que muestra el estado y los resultados del análisis. Se puede escanear un rango de 16 direcciones IPS utilizando la versión Home de este software gratuito, que también administra las ediciones Nessus Professional

y Nessus Manager. los dos últimos tienen una licencia que se paga.(Hernandez Hernandez 2016)

Defaz, Salazar (2020) La centralita IP se integra con la red telefónica pública y proporciona comunicación VoIP dentro y fuera de la oficina. Isabel fue diseñada para brindar una alta capacidad de llamadas simultáneas utilizando la infraestructura de red actual. Al interconectar sucursales en ubicaciones remotas a través de Internet, puede mantener sucursales remotas en otra ciudad o país y, al mismo tiempo, reducir drásticamente los costos de comunicación entre ellas. Mediante la instalación de un Softphone o el uso de adaptadores, esta tecnología también posibilita el uso de computadoras como teléfonos para teléfonos tradicionales. todo lo conectado a su red LAN, incluidos los especiales.(Defaz Parra y Salazar Barrionuevo 2020)

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

El proyecto de investigación fue de tipo aplicada, el nivel de la investigación fue descriptivo. También se puso en práctica los conocimientos adquiridos con la finalidad de aportar el enriquecimiento científico. El diseño de la presente investigación fue no experimental, ámbito demostrativo mediante un trabajo de simulaciones que se realizó basándonos en las tesis y artículos estudiados respecto a la variable objeto de estudio.

3.2. Variables y operacionalización

- **Definición conceptual**

  La variable de estudio que se utilizó para la presente investigación es seguridad VoIP. VoIP para Adhilaksono y Setiawan (2022), son servicios de telefonía a través de Internet, habilitado por combinaciones de tecnologías de comunicación, métodos, protocolos y técnicas de transmisión. Con VoIP, las llamadas de audio se pueden entregar utilizando redes IP como Internet en lugar de una línea telefónica analógica. (Adhilaksono, Setiawan 2022)

- **Definición operacional**

  La variable seguridad VoIP en la telefonía IP se dividió en las siguientes dimensiones: Protección, control de acceso, disponibilidad.

  - **Indicadores**

  El indicador de la dimensión “Protección” fue “Porcentaje promedio de vulnerabilidades por escenario”, de la dimensión “Control de acceso” fue “Porcentaje de Controles según escenario” y la dimensión “Disponibilidad” su indicador fue “Nivel de riesgo de aplicaciones por escenario”.

3.3. Población

Las poblaciones utilizadas fueron las interacciones realizadas según el indicador, a continuación, se detallan: para el indicador “Porcentaje promedio de vulnerabilidades por escenario” su población fue la cantidad de

simulaciones que se realizaron para este indicador, para el indicador “Porcentaje de Controles según escenario” y “Nivel de riesgo de aplicaciones por escenario”, su población también fue la cantidad de interacciones realizadas. Los criterios de exclusión fueron todas las interacciones o simulaciones que se vieron afectadas por factores externos como por ejemplo apagones, error en red, dificultades con el software, dificultades con el rendimiento de laptop. Como criterios de inclusión se tomó en cuenta todas las interacciones o simulaciones que se realizaron en óptimas condiciones sin ningún tipo de interrupción.

3.4. Técnicas e instrumentos de recolección de datos

En la investigación se utilizó, la técnica de observación, esta técnica se utilizó en los siguientes indicadores: Porcentaje promedio de vulnerabilidades por escenario, porcentaje de Controles según escenario, flujos de información y el nivel de riesgo de aplicaciones por escenario. Para esta técnica se utilizó la ficha de observación como instrumento de recolección de datos, posteriormente realizaremos la descripción de los datos obtenidos para la guía de observación.

3.5. Procedimientos

Para los indicadores porcentaje promedio de vulnerabilidades por escenario, porcentaje de controles según escenario y nivel de riesgo de aplicaciones, por escenario utilizamos el software Nessus que nos permitió experimentar distintos niveles de seguridad basado en las tesis y artículos estudiados. En el primer escenario se realizó un escaneo a la empresa simulada número 1 con la finalidad de obtener el porcentaje de vulnerabilidades. En el segundo escenario también se realizó escaneo a la empresa simulada número 2 con la finalidad de obtener el porcentaje de controles. Y por último se escaneo la empresa simulada número 3 con finalidad de identificar el nivel se seguridad. Los resultados de estos indicadores se midieron en la ficha de observación, posteriormente se representaron en el software SPSS.

3.6. Método de análisis de datos

Para la recolección de datos de los indicadores: Porcentaje promedio de vulnerabilidades por escenario, porcentaje de controles según escenario y nivel de riesgo de aplicaciones por escenario, utilizamos el software llamado NESSUS, este permitió analizar el porcentaje o la cantidad de vulnerabilidades encontradas en las 3 empresas simuladas. Los datos obtenidos se representaron como estadística descriptiva en el software SPSS.

3.7. Aspectos éticos

El grupo de investigación garantiza que las simulaciones realizadas se desarrollaron en un ambiente controlado, en el cual se aseguró que no afecte la naturaleza. La investigación utilizó datos de manera interna. Nuestra investigación cumplió correctamente con las citas y referencias de los antecedentes y teorías, ya que se menciona de manera correcta los autores, la fecha y el lugar de publicación de las mismas, guiándonos al reglamento establecido por la Universidad César Vallejo. Finalmente se aseguró la originalidad del proyecto de investigación, esto se validó utilizando el software Turnitin.

IV. RESULTADOS

En la presente investigación se trabajó con estadística descriptiva. Para lograr que se cumplan los objetivos planteados se utilizaron diferentes softwares para facilitar la investigación, estos fueron:

- **Virtual Box**

  Romero (2019) Es una herramienta muy dinámica que le permite construir varios mundos virtuales, desde simulación de software hasta simulación de hardware. Actualmente se utilizan ampliamente para la simulación de redes inteligentes, gestión de servidores, etc.(Romero Flores 2019)

- **Tenable Nessus**

  Hernandez (2016) Es un software para escanear vulnerabilidades. Es un escáner muy completo, es el más utilizado.(Hernandez Hernandez 2016)

- **Issabel**

  Defaz, Salazar (2020) Es un software de servidor de comunicaciones unificadas que combina funciones IP PBX, correo, mensajería instantánea, fax y otras tareas cooperativas. Tiene una interfaz web y opciones de centro de llamadas disponibles.(Defaz Parra y Salazar Barrionuevo 2020)

Para realizar la investigación se aseguró que los softwares mencionados estén correctamente instalados y funcionales.

Variable: seguridad VoIP en la telefonía IP

Para poder realizar el proceso de análisis de los indicadores de la variable, se aplicó escaneos de vulnerabilidades con la herramienta o software Nessus. Estos escaneos se aplicaron a tres empresas simuladas, cada una de estas 3 empresas se configuraron aleatoriamente, para ser más exactos se denominó las empresas con los nombres de las recomendaciones para mejorar la seguridad VoIP. EMPRESA 1 = UIT-T X.805, EMPRESA 2 = ISO/IEC 27002 y EMPRESA 3 = NIST. Para un mayor orden tomamos el escaneo de cada empresa como escenario.

OE1: determinar las características de seguridad según la protección VoIP.

Indicador: Porcentaje promedio de vulnerabilidades por escenario.

Para el primer indicador se tomó como referencia los 3 escenarios mencionados. Al utilizar Nessus para escaneo arrojó la siguiente cantidad de vulnerabilidades:

Empresa 1: 80% de vulnerabilidad

- IP: 50
- Máscara de Subred: 0
- Gateway: 16
- DNS Primario: 10
- DNS Secundario: 10

Empresa 2: 80% de vulnerabilidad

- IP: 5
- Máscara de Subred: 0
- Gateway: 15
- DNS Primario: 9
- DNS Secundario: 10

Empresa 3: 40% de vulnerabilidad

- IP: 0
- Máscara de Subred: 0
- Gateway: 0
- DNS Primario: 8
- DNS Secundario: 11

Al culminar este primer indicador, arrojó el porcentaje de vulnerabilidad de la Empresa 1 y 2 fue alto mientras que la Empresa 3 tuvo un 40% lo que indica que es mejor pero que aún puede ser vulnerada.

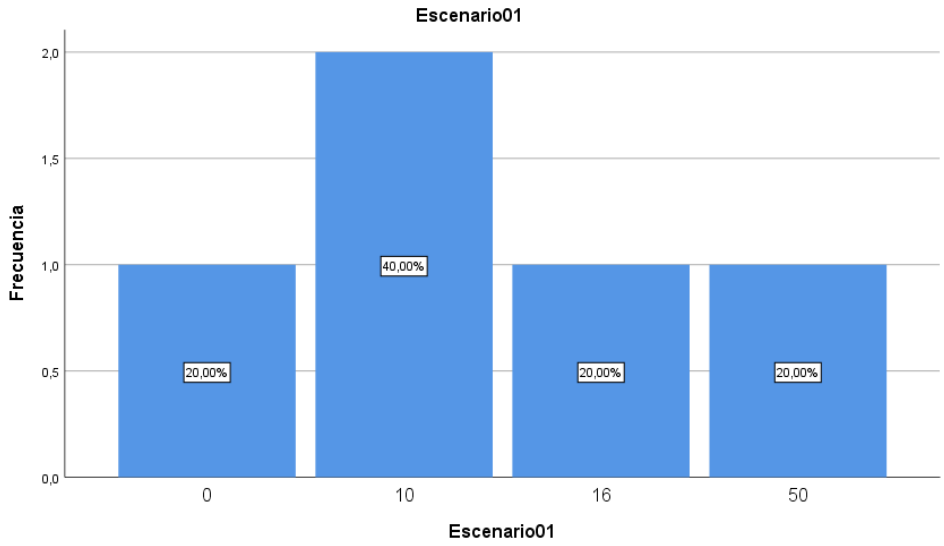


Figura 3. Indicador 01 del escenario 01 de la empresa simulada 1

Descripción: El grafico 01 del indicador 01 podemos observar la frecuencia de la cantidad de vulnerabilidades

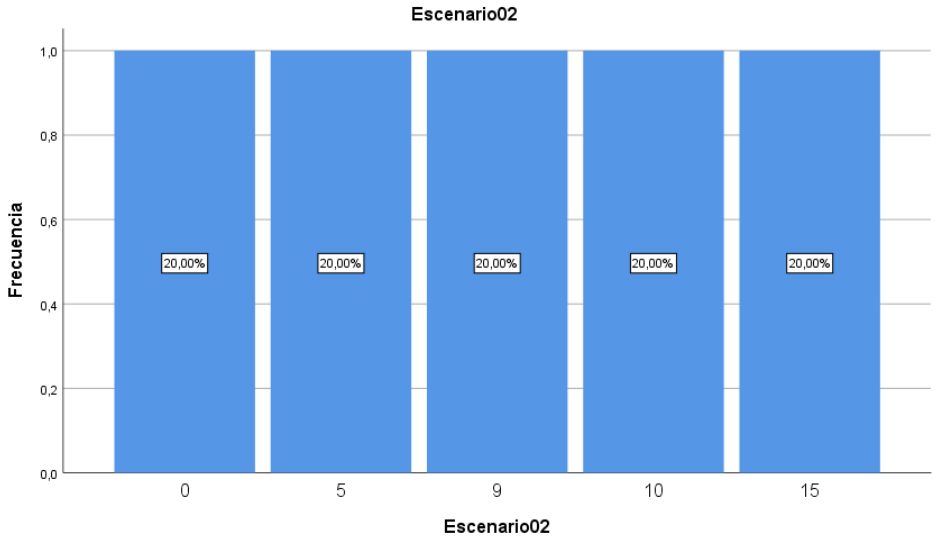


Figura 4. Indicador 01 del escenario 02 de la empresa simulada 2

Descripción: El grafico 02 del indicador 01 podemos observar la frecuencia de la cantidad de vulnerabilidades

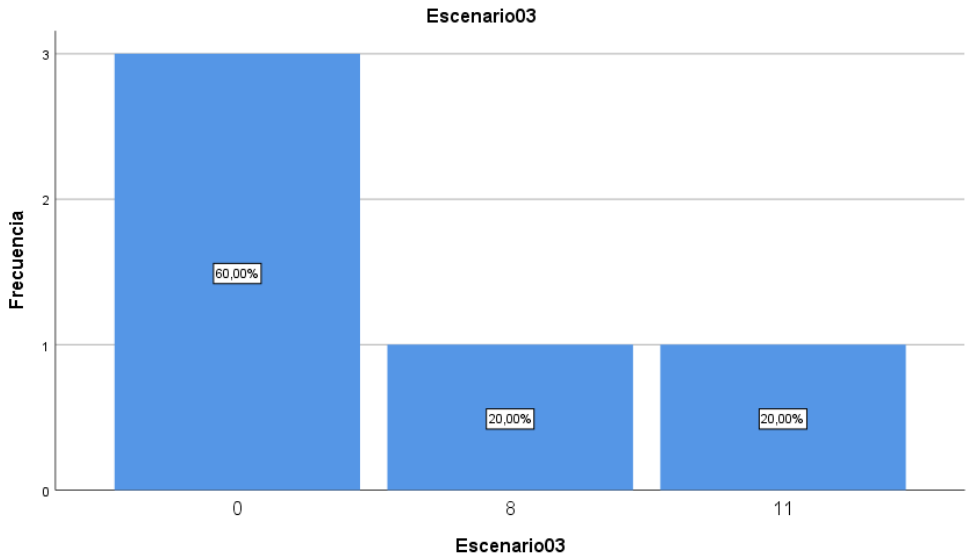


Figura 5. Indicador 01 del escenario 03 de la empresa simulada 3

Fuente: Propia del autor

Descripción: El grafico 03 del indicador 01 podemos observar la frecuencia de la cantidad de vulnerabilidades

OE2: Determinar el nivel de seguridad según el control de acceso VoIP.

Indicador: Porcentaje de Controles según escenario.

Para el segundo indicador se tomó como referencia los 3 escenarios mencionados.

Al utilizar Nessus para escaneo arrojó la siguiente cantidad de soluciones:

Empresa 1: 80% soluciones

- IP: 40
- Mascara de Subred: 0
- Gateway: 11
- DNS Primario: 6
- DNS Secundario: 6

Empresa 2: 80% soluciones

- IP: 2
- Mascara de Subred: 0
- Gateway: 10
- DNS Primario: 6
- DNS Secundario: 6

Empresa 3: 40% soluciones

- IP: 0
- Mascara de Subred: 0
- Gateway: 0
- DNS Primario: 9
- DNS Secundario: 19

Al culminar este segundo indicador observamos que la cantidad de soluciones el alto lo cual indicó que habría una probabilidad que se dé solución a las vulnerabilidades.

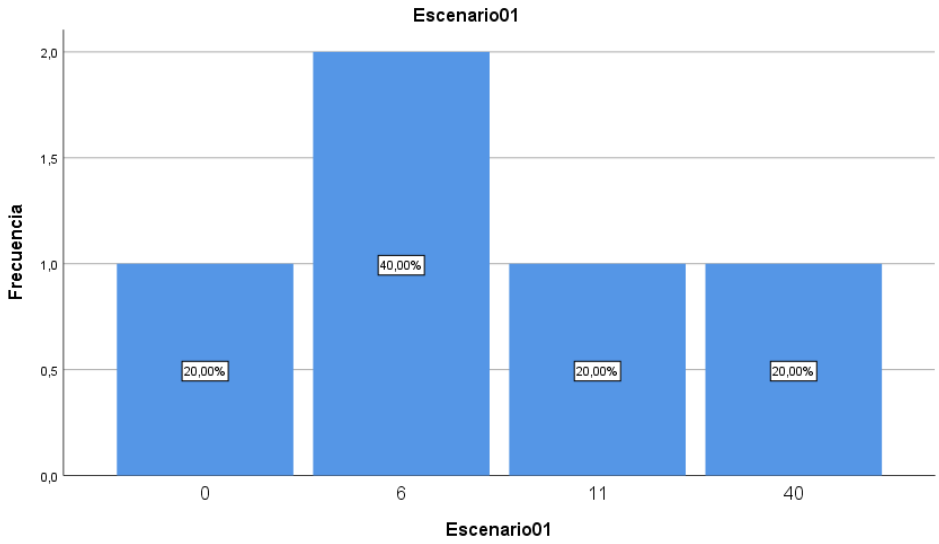


Figura 6. Indicador 02 del escenario 01 de la empresa simulada 1

Descripción: El grafico 01 del indicador 2 podemos observar la frecuencia de la cantidad de soluciones y también su porcentaje.

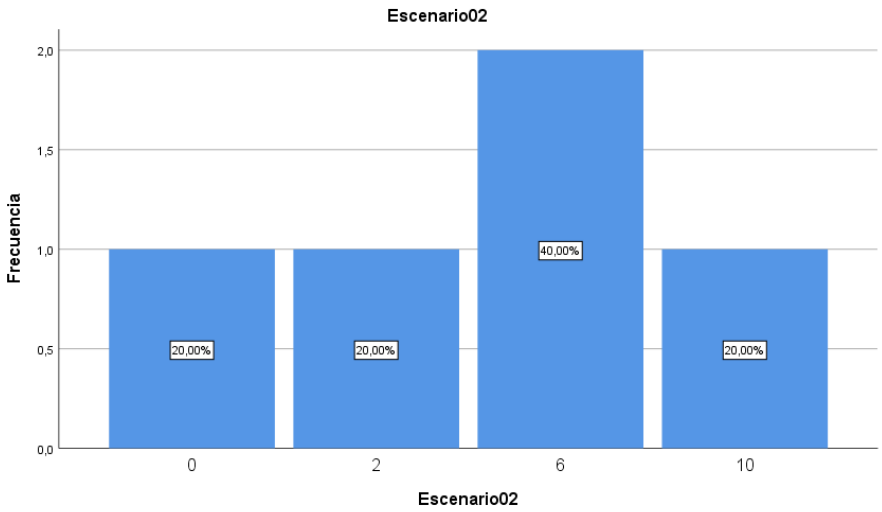


Figura 7. Indicador 02 del escenario 02 de la empresa simulada 2

Descripción: El grafico 02 del indicador 2 podemos observar la frecuencia de la cantidad de soluciones y también su porcentaje

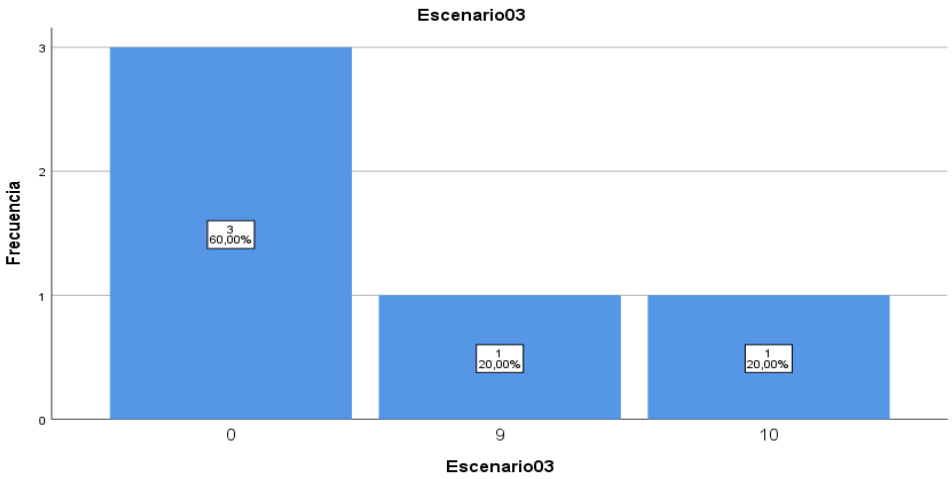


Figura 8. Indicador 02 del escenario 03 de la empresa simulada 3

Descripción: El grafico 03 del indicador 2 podemos observar la frecuencia de la cantidad de soluciones y también su porcentaje

OE3: determinar el nivel de seguridad según la disponibilidad VoIP.

Indicador: Nivel de riesgo de aplicaciones por escenario.

Para el tercer indicador se tomó como referencia los 3 escenarios mencionados. Al utilizar Nessus para escaneo arrojó la siguiente cantidad de vulnerabilidades y los niveles de riesgo:

Tabla 1. *Indicador 03 del escenario 01*

	Niveles de puntuación CVSS 3				
	NINGUNO	**BAJO**	**MEDIO**	**ALTO**	**CRÍTICO**
	0.0	**0.1 - 3.9**	**4.0 - 6.9**	**7.0 - 8.9**	**9.0 - 10.0**
IP	120	2	12	0	3
Máscara De Subred	0	0	0	0	0
Gateway	18	1	2	0	0
DNS Primario	10	0	1	1	0
DNS Secundario	10	0	1	1	0

Fuente: elaboración propia

Tabla 2. *Indicador 03 del escenario 02*

	Niveles de puntuación CVSS 3				
	NINGUNO	**BAJO**	**MEDIO**	**ALTO**	**CRÍTICO**
	0.0	**0.1 - 3.9**	**4.0 - 6.9**	**7.0 - 8.9**	**9.0 - 10.0**
IP	5	0	0	0	0
Máscara De Subred	0	0	0	0	0
Gateway	18	1	1	0	0
DNS Primario	9	0	1	1	0
DNS Secundario	10	0	1	1	0

Fuente: elaboración propia

Tabla 3. *Indicador 03 del escenario 03*

	Niveles de puntuación CVSS 3				
	NINGUNO	**BAJO**	**MEDIO**	**ALTO**	**CRÍTICO**
	0.0	**0.1 - 3.9**	**4.0 - 6.9**	**7.0 - 8.9**	**9.0 - 10.0**
IP	0	0	0	0	0
Máscara De Subred	0	0	0	0	0
Gateway	0	0	0	0	0
DNS Primario	21	0	1	1	0
DNS Secundario	20	2	1	1	0

Fuente: elaboración propia

V. DISCUSIÓN

La seguridad VoIP es parte fundamental para el desarrollo o la buena implementación de la telefonía IP en una empresa. Es por este motivo que este trabajo de investigación se planteó realizar un análisis de la seguridad VoIP en la telefonía IP, con la finalidad de determinar las características de la seguridad VoIP. Para poder realizar este análisis se plantean 3 objetivos específicos, estos fueron: Determinar las características de seguridad según la protección VoIP; determinar el nivel de seguridad según el control de acceso VoIP y por último determinar el nivel de seguridad según la disponibilidad VoIP.

Para realizar este análisis primero se tomó como referencia 3 recomendaciones de seguridad para sistemas de comunicación como lo es VoIP, estas son: UIT-T X.805, ISO/IEC 27002, NIST, también se simularon 3 empresas con una configuración distinta para cada una, esto lo realizamos para tener un mayor orden en la ejecución de los escenarios. Para poder analizar y escanear la seguridad de cada una de estas empresas simuladas se utilizó el Software Nessus, los datos que nos arrojó se recopilaron en fichas de observación.

Los resultados obtenidos tienen relación con las tesis o artículos que fueron seleccionados como antecedentes.

Para el objetivo específico 1, determinar las características de seguridad según la protección VoIP, utilizamos el software Nessus para analizar la seguridad de las 3 empresas ficticias, este análisis arrojó que la empresa número 1 se encontraron un total de 86 vulnerabilidades, obteniendo un 80% de vulnerabilidad, en la empresa número 2 se encontraron un total de 39, obteniendo también un 80% de vulnerabilidad y por último en la empresa número 3 se encontraron 19, obteniendo un 40% de vulnerabilidad, lo que quiere decir que la configuración realizada en el ámbito simulado en cada empresa tuvo vulnerabilidades altas según la escala de medición del software Nessus. Este análisis indicó de manera precisa el número exacto de vulnerabilidades y el detalle de cada una de ellas por empresa. De esta manera se determinó características necesarias para la protección de VoIP. El autor Franco Romero Gustavo Armando (2019), en su investigación “Análisis de

vulnerabilidades de seguridad en sistemas de VoIP, con el uso de herramientas de hacking ético - 2019", realizó un análisis a un servidor en la cual arrojó 36 vulnerabilidades, el cual corresponde a un 78%. Gracias a este resultado pudo determinar qué características debería tener el servicio para elevar la protección VoIP. El concluye que gracias al análisis realizado pudo encontrar de manera precisa las vulnerabilidades, lo cual ayuda a incrementar la protección de la seguridad. De la misma manera el autor. Espinoza Araujo, Christian Omar (2020), en su investigación para fin de grado titulada "Implementación de Ethical Hacking para Mejorar la Gestión de Riesgos en los Sistemas Informáticos de la Municipalidad Provincial de Moyobamba", realizó el análisis de vulnerabilidades de los servicios de la municipalidad, en el cual llegó a encontrar 35 vulnerabilidades lo cual ayudó a determinar los mecanismos y características que debería la municipalidad para la protección de la seguridad.

Para el objetivo específico número 2, Determinar las características de la seguridad VoIP según el control de accesos, nuevamente se utilizó Nessus. Este software muy aparte de detectar las vulnerabilidades también da las soluciones, lo cual es de gran ayuda puesto que mejoraría la seguridad VoIP. En este análisis se detectó que hay gran cantidad de soluciones, en la empresa simulada número 1 se encontraron un total de 63 soluciones, obteniendo un 80% de control de accesos, en la empresa número 2 se encontraron un total de 24 soluciones, obteniendo también un 80% de control de accesos y por último en la empresa simulada número 3 se encontraron 19. Parte importante del hallazgo de las soluciones, es tomar acción y ejecutarlas, de esta manera poder controlar las vulnerabilidades y mejorar los accesos. María Eugenia Cotto Soliz (2019) en su investigación titulada "Estudio de Medidas y Protocolos de Seguridad en las Redes Informáticas del UPC (Unidad de Policía Comunitaria) de la Parroquia Barreiro - 2019", encontró 2 soluciones a las vulnerabilidades que arrojó Nessus, ella afirma que saber cuáles son los errores y sus soluciones es de gran importancia para que los atacantes no tengan facilidad para infiltrarse en sus servicios. también confirma en base a sus resultados que conocer las soluciones ayuda a reducir el nivel riesgo de seguridad. Asimismo,

Bolaños, Cruz y Reyes (2018), en su investigación “Identificación y propuesta de una solución de mejora a las vulnerabilidades informáticas de la red y del ambiente de servidores de preproducción de la entidad KERALTY”, realizan un análisis a los servidores, de un total de 178 tomaron como objeto de estudio 14 servidores. En el análisis se encontraron un total de 87 soluciones, esto permitió identificar los puntos débiles de sus servidores con lo cual propusieron un plan para su mejora. Ellos concluyen la importancia del escaneo para poder reconocer las vulnerabilidades para darle solución rápida, debido a que puede ser perjudicial para la empresa.

Para el objetivo específico número 3, determinar el nivel de seguridad según la disponibilidad VoIP también se utilizó el software Nessus para analizar las 3 empresas simuladas, este software utiliza el CVSS (sistema de puntuación de vulnerabilidad común) para indicar el nivel de impacto o nivel de riesgo que puede tener cada vulnerabilidad encontrada. Este sistema de puntuación mide en 5 niveles: ninguno, bajo, medio, alto y crítico. Se logró encontrar en la empresa 1 un total de 158 vulnerabilidades que no tuvieron impacto alguno, también se encontraron 3 en nivel bajo, 16 en nivel medio, 2 en nivel alto y 3 en nivel crítico. En la empresa número 2 se encontró 42 vulnerabilidades que no tuvieron impacto alguno, también se encontró 1 vulnerabilidad en nivel bajo, 3 en nivel medio y 2 en nivel alto. En la empresa número 3 se encontró 41 vulnerabilidades que no tuvieron impacto, también se encontraron 2 en nivel bajo, nivel medio y alto. Con este análisis se pudo determinar qué nivel de seguridad tenía cada empresa según CVSS. De la misma manera los autores Eche Pingo, Jorge Luis y Lizano Mendoza, Anyi Exmit (2022), en su tesis “Implementación de seguridad de la información para mejorar la gestión de riesgos de TI en la Municipalidad de Sechura. 2022“, lograron identificar vulnerabilidades y riesgos informáticos, en su análisis realizado con el software Nessus, se encontró 7 vulnerabilidades en nivel crítico, 13 en nivel alto, 7 en nivel medio y 1 de nivel bajo. De esta manera ellos lograron determinar el nivel de seguridad que tenía la empresa estudiada. Así mismo Sergio Llorens Muñoz (2022), en su investigación para fin de grado titulada “Análisis e investigación en ataques de vulnerabilidades con Nessus.", realizó 4 escaneos a 4 máquinas

virtuales en el cual se encontraron una cantidad considerable de vulnerabilidades, en la máquina número 1 encontró 88 vulnerabilidades de nivel crítico, 243 de nivel alto y 44 de nivel medio. En la máquina número 2 encontró 72 vulnerabilidades de nivel crítico, 141 de nivel alto y 16 de nivel medio. En la máquina número 3 encontró 16 vulnerabilidades de nivel crítico, 143 de nivel alto y 31 de nivel medio. Por último, en la máquina número 4 se encontró 35 vulnerabilidades de nivel crítico, 106 de nivel alto y 39 de nivel medio. Ellos concluyen que se debe tener muy en cuenta el nivel de criticidad de las vulnerabilidades porque de esta manera se puede determinar el nivel de seguridad que tienen las empresas.

En la actualidad se puede ver que la mayoría de empresas adquieren un servicio de telefonía IP con tecnología VoIP. Es de suma importancia la presente investigación, debido a que los ciberdelincuentes atacan este tipo de servicios con la finalidad de robar información confidencial. No es algo nuevo que muchas empresas pierdan información muy importante por consecuencia de una mala gestión en la instalación de sus servicios. Otro de los motivos por los cuales se ve afectado es por la falta de seguimiento al funcionamiento de sus servicios. Es importante que las empresas inviertan en un software para poder realizar escaneos de vulnerabilidades o deficiencias en sus servicios, de esta manera por encontrar la solución y ejecutarla, teniendo en cuenta que si no se realiza esta acción a tiempo puede ser muy perjudicial para ellos. La presente investigación es de consideración para prevalecer el análisis de la seguridad VoIP, así lo confirma también el autor Franco Romero (2019) en su investigación ha realizado un análisis de vulnerabilidades afectadas a los sistemas VoIP, Se concluye que el test de análisis de vulnerabilidades a la central telefónica VoIP les ayudó a incrementar los niveles de seguridad, también permitió garantizar de la disponibilidad, confidencialidad e integridad de la comunicación.

VI. CONCLUSIONES

Con respecto al primer objetivo específico, determinar las características de seguridad según la protección VoIP, se logró encontrar en la empresa simulada número 1 un total de 86 vulnerabilidades. En la empresa número 2 se encontraron un total de 39 vulnerabilidades. Por último, en la empresa simulada número 3 se encontraron 19 vulnerabilidades. Luego de analizar los resultados se concluye que en la empresa número 1 el servicio más afectado fue el IP, en la empresa 2 en Gateway y en la empresa 3 en DNS, por lo tanto, se logró determinar las características que debería tener para tener una mejor protección VoIP como por ejemplo entre las más importantes realizar una correcta configuración del servidor SIP, adquirir un certificado SSL y tener los softwares actualizados.

El segundo objetivo específico, determinar el nivel de seguridad según el control de acceso VoIP, se logró encontrar distintas soluciones para las empresas simuladas. En la empresa simulada número 1 arrojó un total de 63 soluciones. En la empresa número 2 se encontraron un total de 24. Por último, en la empresa simulada número 3 se encontraron 19. Con estos resultados se concluye que es posible determinar el nivel de seguridad encontrando las soluciones de las vulnerabilidades, también se concluye que es importante poner en marcha las soluciones encontradas porque de lo contrario podría ser perjudicial para la empresa.

El tercer objetivo específico, determinar el nivel de seguridad según la disponibilidad VoIP, se concluyó que es posible reconocer el nivel de impacto de las vulnerabilidades gracias a Nessus, este software para medir el nivel de riesgos trabaja con el sistema de puntuación CSSV, el cual nos indica qué tan perjudicial se puede ser cada vulnerabilidad. En el escaneo general de la empresa número 1, indicó que tuvo 3 vulnerabilidades de nivel bajo, 16 de nivel medio, 2 de nivel alto y 3 de nivel crítico. En la empresa número 2, indicó que tuvo 1 vulnerabilidad de nivel bajo, 3 de nivel medio, 2 de nivel alto y 0 de nivel crítico. En la empresa número 3 indicó que tuvo 2 vulnerabilidades de nivel bajo, 2 de nivel medio, 2 de nivel alto y 0 de nivel crítico.

VII. RECOMENDACIONES

Se recomienda que toda empresa que desee implementar servicios de telefonía IP con tecnología VoIP, tengan una capacitación previa con expertos, sobre los procesos que se deben realizar para tener una seguridad estable que no perjudique a los usuarios y que tampoco a ellos como empresa.

Se recomienda que después de implementar el servicio se realice un escaneo para analizar las vulnerabilidades que se pueden encontrar. Se sugiere que este escaneo se realice de manera periódica, por ejemplo, una vez al mes. Si es el caso que se encuentren vulnerabilidades, se debe dar solución de manera inmediata para reducir el nivel de riesgo. Es importante que toda empresa, tenga un experto en redes o en el rubro con la finalidad de dar soporte necesario en el caso se requiera.

Se recomienda que las empresas no adquieran servicios de bajo costo, no se debe economizar en este tipo de servicios. Adquirir los servicios de telefonía IP con tecnología VoIP a bajo precio podría ser perjudicial para las empresas debido a que los ciberdelincuentes pueden robar información relevante.

REFERENCIAS BIBLIOGRAFICAS

ADHILAKSONO, Bramantyo y SETIAWAN, Bambang, 2022. A study of Voice-over-Internet Protocol quality metrics. *Procedia Computer Science*. 1 enero de 2022. Vol. 197, pp. 377-384. DOI 10.1016/j.procs.2021.12.153. Disponible en: https://www.sciencedirect.com/science/article/pii/S1877050921023772

ALVARES, Christabelle, DINESH, Dristi, ALVI, Syed, GAUTAM, Tannish, HASIB, Maheen y RAZA, Ali, 2021. Dataset of attacks on a live enterprise VoIP network for machine learning based intrusion detection and prevention systems. *Computer Networks*. octubre 2021. Vol. 197, pp. 108283. DOI 10.1016/j.comnet.2021.108283. Disponible en: https://linkinghub.elsevier.com/retrieve/pii/S1389128621003030

ANRANGO COTACACHI, Wilson Hernán, 2016. Diseño de una red de telefonía IP para el instituto tecnológico superior “17 de julio” sede Yachay. en línea. 2016. [Accedido 16 septiembre 2022]. Recuperado a partir de: http://repositorio.puce.edu.ec:80/handle/22000/13177 Accepted: 2017-06-14T17:31:24Z

ARMANDO, F.R.G., 2019. Análisis de vulnerabilidades de seguridad en sistemas de VoIP, con el uso de herramientas de hacking ético. [en línea], Disponible en: http://repositorio.ug.edu.ec/handle/redug/39259.

AZAD, Muhammad Ajmal, MORLA, Ricardo y SALAH, Khaled, 2018. Systems and methods for SPIT detection in VoIP: Survey and future directions. Computers & Security. 1 agosto 2018. Vol. 77, pp. 1-20. DOI 10.1016/j.cose.2018.03.005. Disponible en: https://linkinghub.elsevier.com/retrieve/pii/S0167404818302414

AZROUR, Mourade, FARHAOUI, Yousef, OUANAN, Mohammed y GUEZZAZ, Azidine, 2019. SPIT Detection in Telephony over IP Using K-Means Algorithm. Procedia Computer Science. 1 enero 2019. Vol. 148, pp. 542-551. DOI 10.1016/j.procs.2019.01.027. Disponible en: https://www.sciencedirect.com/science/article/pii/S1877050919300274

BAHNASSE, A., BADRI, A., LOUHAB, F.E., TALEA, M., KHIAT, A. y PANDEY, B., 2018. Behavior analysis of VoIP performances in next-generation networks. International Journal of Engineering and Technology(UAE). 2018. Vol. 7, no. 3.15 Special Issue 15, pp. 353-359. DOI 10.14419/ijet.v7i2.8.10461. Scopus. Disponible en: https://www.sciencepubco.com/index.php/ijet/article/view/21383

BIONDI, Pietro, BOGNANNI, Stefano y BELLA, Giampaolo, 2020. VoIP Can Still Be Exploited - Badly. En: *2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*. en línea. abril 2020. pp. 237-243. DOI 10.1109/FMEC49853.2020.9144875. Disponible en: https://ieeexplore.ieee.org/document/9144875

BOLAÑOS GONZÁLEZ, H., CRUZ CUELLAR, J.M. y REYES PEÑALOZA, J., 2018. Identificación y propuesta de una solución de mejora a las vulnerabilidades informáticas de la red y del ambiente de servidores de preproducción de la entidad Keralty. En: Accepted: 2022-07-08T19:11:42Z [en línea], [consulta: 5 julio 2023]. Disponible en: https://repositorio.unbosque.edu.co/handle/20.500.12495/8143.

BUÑAY, Pamela, PASTOR, Danilo, PAGUAY, Paúl, MORENO, Samuel, BUÑAY, Pamela, PASTOR, Danilo, PAGUAY, Paúl y MORENO, Samuel, 2019. Análisis de la Arquitectura DIFFSERV sobre redes MPLS para la provisión de QoS en aplicaciones en tiempo real (VoIP). Revista Digital Novasinergia. mayo 2019. Vol. 2, no. 1, pp. 33-40. DOI 10.37135/unach.ns.001.03.04. Disponible en: http://scielo.senescyt.gob.ec/scielo.php?script=sci_abstract&pid=S2631-26542019000100033&lng=es&nrm=i

CARRILLO-MONDÉJAR, J., MARTINEZ, J. L. y SUAREZ-TANGIL, G., 2022. On how VoIP attacks foster the malicious call ecosystem. Computers & Security. 1 agosto 2022. Vol. 119, pp. 102758. DOI 10.1016/j.cose.2022.102758. Disponible en: https://www.sciencedirect.com/science/article/pii/S0167404822001535

COTTO SOLIZ, M.E., 2019. Estudio de Medidas y Protocolos de Seguridad en las Redes Informáticas del UPC (Unidad de Policía Comunitaria) de la Parroquia Barreiro [en línea]. bachelorThesis. S.l.: BABAHOYO. [consulta: 27 junio 2023]. Disponible en: http://dspace.utb.edu.ec/handle/49000/5597.

DEFAZ PARRA, K.A. y SALAZAR BARRIONUEVO, D.S., 2020. “Implementación de una central telefónica voz IP utilizando software libre Issabel PBX y comunicaciones unificadas basado en Asterisk en la constructora MA Construcciones”. [en línea]. bachelorThesis. S.l.: Ecuador: Latacunga: Universidad Técnica de Cotopaxi (UTC). [consulta: 5 julio 2023]. Disponible en: http://repositorio.utc.edu.ec/handle/27000/8609.

DIJKSTRA, F., ANDREE, B., KOYMANS, K., y VAN DER HAM, JEROEN, 2007. Introduction to ITU-T Recommendation G.805. Disponible en: https://jvdham.nl/research/publications/0507-G805-introduction.pdf.

ECHE PINGO, J.L. y LIZANO MENDOZA, A.E., 2023. Implementación de seguridad de la información para mejorar la gestión de riesgos de TI en la Municipalidad de Sechura. 2022. En: Accepted: 2023-05-02T22:45:55Z, Repositorio Institucional - UCV [en línea], [consulta: 27 junio 2023]. Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/112908.

ESPINOZA ARAUJO, C.O., 2020. Implementación de Ethical Hacking para mejorar la gestión de riesgos en los sistemas informáticos de la Municipalidad Provincial de Moyobamba. En: Accepted: 2020-10-02T19:16:13Z, Repositorio Institucional - UCV [en línea], [consulta: 1 julio 2023]. Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/47290.

ESTRADA, José, CALVA, Mayra, RODRÍGUEZ, Ana, TIPANTUÑA, Christian, ESTRADA, José, CALVA, Mayra, RODRÍGUEZ, Ana y TIPANTUÑA, Christian, 2016. Security of IP Telephony in Ecuador: Online Analysis. Enfoque UTE. junio 2016. Vol. 7, no. 2, pp. 25-40. DOI 10.29019/enfoqueute.v7n2.93. Disponible: http://scielo.senescyt.gob.ec/scielo.php?script=sci_abstract&pid=S1390-65422016000200025&lng=es&nrm=iso&tlng=es

FRANCO ROMERO, G.A., 2019. Análisis de vulnerabilidades de seguridad en sistemas de VoIP, con el uso de herramientas de hacking ético. [en línea], Disponible en: http://repositorio.ug.edu.ec/handle/redug/39259.

GAD, Ahmed Fawzy, 2018. Comparison of signaling and media approaches to detect VoIP SPIT attack. En: 2018 International Conference on Innovative Trends in Computer Engineering (ITCE). febrero 2018. pp. 56-62. DOI 10.1109/ITCE.2018.8316600. Disponible en: https://ieeexplore.ieee.org/abstract/document/8316600

GAONA GARCÍA, Elvis Eduardo, ÁVILA ANGULO, Miguel Antonio y MUSKUS, Elkin Gabriel, 2014. APROXIMACIÓN DE LA CALIDAD DE VOZ Y COBERTURA ENUNA RED GSM DE EMERGENCIA. Ciencia e Ingeniería Neogranadina. julio 2014. Vol. 24, no. 2, pp. 23-36. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_abstract&pid=S0124-81702014000200002&lng=en&nrm=iso&tlng=es

GAVILANEZ, O., RODRIGUEZ, G. y GAVILANEZ, F., 2017. Audit analysis models, security frameworks and their relevance for VoIP. En: Proceedings of the 12th International Conference on Cyber Warfare and Security, ICCWS 2017. 2017. pp. 143-151. Scopus. Disponible en: https://doi.org/10.48550/arXiv.1704.02440

GUAMÁN DEL PINO, Alex Fernando y RUBIO QUINCHUELA, Karen Abigail, 2022. Análisis, implementación y evaluación de un asistente basado en telefonía IP para gestión de archivos e información de documentación para las Carreras del Departamento de Eléctrica, Electrónica y Telecomunicaciones de la ESPE. en línea. 2022. [Accedido 28 septiembre 2022]. Recuperado a partir de: http://repositorio.espe.edu.ec/jspui/handle/21000/28525 Accepted: 2022-02-22T16:21:06Z

HERNANDEZ HERNANDEZ, A., 2016. Análisis de vulnerabilidades informáticas en una red de datos privada: División de Ciencias e Ingeniería, un caso de estudio. En: Accepted: 2018-06-25T17:43:27Z [en línea], [consulta: 5 julio 2023]. Disponible en: http://risisbi.uqroo.mx/handle/20.500.12249/1235.

ISLAM, Faiz Ul, LIU, Guangjie, ZHAI, Jiangtao y LIU, Weiwei, 2021. VoIP Traffic Detection in Tunneled and Anonymous Networks Using Deep Learning. *IEEE Access*. 2021. Vol. 9, pp. 59783-59799. DOI 10.1109/ACCESS.2021.3073967. Disponible en: https://ieeexplore.ieee.org/document/9406580

JAPA ÁVILA, L.I., 2019. Revisión sistemática de literatura: análisis de la seguridad informática en los sistemas VoIP. [en línea]. bachelorThesis. S.l.: Loja:Universidad Nacional de Loja. [consulta: 27 junio 2023]. Disponible en: https://dspace.unl.edu.ec//handle/123456789/22516.

KAMAS, S. y AYDIN, M.A., 2017. SPIT detection and prevention. Istanbul University - Journal of Electrical and Electronics Engineering, vol. 17, ISSN 1303-0914. Scopus. Disponible en: https://electricajournal.org/en/spit-detection-and-prevention-13690.

KHAN, Hafiz Muhammad Ashja, INAYAT, Usman, ZIA, Muhammad Fahad, ALI, Fahad, JABEEN, Taila y ALI, Syed Moshin, 2021. Voice Over Internet Protocol: Vulnerabilities and Assessments. En: 2021 International Conference on Innovative Computing (ICIC). noviembre 2021. pp. 1-6. DOI 10.1109/ICIC53490.2021.9692955. Disponible en: https://ieeexplore.ieee.org/document/9692955

KILINÇ, H. Hakan y ÇAĞAL, Uğur, 2017. Detecting VoIP fuzzing attacks by using a honeypot system. En: 2017 25th Signal Processing and Communications Applications Conference (SIU). mayo 2017. pp. 1-4. DOI 10.1109/SIU.2017.7960190. Disponible en: https://ieeexplore.ieee.org/document/7960190.

LLORENS MUÑOZ, S., 2022. Análisis e investigación en ataques de vulnerabilidades con Nessus. En: Accepted: 2023-05-29T16:16:31Z [en línea], [consulta: 1 julio 2023]. Disponible en: https://ebuah.uah.es/dspace/handle/10017/57074.

MAHESWARI, K., BALAMURUGAN, A., CHARLYN PUSHPA LATHA, G. y RAMKUMAR, S., 2021. Performance analysis of VoIP codecs in interactive streaming data environment. Materials Today: Proceedings. en línea. 23 febrero 2021. [Accedido 19 septiembre 2022]. DOI 10.1016/j.matpr.2021.01.225. Disponible en: https://www.sciencedirect.com/science/article/pii/S221478532100314X

MAHN, A., MARRON, J., QUINN, S. y TOPPER, D., 2022. Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide (Spanish Translation). [en línea]. S.l.: National Institute of Standards and Technology. [consulta: 1 julio 2023]. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271es.pdf.

MAMANI BAUTISTA, Fernando, 2017. Implementación de telefonia IP para Laboratorios COFAR. en línea. [Accedido 16 septiembre 2022]. Recuperado a partir de: http://repositorio.umsa.bo/xmlui/handle/123456789/15766 Accepted: 2018-05-09T20:14:58Z.

MANUNZA, L., MARSEGLIA, S. y ROMANO, S. P., 2017. Kerberos: A real-time fraud detection system for IMS-enabled VoIP networks. *Journal of Network and Computer Applications*. 15 febrero 2017. Vol. 80, pp. 22-34. DOI 10.1016/j.jnca.2016.12.018. Diponible en: https://www.sciencedirect.com/science/article/pii/S1084804516303228

OLANO DÍAZ, Juan Daniel y SÁNCHEZ AGUILAR, Segundo Román, 2017. “Desarrollo de un Sistema de Telefonía IP y Videovigilancia que permita agilizar y mejorar la comunicación y seguridad entre las diferentes áreas de la Municipalidad Distrital de la Victoria- 2016”. . 2017. pp. 250. disponible en: https://repositorio.unprg.edu.pe/handle/20.500.12893/2122

PINCAY AYÓN, Yuri Adrián, 2018. “DISEÑO E IMPLEMENTACIÓN DE UN MODELO DIDÁCTICO PARA LAS PRÁCTICAS DE TELEFONÍA IP. en línea. Jipijapa-UNESUM. [Accedido 15 octubre 2022]. Recuperado a partir de: http://repositorio.unesum.edu.ec/handle/53000/1197 Accepted: 2018-05-08T20:46:57Z

ROMERO FLORES, C.R., 2019. Simulador virtual y logro competencias en los alumnos del II semestre de la carrera Soporte y Mantenimiento de Equipos de Computación SENATI Huaraz. En: Accepted: 2019-04-30T20:59:51Z [en línea], [consulta: 5 julio 2023]. Disponible en: https://repositorio.upch.edu.pe/handle/20.500.12866/6546.

SAENGER, Jens, MAZURCZYK, Wojciech, KELLER, Jörg y CAVIGLIONE, Luca, 2020. VoIP network covert channels to enhance privacy and information sharing. Future Generation Computer Systems. 1 octubre 2020. Vol. 111, pp. 96-106. DOI 10.1016/j.future.2020.04.032. Disponible en: https://www.sciencedirect.com/science/article/pii/S0167739X19333965

SANCHEZ ESPINOZA, David Junior, 2021. Diseño e implementación de una central telefónica Voip de bajo costo mediante Asterisk y Raspberry Pi para pequeñas o medianas empresas. en línea. 2021. [Accedido 30 septiembre 2022]. Recuperado a partir de: https://repositorio.uch.edu.pe//handle/20.500.12872/647 Disponible en: 2022-01-11T18:33:12Z

SÁNCHEZ-REYES, Sergio, RIVERO-ÁNGELES, Mario E., TORRES-CRUZ, Noé, SÁNCHEZ-REYES, Sergio, RIVERO-ÁNGELES, Mario E. y TORRES-CRUZ, Noé, 2018. Teletraffic Analysis for VoIP Services in WLAN Systems with Handoff Capabilities. Computación y Sistemas. septiembre 2018. Vol. 22, no. 3, pp. 997-1007. DOI 10.13053/cys-22-3-2749. Disponible en: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-55462018000300997

SCHMIDT, Sabine, MAZURCZYK, Wojciech, KULESZA, Radoslaw, KELLER, Jörg y CAVIGLIONE, Luca, 2018. Exploiting IP telephony with silence suppression for hidden data transfers. Computers & Security. 1 noviembre 2018. Vol. 79, pp. 17-32. DOI 10.1016/j.cose.2018.08.006. Disponible en: https://www.sciencedirect.com/science/article/pii/S0167404818305777

UIT-T X.805, 2003. X.805: Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo. [en línea]. [consulta: 1 julio 2023]. Disponible en: https://www.itu.int/rec/T-REC-X.805-200310-I/es.

VENNILA, Ganesan, MANIKANDAN, M. S. K. y SURESH, M. N., 2018. Dynamic voice spammers detection using Hidden Markov Model for Voice over Internet Protocol network. Computers & Security. 1 marzo 2018. Vol. 73, pp. 1-16. DOI 10.1016/j.cose.2017.10.003. Disponible en: https://www.sciencedirect.com/science/article/pii/S0167404817302080

VESGA-FERREIRA, Juan Carlos, GRANADOS-ACUÑA, Gerardo y VESGA-BARRERA, José Antonio, 2016. Evaluación del rendimiento de una red LAN sobre Power Line Communications para la transmisión de VoIP. Iteckne. junio 2016. Vol. 13, no. 1, pp. 83-95. Disponible en: http://www.scielo.org.co/scielo.php?pid=S1692-17982016000100010&script=sci_abstract&tlng=es

VILLARREAL, Marco Aurelio Rosario, ARROYO, Janeth Bertha Mariño, CAMARENA, Javier Francisco Márquez, LIRA, Luis Alberto Núñez, VILLARREAL, Marco Aurelio Rosario, ARROYO, Janeth Bertha Mariño, CAMARENA, Javier Francisco Márquez y LIRA, Luis Alberto Núñez, 2019. Evaluación de una red inalámbrica de banda ancha para VoIP. Enfoque UTE. diciembre 2019. Vol. 10, no. 4, pp. 28-44. DOI 10.29019/enfoque.v10n4.513. Disponible en: http://scielo.senescyt.gob.ec/scielo.php?script=sci_abstract&pid=S1390-65422019000400028&lng=pt&nrm=iso

YEH, J.F., LIN, P.C., KUO, M.D. y HSU, Z.H., 2013. Bilateral Waveform Similarity Overlap-and-Add Based Packet Loss Concealment for Voice over IP. Journal of Applied Research and Technology. agosto 2013. Vol. 11, no. 4, pp. 559-567. DOI 10.1016/S1665-6423(13)71563-3. Disponible en: https://www.scielo.org.mx/scielo.php?pid=S1665-64232013000400008&script=sci_abstract

ZHANG, Z.-L., KANG, H.J., RANJAN, S. y NUCCI, A., 2018. SIP-Based VoIP Traffic Behavior Profiling and Its Applications. En: *VoIP Handbook: Applications, Technologies, Reliability, and Security*. en línea. pp. 187-206. ISBN 978-1-4200-7021-7. Recuperado a partir de: https://www.scopus.com/record/display.uri?eid=2-s2.0-85137498692&origin=resultslist&sort=plf-f&src=s&st1=SIP-Based+VoIP+Traffic+Behavior+Profiling+and+Its+Applications&sid=44f4d9b4108150d85036d567d9487add&sot=b&sdt=b&sl=77&s=TITLE-ABS-KEY%28SIP-Based+VoIP+Traffic+Behavior+Profiling+and+Its+Applications%29&relpos=0&citeCnt=0&searchTerm=Scopus

ANEXOS

Anexo 1: Matriz de operacionalización de variables

VARIABLES DE ESTUDIO	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADORES	ESCALA DE MEDICIÓN	TÉCNICA	CÓMO MEDIRLO O INSTRUMENTO
Seguridad VoIP en la telefonía IP	La variable obtenida es la seguridad VoIP en la telefonía IP. VoIP para Adhilaksono y Setiawan (2022),son servicios de telefonía a través de Internet, habilitado por combinaciones de tecnologías de comunicación, métodos, protocolos y técnicas de transmisión. Con VoIP, las llamadas de audio se pueden entregar utilizando redes IP como Internet en lugar de una línea telefónica analógica. (Adhilaksono, Setiawan 2022)	La variable seguridad VoIP se dividirá en las siguientes dimensiones: contraseñas y llamadas.	Protección	Porcentaje promedio de vulnerabilidades por escenario	Razón	Observación	Ficha de Observación
			Control de acceso	Porcentaje de Controles según escenario	Razón	Observación	Ficha de Observación
			Disponibilidad	Nivel de riesgo de aplicaciones por escenario	Razón	Observación	Ficha de Observación

Fuente: Elaboración propia de los autores.

Anexo 2: Matriz de Consistencia

TEMÁTICA	TÍTULO	PROBLEMA	PROBLEMA ESPECÍFICOS	OBJETIVO	OBJETIVOS ESPECÍFICOS
Seguridad VoIP	Análisis de la seguridad VoIP en la telefonía IP	¿Cómo identificar el nivel de seguridad de VoIP?	¿Cómo identificar el nivel de características de la seguridad según la protección VoIP?	Determinar las características de la seguridad VoIP	Determinar las características de seguridad según la protección VoIP
			¿Cómo identificar el nivel de seguridad según el control de acceso VoIP?		Determinar el nivel de seguridad según el control de acceso VoIP

			¿Cómo identificar el nivel de seguridad según la disponibilidad de VoIP?		Determinar el nivel de seguridad según la disponibilidad VoIP

Fuente: Elaboración propia de los autores.

Anexo 3: Indicadores de variables

OBJETIVO ESPECÍFICO	INDICADOR	DESCRIPCIÓN	TÉCNICA / INSTRUMENTO	TIEMPO EMPLEADO	MODO DE CÁLCULO
Determinar las características de seguridad según la protección voip	Porcentaje promedio de vulnerabilidades por escenario	Se representa el porcentaje de vulnerabilidades por escenario.	observación / ficha de observación	3 semanas	estadística descriptiva
Determinar el nivel de seguridad según el control de acceso voip	Porcentaje de controles según escenario	Se representa el porcentaje de soluciones por escenario.	observación / ficha de observación	3 semanas	estadística descriptiva
Determinar el nivel de seguridad según la disponibilidad voip	Nivel de riesgo de aplicaciones por escenario	Se representa el impacto o riesgo de las vulnerabilidades.	observación / ficha de observación	3 semanas	estadística descriptiva

Fuente: Elaboración propia de los autores.

Anexo 04: Instrumento de recolección de datos – Ficha de observación I

Ficha de registro de protección					
Investigadores		- De La Cruz Garcia Julian Jesus - Alvarez Núñez Cristhian Enmanuel		**Tipo de prueba**	No experimental
Objetivo específico		Determinar las características de la seguridad VoIP según el control de accesos			
Dimensión de estudio		Protección			
Fecha de inicio			**Fecha final**		
Variable	**Indicador**				
Seguridad VoIP en la telefonía IP	Porcentaje promedio de vulnerabilidades por escenario				
ITEMS	**Escenario**	**Elementos de la red**	**Servicios de red**	**Vulnerabilidades (cantidad)**	**% de Vulnerabilidad**
1	**Empresa 1**	Servidor virtual	IP	50	80,00%
	UIT-T X.805	Router	Máscara De Subred	0	
		Zoiper	Gateway	16	
		Linphone	DNS Primario	10	
		Computadora	DNS Secundario	10	
2	**Empresa 2**	Servidor virtual	IP	5	80,00%
	ISO/IEC 27002	Router	Máscara De Subred	0	
		Computadora	Gateway	15	
			DNS Primario	9	
			DNS Secundario	10	
3	**Empresa 3**	Servidor virtual	IP	0	40,00%
	NIST	Router	Máscara De Subred	0	
		Computadora	Gateway	0	
			DNS Primario	8	
			DNS Secundario	11	

Fuente: Elaboración propia de los autores.

Anexo 05: Instrumento de recolección de datos – Ficha de observación II

Ficha de registro de control de acceso					
Investigadores		- De La Cruz Garcia Julian Jesus - Alvarez Núñez Cristhian Enmanuel		**Tipo de prueba**	No experimental
Objetivo específico		Determinar las características de la seguridad VoIP según el control de accesos			
Dimensión de estudio		Control de acceso			
Fecha de inicio			**Fecha final**		
Variable	**Indicador**				
Seguridad VoIP en la telefonía IP	Porcentaje de Controles según escenario				
ITEMS	**Escenario**	**Elementos de la red**	**Servicios de red**	**Cantidad de soluciones**	**% de Controles según escenario (cantidad)**
1	**Empresa 1**	Servidor virtual	IP	40	80,00%
	UIT-T X.805	Router	Máscara De Subred	0	
		Zoiper	Gateway	11	
		Linphone	DNS Primario	6	
		Computadora	DNS Secundario	6	
2	**Empresa 2**	Servidor virtual	IP	2	80,00%
	ISO/IEC 27002	Router	Máscara De Subred	0	
		Computadora	Gateway	10	
			DNS Primario	6	
			DNS Secundario	6	
3	**Empresa 3**	Servidor virtual	IP	0	40,00%

	NIST	Router	Máscara De Subred	0	
		Computadora	Gateway	0	
			DNS Primario	9	
			DNS Secundario	10	

Fuente: Elaboración propia de los autores.

Anexo 06: Instrumento de recolección de datos – Ficha de observación III

Ficha de registro de disponibilidad								
Investigadores				- De La Cruz Garcia Julian Jesus - Alvarez Núñez Cristhian Enmanuel		**Tipo de prueba**	No experimental	
Objetivo específico				Identificar el nivel de seguridad según la disponibilidad VoIP				
Dimensión de estudio				Disponibilidad				
Fecha de inicio					**Fecha final**			
Variable	**Indicador**							
Seguridad VoIP en la telefonía IP	Nivel de riesgo de aplicaciones por escenario							
ITEMS	**Escenario**	**Elementos de la red**	**Servicios de red**	**Niveles de puntuación CVSS 3**				
				NINGUNO	**BAJO**	**MEDIO**	**ALTO**	**CRITICO**
				0.0	**0.1 - 3.9**	**4.0 - 6.9**	**7.0 - 8.9**	**9.0 - 10.0**
1	**Empresa 1**	Servidor virtual	IP	120	2	12	0	3
	UIT-T X.805	Router	Máscara De Subred	0	0	0	0	0
		Zoiper	Gateway	18	1	2	0	0
		Linphone	DNS Primario	10	0	1	1	0
		Computadora	DNS Secundario	10	0	1	1	0
2	**Empresa 2**	Servidor virtual	IP	5	0	0	0	0
	ISO/IEC 27002	Router	Máscara De Subred	0	0	0	0	0
		Computadora	Gateway	18	1	1	0	0
			DNS Primario	9	0	1	1	0
			DNS Secundario	10	0	1	1	0
3	**Empresa 3**	Servidor virtual	IP	0	0	0	0	0

	NIST	Router	Máscara De Subred	0	0	0	0	0
		Computadora	Gateway	0	0	0	0	0
			DNS Primario	21	0	1	1	0
			DNS Secundario	20	2	1	1	0

Fuente: Elaboración propia de los autores.

Anexo 7: Validez y confiabilidad N°1 – Ficha de observación I.

Castillo Jiménez Iván Michell
Dr. en Tecnología de la Información y Comunicaciones

I. DATOS GENERALES

Apellidos y Nombres del Experto:
Título y/o Grado Académico:

Doctor (X) **Magister ( )** **Ingeniero ( )** **Licenciado ( )** **Otro ( )**.....

Universidad que labora:	Universidad César Vallejo
Fecha:	22/06/2023

TESIS: Análisis de la seguridad VoIP en la telefonía IP

Autores: De La Cruz Garcia, Julian Jesus y Alvarez Núñez, Cristhian Enmanuel

Deficiente (0-20%) **Regular (21-50%)** **Bueno (51-70%)** **Muy Bueno (71-80%)** **Excelente (81-100%)**

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACION				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				80	
OBJETIVIDAD	Esta expresado en conducta observable.					90
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				70	
ORGANIZACION	Existe una organización lógica.					90
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				70	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					100
CONSISTENCIA	Está basado en aspectos teóricos y científicos.				80	
COHERENCIA	En los datos respecto al indicador.				80	
METODOLOGIA	Responde al propósito de investigación.				80	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					90
	TOTAL				460	370

III. PROMEDIO DE VALIDACIÓN

83%

IV. OPCION DE APLICABILIDAD

(X) El instrumento puede ser aplicado, tal como está elaborado

( ) El instrumento debe ser mejorado antes de ser aplicado

FIRMA DEL EXPERTO

Anexo 8: Validez y confiabilidad N°1 – Ficha de observación II

Castillo Jiménez Iván Michell
Dr. en Tecnología de la Información y Comunicaciones

I. DATOS GENERALES

Apellidos y Nombres del Experto:
Título y/o Grado Académico:

Doctor (X) **Magister ( )** **Ingeniero ( )** **Licenciado ( )** **Otro ( )**.....

Universidad que labora:	Universidad César Vallejo
Fecha:	**21/06/2023**

TESIS: Análisis de la seguridad VoIP en la telefonía IP

Autores: De La Cruz Garcia, Julian Jesus y Alvarez Núñez, Cristhian Enmanuel

Deficiente (0-20%) **Regular (21-50%)** **Bueno (51-70%)** **Muy Bueno (71-80%)** **Excelente (81-100%)**

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACION				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				80	
OBJETIVIDAD	Esta expresado en conducta observable.				80	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				70	
ORGANIZACION	Existe una organización lógica.					90
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				70	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					100
CONSISTENCIA	Está basado en aspectos teóricos y científicos.				70	
COHERENCIA	En los datos respecto al indicador.					90
METODOLOGIA	Responde al propósito de investigación.				80	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					90
	TOTAL				450	370

III. PROMEDIO DE VALIDACIÓN

82%

IV. OPCION DE APLICABILIDAD

(x) El instrumento puede ser aplicado, tal como está elaborado

( ) El instrumento debe ser mejorado antes de ser aplicado

FIRMA DEL EXPERTO

Anexo 9: Validez y confiabilidad N°1 – Ficha de Observación III.

Castillo Jiménez Iván Michell
Dr. en Tecnología de la Información y Comunicaciones

I. DATOS GENERALES

Apellidos y Nombres del Experto:
Título y/o Grado Académico:

Doctor (X) **Magister ( )** **Ingeniero ( )** **Licenciado ( )** **Otro ( )**.....

Universidad que labora:	Universidad César Vallejo
Fecha:	**21/06/2023**

TESIS: Análisis de la seguridad VoIP en la telefonía IP

Autores: De La Cruz Garcia, Julian Jesus y Alvarez Núñez, Cristhian Enmanuel

Deficiente (0-20%) **Regular (21-50%)** **Bueno (51-70%)** **Muy Bueno (71-80%)** **Excelente (81-100%)**

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACION				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				80	
OBJETIVIDAD	Esta expresado en conducta observable.				80	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				70	
ORGANIZACION	Existe una organización lógica.				80	
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				70	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					100
CONSISTENCIA	Está basado en aspectos teóricos y científicos.					90
COHERENCIA	En los datos respecto al indicador.					95
METODOLOGIA	Responde al propósito de investigación.				80	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					95
	TOTAL				460	380

III. PROMEDIO DE VALIDACIÓN

84%

IV. OPCION DE APLICABILIDAD

(X) El instrumento puede ser aplicado, tal como está elaborado

( ) El instrumento debe ser mejorado antes de ser aplicado

FIRMA DEL EXPERTO

Anexo 10: Validez y confiabilidad N°2 – Ficha de Observación I.

Correa Calle Teófilo Roberto
Mg en Ingeniería de Sistemas con Mención en Tecnología de la Información y Comunicación e Ingeniero de Sistemas

I. DATOS GENERALES

Apellidos y Nombres del Experto: Correa Calle Teófilo Roberto

Título y/o Grado Académico: Maestro en dirección y gestión de las TIC

Doctor ( ) **Magister (X)** **Ingeniero ( )** **Licenciado ( )** **Otro ( )**.....

Universidad que labora:	Universidad César Vallejo
Fecha:	**21/06/2023**

TESIS: Análisis de la seguridad VoIP en la telefonía IP

Autores: De La Cruz Garcia, Julian Jesus y Alvarez Núñez, Cristhian Enmanuel

Deficiente (0-20%) **Regular (21-50%)** **Bueno (51-70%)** **Muy Bueno (71-80%)** **Excelente (81-100%)**

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACION				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				80	
OBJETIVIDAD	Esta expresado en conducta observable.				80	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					90
ORGANIZACIÓN	Existe una organización lógica.				80	
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				80	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80	
CONSISTENCIA	Está basado en aspectos teóricos y científicos.			70		
COHERENCIA	En los datos respecto al indicador.				80	
METODOLOGÍA	Responde al propósito de investigación.				80	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				80	
	TOTAL			70	640	90

III. PROMEDIO DE VALIDACIÓN

(70%+640%+90%)/10=80%

IV. OPCIÓN DE APLICABILIDAD

(X) El instrumento puede ser aplicado, tal como está elaborado

( ) El instrumento debe ser mejorado antes de ser aplicado

FIRMA DEL EXPERTO

Anexo 11: Validez y confiabilidad N°2 – Ficha de Observación II.

Correa Calle Teófilo Roberto
Mg en Ingeniería de Sistemas con Mención en Tecnología de la Información y Comunicación e Ingeniero de Sistemas

I. DATOS GENERALES

Apellidos y Nombres del Experto: Correa Calle Teófilo Roberto

Título y/o Grado Académico: Maestro en dirección y gestión de las TIC

Doctor ( ) **Magister (X)** **Ingeniero ( )** **Licenciado ( )** **Otro ( )**.....

Universidad que labora:	Universidad César Vallejo
Fecha:	**21/06/2023**

TESIS: Análisis de la seguridad VoIP en la telefonía IP

Autores: De La Cruz Garcia, Julian Jesus y Alvarez Núñez, Cristhian Enmanuel

Deficiente (0-20%) **Regular (21-50%)** **Bueno (51-70%)** **Muy Bueno (71-80%)** **Excelente (81-100%)**

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACION				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				**80**	
OBJETIVIDAD	Esta expresado en conducta observable.				**80**	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					**90**
ORGANIZACIÓN	Existe una organización lógica.				**80**	
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				**80**	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				**80**	
CONSISTENCIA	Está basado en aspectos teóricos y científicos.			**70**		
COHERENCIA	En los datos respecto al indicador.				**80**	
METODOLOGÍA	Responde al propósito de investigación.				**80**	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				**80**	
	TOTAL			**70**	**640**	**90**

III. PROMEDIO DE VALIDACIÓN

(70%+640%+90%)/10=80%

IV. OPCIÓN DE APLICABILIDAD

(X) El instrumento puede ser aplicado, tal como está elaborado

( ) El instrumento debe ser mejorado antes de ser aplicado

Anexo 12: Validez y confiabilidad N°2 – Ficha de Observación III.

Correa Calle Teófilo Roberto
Mg en Ingeniería de Sistemas con Mención en Tecnología de la Información y Comunicación e Ingeniero de Sistemas

I. DATOS GENERALES

Apellidos y Nombres del Experto: Correa Calle Teófilo Roberto

Título y/o Grado Académico: Maestro en dirección y gestión de las TIC

Doctor ( ) **Magister (X)** **Ingeniero ( )** **Licenciado ( )** **Otro ( )**.....

Universidad que labora:	Universidad César Vallejo
Fecha:	**21/06/2023**

TESIS: Análisis de la seguridad VoIP en la telefonía IP

Autores: De La Cruz Garcia, Julian Jesus y Alvarez Núñez, Cristhian Enmanuel

Deficiente (0-20%) **Regular (21-50%)** **Bueno (51-70%)** **Muy Bueno (71-80%)** **Excelente (81-100%)**

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACION				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				**80**	
OBJETIVIDAD	Esta expresado en conducta observable.				**80**	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					**90**
ORGANIZACIÓN	Existe una organización lógica.				**80**	
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				**80**	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				**80**	
CONSISTENCIA	Está basado en aspectos teóricos y científicos.			**70**		
COHERENCIA	En los datos respecto al indicador.				**80**	
METODOLOGÍA	Responde al propósito de investigación.				**80**	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				**80**	
	TOTAL			**70**	**640**	**90**

III. PROMEDIO DE VALIDACIÓN

(70%+640%+90%)/10=80%

IV. OPCIÓN DE APLICABILIDAD

(X) El instrumento puede ser aplicado, tal como está elaborado

( ) El instrumento debe ser mejorado antes de ser aplicado

FIRMA DEL EXPERTO

Anexo 13: Validez y confiabilidad N°3 – Ficha de Observación I.

Carlos De La Cruz García
Ing. Electrónica y telecomunicaciones

I. DATOS GENERALES

Apellidos y Nombres del Experto:
Título y/o Grado Académico:

Doctor ( ) Magister ( ) Ingeniero (X) Licenciado ( ) Otro ( ).....

Universidad que labora:	Universidad César Vallejo
Fecha:	22/06/2023

TESIS: Análisis de la seguridad VoIP en la telefonía IP

Autores: De La Cruz Garcia, Julian Jesus y Alvarez Núñez, Cristhian Enmanuel

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACION				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				80	
OBJETIVIDAD	Esta expresado en conducta observable.					90
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				80	
ORGANIZACION	Existe una organización lógica.					90
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				75	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					100
CONSISTENCIA	Está basado en aspectos teóricos y científicos.				80	
COHERENCIA	En los datos respecto al indicador.				80	
METODOLOGIA	Responde al propósito de investigación.				80	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					90
	TOTAL				475	370

III. PROMEDIO DE VALIDACIÓN

84.5%

IV. OPCION DE APLICABILIDAD

(X) El instrumento puede ser aplicado, tal como está elaborado

(|) El instrumento debe ser mejorado antes de ser aplicado

FIRMA DEL EXPERTO

Anexo 14: Validez y confiabilidad N°3 – Ficha de Observación II.

Carlos De La Cruz García
Ing. Electrónica y Telecomunicaciones

I. DATOS GENERALES

Apellidos y Nombres del Experto:
Título y/o Grado Académico:

Doctor () **Magister ( )** **Ingeniero (x)** **Licenciado ( )** **Otro ( )**.....

Universidad que labora:	Universidad César Vallejo
Fecha:	**21/06/2023**

TESIS: Análisis de la seguridad VoIP en la telefonía IP

Autores: De La Cruz Garcia, Julian Jesus y Alvarez Núñez, Cristhian Enmanuel

Deficiente (0-20%) **Regular (21-50%)** **Bueno (51-70%)** **Muy Bueno (71-80%)** **Excelente (81-100%)**

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACION				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				80	
OBJETIVIDAD	Esta expresado en conducta observable.				80	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				75	
ORGANIZACION	Existe una organización lógica.					95
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				70	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					100
CONSISTENCIA	Está basado en aspectos teóricos y científicos.				75	
COHERENCIA	En los datos respecto al indicador.					90
METODOLOGIA	Responde al propósito de investigación.				80	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					90
	TOTAL				460	375

III. PROMEDIO DE VALIDACIÓN

83.5%

IV. OPCION DE APLICABILIDAD

(x) El instrumento puede ser aplicado, tal como está elaborado

( ) El instrumento debe ser mejorado antes de ser aplicado

FIRMA DEL EXPERTO

Anexo 15: Validez y confiabilidad N°3 – Ficha de Observación III.

Carlos De La Cruz García
Ing. Electrónica y Telecomunicaciones

I. DATOS GENERALES

Apellidos y Nombres del Experto:
Título y/o Grado Académico:

Doctor (X) **Magister ( )** **Ingeniero ( )** **Licenciado ( )** **Otro ( )**.....

Universidad que labora:	Universidad César Vallejo
Fecha:	21/06/2023

TESIS: Análisis de la seguridad VoIP en la telefonía IP

Autores: De La Cruz Garcia, Julian Jesus y Alvarez Núñez, Cristhian Enmanuel

Deficiente (0-20%) **Regular (21-50%)** **Bueno (51-70%)** **Muy Bueno (71-80%)** **Excelente (81-100%)**

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				85	
OBJETIVIDAD	Esta expresado en conducta observable.				80	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				75	
ORGANIZACION	Existe una organización lógica.				80	
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				75	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					100
CONSISTENCIA	Está basado en aspectos teóricos y científicos.					95
COHERENCIA	En los datos respecto al indicador.					95
METODOLOGIA	Responde al propósito de investigación.				85	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					95
	TOTAL				480	380

III. PROMEDIO DE VALIDACIÓN

86%

IV. OPCION DE APLICABILIDAD

(X) El instrumento puede ser aplicado, tal como está elaborado

( ) El instrumento debe ser mejorado antes de ser aplicado

FIRMA DEL EXPERTO

Anexo 16: Check List de Verificación

CHECK LIST PARA MEJORAR EL NIVEL DE SEGURIDAD DE SERVICIO DE TELEFONIA IP CON VOIP		
EMPRESA:		
ENCARGADO :		
ITEM	**PASOS A VERIFICAR**	**CUMPLE**
1	**Configure el servidor SIP** Instalación: para comenzar, instale Asterisk en su servidor siguiendo las instrucciones en el sitio web oficial de Asterisk. Asegúrese de que todas las dependencias requeridas estén instaladas. Asterisk controla su funcionamiento utilizando una variedad de archivos de configuración. "Sip .conf" y "Extensions .conf" son los archivos principales. El directorio "/etc/asterisk" es donde encontrará estos archivos. Utilice un editor de texto para ver estos archivos. sorbo. configuración conf: Usted define sus usuarios SIP y su configuración en el archivo "sip . conf"	
2	**Adquiera o genere un certificado SSL adecuado para este servicio.** Un navegador o servidor intenta conectarse a un sitio web (es decir, un servidor web) protegido mediante certificados SSL. El navegador o servidor solicita que el servidor web se identifique. En respuesta el servidor web envía al navegador o servidor una copia de su certificado SSL. El navegador o servidor evalúa si el certificado SSL es confiable. En caso afirmativo, envía una señal al servidor web. A continuación, el servidor web devuelve un reconocimiento firmado digitalmente para iniciar una sesión cifrada mediante SSL. Los datos cifrados se comparten entre el navegador o servidor y el servidor web.	
3	**Activar el cifrado en modo CTR** Para desactivar el servicio Telnet, los pasos pueden variar según el sistema operativo. Aquí tienes dos enfoques diferentes: Enfoque 1: Desactivar el servicio Telnet en Windows: Presiona las teclas "Win + R" para abrir el cuadro de diálogo "Ejecutar". Escribe "appwiz.cpl" y presiona Enter. Esto abrirá la ventana "Programas y características". En la lista de programas instalados, busca "Cliente Telnet" o "Telnet Client". Haz clic derecho sobre él y selecciona "Desinstalar" o "Cambiar". Sigue las instrucciones en pantalla para completar el proceso de desinstalación. Enfoque 2: Desactivar el servicio Telnet en Linux (específicamente Ubuntu): Abre una terminal. Dependiendo de la distribución de Linux que estés utilizando, ejecuta uno de los siguientes comandos con privilegios de superusuario (por ejemplo, usando sudo): Para distribuciones basadas en Debian/Ubuntu: apt-get remove telnet Para distribuciones basadas en Red Hat/Fedora: yum remove telnet Para distribuciones basadas en SUSE: zypper remove telnet Proporciona tu contraseña de superusuario cuando se te solicite. El comando desinstalará el paquete Telnet y todos sus componentes relacionados.	

4	**Deshabilite el servicio Telnet** Para habilitar SSH en un sistema, los pasos pueden variar según el sistema operativo que estés utilizando. A continuación, te proporcionaré los pasos generales para los sistemas operativos más comunes: **Windows:** Verifica si tienes instalado un cliente SSH. Si no lo tienes, puedes instalar herramientas como PuTTY o OpenSSH for Windows. Una vez que tengas un cliente SSH instalado, puedes abrirlo y configurar la conexión especificando la dirección IP o el nombre de host del servidor SSH al que deseas conectarte. **Linux:** Verifica si el paquete OpenSSH Server está instalado en tu sistema. Si no está instalado, puedes instalarlo usando el administrador de paquetes de tu distribución de Linux. Una vez que OpenSSH Server esté instalado, el servicio se iniciará automáticamente y SSH estará habilitado en tu sistema. Puedes conectarte al servidor SSH utilizando la herramienta de línea de comandos "ssh" seguida de la dirección IP o el nombre de host del servidor. Por ejemplo: ssh usuario@direccion_ip. **macOS:** En macOS, el servidor SSH (OpenSSH) suele estar instalado de forma predeterminada. Para habilitar SSH, debes ir a las "Preferencias del Sistema" y luego seleccionar "Compartir". Asegúrate de marcar la casilla "Acceso remoto" o "Compartir archivos y servicios" y luego hacer clic en "Opciones". Aquí podrás habilitar "Acceso remoto" y seleccionar qué usuarios tendrán permiso para conectarse a través de SSH. Después de habilitar SSH, puedes conectarte al servidor utilizando la herramienta de línea de comandos "ssh" de la siguiente manera: ssh usuario@direccion_ip. Recuerda que una vez que SSH esté habilitado, es importante tomar medidas adicionales para asegurar tu servidor, como utilizar claves de autenticación seguras y desactivar el acceso de root si no es necesario.	
5	**Habilitar SSH** Para habilitar SSH en un sistema, los pasos pueden variar según el sistema operativo que estés utilizando. A continuación, te proporcionaré los pasos generales para los sistemas operativos más comunes: **Windows:** Verifica si tienes instalado un cliente SSH. Si no lo tienes, puedes instalar herramientas como PuTTY o OpenSSH for Windows. Una vez que tengas un cliente SSH instalado, puedes abrirlo y configurar la conexión especificando la dirección IP o el nombre de host del servidor SSH al que deseas conectarte. **Linux:** Verifica si el paquete OpenSSH Server está instalado en tu sistema. Si no está instalado, puedes instalarlo usando el administrador de paquetes de tu distribución de Linux. Una vez que OpenSSH Server esté instalado, el servicio se iniciará automáticamente y SSH estará habilitado en tu sistema. Puedes conectarte al servidor SSH utilizando la herramienta de línea de comandos "ssh" seguida de la dirección IP o el nombre de host del servidor. Por ejemplo: ssh usuario@direccion_ip. **macOS:** En macOS, el servidor SSH (OpenSSH) suele estar instalado de forma predeterminada. Para habilitar SSH, debes ir a las "Preferencias del Sistema" y luego seleccionar "Compartir". Asegúrate de marcar la casilla "Acceso remoto" o "Compartir archivos y servicios" y luego hacer clic en "Opciones". Aquí podrás habilitar "Acceso remoto" y seleccionar qué usuarios tendrán permiso para conectarse a través de SSH. Después de habilitar SSH, puedes conectarte al servidor utilizando la herramienta de línea de comandos "ssh" de la siguiente manera: ssh usuario@direccion_ip. Recuerda que una vez que SSH esté habilitado, es importante tomar medidas adicionales para asegurar tu servidor, como utilizar claves de autenticación seguras y desactivar el acceso de root si no es necesario.	

6	**Restrinja el acceso a su servidor DNS** Para restringir el servidor DNS y limitar el acceso a ciertos usuarios o direcciones IP, puedes seguir los siguientes pasos generales, aunque el proceso exacto puede variar dependiendo del servidor DNS que estés utilizando: Accede a la configuración de tu servidor DNS: Esto puede hacerse a través de un panel de control, una línea de comandos o un archivo de configuración, según el servidor DNS que estés utilizando. Algunos servidores DNS populares son BIND, Microsoft DNS Server, PowerDNS, etc. Identifica las opciones de restricción disponibles: Investiga las opciones de configuración de tu servidor DNS para determinar qué métodos de restricción están disponibles. Algunas de las opciones comunes incluyen listas de acceso (ACL), listas de bloqueo (blacklists), configuración de firewalls, autenticación de clientes, entre otros. Crea una lista de acceso (ACL): Una forma común de restringir el acceso al servidor DNS es utilizar listas de acceso (ACL). Estas listas permiten especificar qué direcciones IP o rangos de IP tienen permiso para hacer consultas al servidor DNS. Puedes permitir o denegar el acceso según tus necesidades. Configura la lista de acceso en el servidor DNS: Una vez que hayas creado la lista de acceso, deberás configurarla en tu servidor DNS. Esto implica agregar la lista de acceso a la configuración del servidor DNS y especificar las reglas que deseas aplicar. Por ejemplo, puedes permitir solo ciertas direcciones IP específicas o bloquear direcciones IP específicas. Guarda y reinicia el servidor DNS: Una vez que hayas realizado los cambios en la configuración del servidor DNS, guarda los cambios y reinicia el servidor DNS para que las nuevas restricciones se apliquen. Es importante destacar que la forma exacta de llevar a cabo estos pasos puede variar según el servidor DNS que estés utilizando. Por lo tanto, te recomendaría consultar la documentación específica del servidor DNS o buscar tutoriales relacionados con tu servidor DNS en particular para obtener instrucciones más detalladas y precisas.	
7	**Restringir el acceso a hosts internos sólo si el servicio está disponible** **Firewall:** Configura un firewall en tu red para controlar el tráfico entrante y saliente. Un firewall permite definir reglas que especifican qué hosts pueden acceder a qué recursos de red. Puedes bloquear o permitir el acceso basado en direcciones IP, puertos o protocolos. Listas de control de acceso (ACL): Las ACL son listas de reglas que se aplican a interfaces de red específicas, como routers o switches. Puedes utilizar ACL para permitir o denegar el tráfico basado en direcciones IP de origen o destino, puertos, protocolos, etc. Segmentación de red: Divide tu red en segmentos más pequeños o subredes. Luego, configura las reglas de acceso entre las subredes para controlar qué hosts pueden comunicarse entre sí. Esto puede hacerse utilizando routers o switches con funcionalidades de enrutamiento o VLAN (redes de área local virtual). Autenticación y autorización: Implementa mecanismos de autenticación y autorización para limitar el acceso a hosts. Por ejemplo, puedes utilizar protocolos como el Protocolo de Autenticación de Línea de Acceso Remoto (RADIUS) o el Protocolo de Inicio de Sesión de Red (NASL) para autenticar y autorizar usuarios antes de que puedan acceder a los recursos de red. VPN (Red Privada Virtual): Utiliza una VPN para crear conexiones seguras y cifradas entre hosts remotos y tu red local. Con una VPN, puedes restringir el acceso a hosts específicos a través de certificados, credenciales de usuario y reglas de firewall. Estas son solo algunas de las medidas que puedes tomar para restringir el acceso a hosts en una red. La mejor opción dependerá de tus requisitos específicos y del equipamiento de red que estés utilizando. Recuerda que es importante mantener tus sistemas y dispositivos actualizados con los últimos parches de seguridad para evitar vulnerabilidades conocidas.	

8	**Restringe las consultas recursivas a los hosts** **Accede a la configuración del servidor DNS**: Esto puede variar según el servidor DNS que estés utilizando. Por ejemplo, si estás utilizando BIND, puedes editar el archivo de configuración named.conf, mientras que en otros servidores DNS puedes utilizar herramientas de administración específicas. Busca la sección que controla las opciones de recursión: En el archivo de configuración, busca la sección que establece las opciones de recursión para el servidor DNS. Esta sección suele estar marcada como options o recursion. **Configura las opciones de recursión:** Dentro de la sección de opciones, deberás establecer las directivas para restringir las consultas recursivas. Aquí tienes algunas opciones comunes: allow-recursion: Define la lista de direcciones IP permitidas para realizar consultas recursivas. Puedes especificar direcciones IP individuales o rangos de direcciones IP. Por ejemplo, puedes usar allow-recursion { localhost; 192.168.0.0/24; }; para permitir consultas recursivas desde localhost y desde la red 192.168.0.0/24. **allow-query-cache:** Esta opción controla qué direcciones IP pueden acceder a la caché de consultas. Puedes configurarla de manera similar a allow-recursion. **recursion no:** Esta opción deshabilita completamente las consultas recursivas en el servidor DNS. Si deseas restringir el acceso a los hosts específicos, puedes omitir esta opción. Guarda y reinicia el servidor DNS: Una vez que hayas realizado los cambios en el archivo de configuración, guárdalo y reinicia el servidor DNS para que los cambios surtan efecto. Es importante tener en cuenta que la configuración exacta puede variar según el servidor DNS que estés utilizando. Te recomiendo consultar la documentación específica del servidor DNS para obtener información más detallada sobre cómo restringir las consultas recursivas en ese entorno particular.	
9	**Desactivar las interfaces IPv4 no utilizadas** Para desactivar las interfaces IPv4 no utilizadas en un sistema operativo, puedes seguir estos pasos generales: Abre el "Panel de control" o la configuración de red de tu sistema operativo. La ubicación exacta puede variar según el sistema operativo que estés utilizando. Busca la opción de "Conexiones de red" o "Red e Internet". Dentro de las conexiones de red, encontrarás una lista de todas las interfaces disponibles en tu sistema. Identifica las interfaces IPv4 que deseas desactivar. Haz clic derecho sobre la interfaz IPv4 que deseas desactivar y selecciona la opción "Propiedades" o "Configuración". Dentro de la configuración de la interfaz, busca la opción que te permita desactivar la interfaz IPv4. Puede haber una casilla de verificación para habilitar o deshabilitar la interfaz. Desmarca la casilla de verificación o selecciona la opción que desactive la interfaz IPv4. Guarda los cambios y cierra la ventana de configuración. Ten en cuenta que estos pasos pueden variar dependiendo del sistema operativo que estés utilizando. Además, ten precaución al desactivar interfaces IPv4, ya que puede afectar la conectividad de tu sistema si se trata de una interfaz necesaria para el funcionamiento de otros dispositivos o servicios.	

10	**Configure el servidor web remoto para utilizar HSTS** Accede al servidor web remoto a través de SSH o mediante otro método de administración remota. Ubica el archivo de configuración del servidor web. El nombre y la ubicación del archivo varían según el servidor web que estés utilizando. Por ejemplo, para Nginx, el archivo de configuración puede ser /etc/nginx/nginx.conf, mientras que para Apache, puede ser /etc/httpd/httpd.conf o /etc/apache2/apache2.conf. Abre el archivo de configuración con un editor de texto. Dentro del archivo de configuración, busca la sección que corresponda a la configuración de los sitios o virtual hosts que deseas proteger con HSTS. Agrega la siguiente directiva en la sección correspondiente: Para Nginx: Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"; Para Apache: Strict-Transport-Security "max-age=31536000; includeSubDomains; preload" Esta directiva indica al navegador que utilice una conexión segura (HTTPS) para acceder al sitio web y establece un período de tiempo (en segundos) durante el cual el navegador recordará utilizar siempre HTTPS. Ten en cuenta que el valor max-age establece la duración en segundos durante la cual el navegador recordará la política HSTS. Puedes ajustar este valor según tus necesidades. La opción includeSubDomains asegura que la política HSTS también se aplique a todos los subdominios del sitio web. La opción preload permite que el sitio web sea incluido en la lista de pre-carga de HSTS en los navegadores, lo que aumenta aún más la seguridad. Guarda los cambios en el archivo de configuración. Reinicia el servidor web para que los cambios surtan efecto.	
11	**Filtre las conexiones entrantes al puerto para que sólo lo utilicen fuentes de confianza.** para filtrar las conexiones entrantes a un puerto específico y permitir solo fuentes de confianza utilizando UFW en sistemas basados en Ubuntu: Instala UFW si no está instalado: sudo apt-get install ufw Habilita UFW: sudo ufw enable Configura UFW para permitir conexiones desde fuentes de confianza al puerto deseado: Ejemplo para el puerto 80 (HTTP): sudo ufw allow from IP1 to any port 80 Agrega reglas adicionales para cada dirección IP o rango de direcciones IP que consideres fuentes de confianza. Aplica las reglas de UFW: sudo ufw reload Recuerda ajustar los comandos según tus necesidades, reemplazando "IP1" con las direcciones IP o rangos correspondientes.	

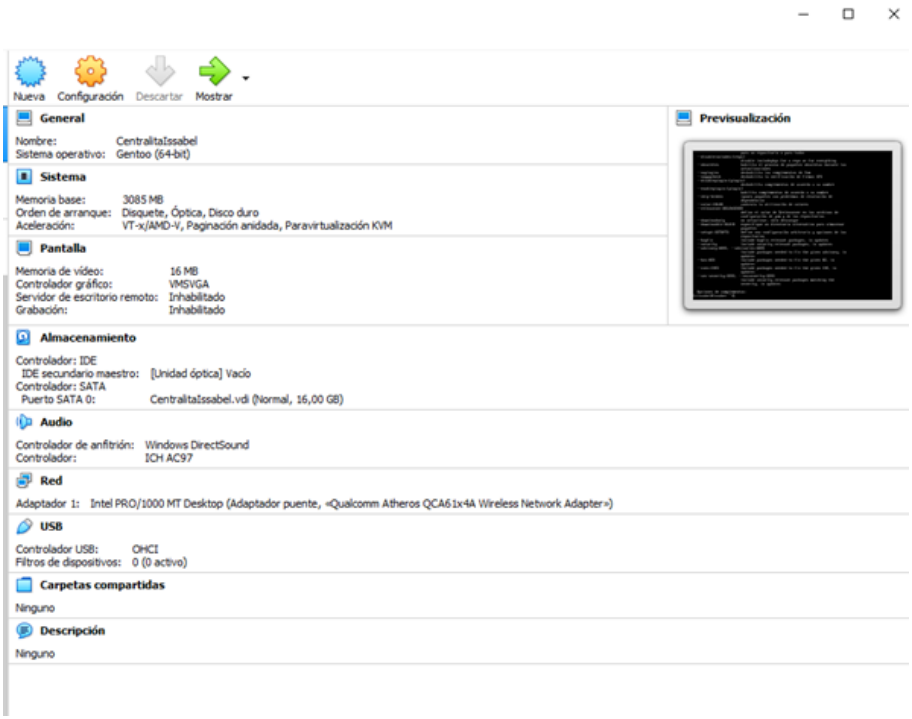
12	**Utiizar filtro IP**	
	Identifica tus necesidades: Determina qué tipo de tráfico deseas permitir o bloquear. Puedes basarte en direcciones IP específicas, rangos de direcciones, puertos, protocolos u otros criterios. Accede al dispositivo de red o firewall: Ingresa al dispositivo de red o software de firewall utilizado en tu entorno. Esto puede ser un enrutador, un switch, un firewall de hardware o un software de seguridad de red. Encuentra la sección de configuración de filtros IP: Busca la sección o función del dispositivo o software que te permite configurar filtros IP. Esto puede variar según el fabricante y el modelo del dispositivo. Crea reglas de filtro IP: Configura reglas para permitir o bloquear el tráfico según tus necesidades. Por ejemplo: Para permitir un rango de direcciones IP, crea una regla que especifique el rango de direcciones que deseas permitir. Para bloquear un puerto específico, crea una regla que indique el número de puerto y la acción de bloqueo. Para permitir un protocolo específico, crea una regla que especifique el protocolo (como TCP, UDP o ICMP) y la acción de permitir. Configura acciones y prioridades: Determina qué acción tomar cuando se cumpla una regla, como permitir o bloquear el tráfico. Además, si hay múltiples reglas que se aplican a un paquete, establece prioridades para definir cuál prevalece. Aplica los cambios: Una vez que hayas configurado tus reglas de filtro IP, guarda los cambios y aplícalos en el dispositivo o software de firewall. Realiza pruebas y monitoreo: Después de aplicar los filtros IP, realiza pruebas para verificar que el tráfico se esté permitiendo o bloqueando según lo esperado. Monitorea el tráfico para asegurarte de que las reglas estén funcionando correctamente y ajusta según sea necesario.	
13	**Creas extensiones en el servidor**	
	Configura el servidor de telefonía IP: Instala y configura un servidor de telefonía IP adecuado para tus necesidades, como Asterisk, FreeSWITCH, 3CX, o cualquier otro software de telefonía IP. Define los requisitos de las extensiones: Determina qué funcionalidades específicas deseas agregar a las extensiones. Esto puede incluir características como llamadas entrantes y salientes, correo de voz, conferencias, transferencias de llamadas, menús interactivos, grabaciones de llamadas, entre otros. Ten claro qué deseas lograr con cada extensión. Configura las extensiones: En el servidor de telefonía IP, configura las extensiones necesarias. Asigna números de extensión únicos y asigna recursos como teléfonos físicos, softphones o dispositivos SIP. Define las reglas de enrutamiento: Establece las reglas de enrutamiento para determinar cómo se manejan las llamadas entrantes y salientes en cada extensión. Puedes configurar reglas basadas en el número marcado, la hora del día, el origen de la llamada, etc. Esto te permitirá dirigir las llamadas a diferentes destinos o aplicar lógica específica según tus necesidades. Implementa las funcionalidades de las extensiones: Utilizando el lenguaje de programación y las herramientas proporcionadas por el servidor de telefonía IP, implementa las funcionalidades deseadas para cada extensión. Esto puede implicar el desarrollo de scripts o programas para manejar las llamadas, interactuar con APIs externas, grabar mensajes de voz o realizar otras acciones específicas. Utiliza la documentación y recursos disponibles para guiar tu desarrollo. Realiza pruebas y depuración: Después de desarrollar las funcionalidades de las extensiones, realiza pruebas exhaustivas para asegurarte de que funcionan correctamente. Simula llamadas y verifica que las funcionalidades se comporten según lo esperado. Realiza la depuración para corregir cualquier error o comportamiento inesperado. Implementa y despliega las extensiones: Una vez que las extensiones hayan pasado las pruebas, implementa y despliega las configuraciones en el servidor de telefonía IP. Asegúrate de que todas las extensiones estén correctamente configuradas y funcionando en el entorno de producción.	

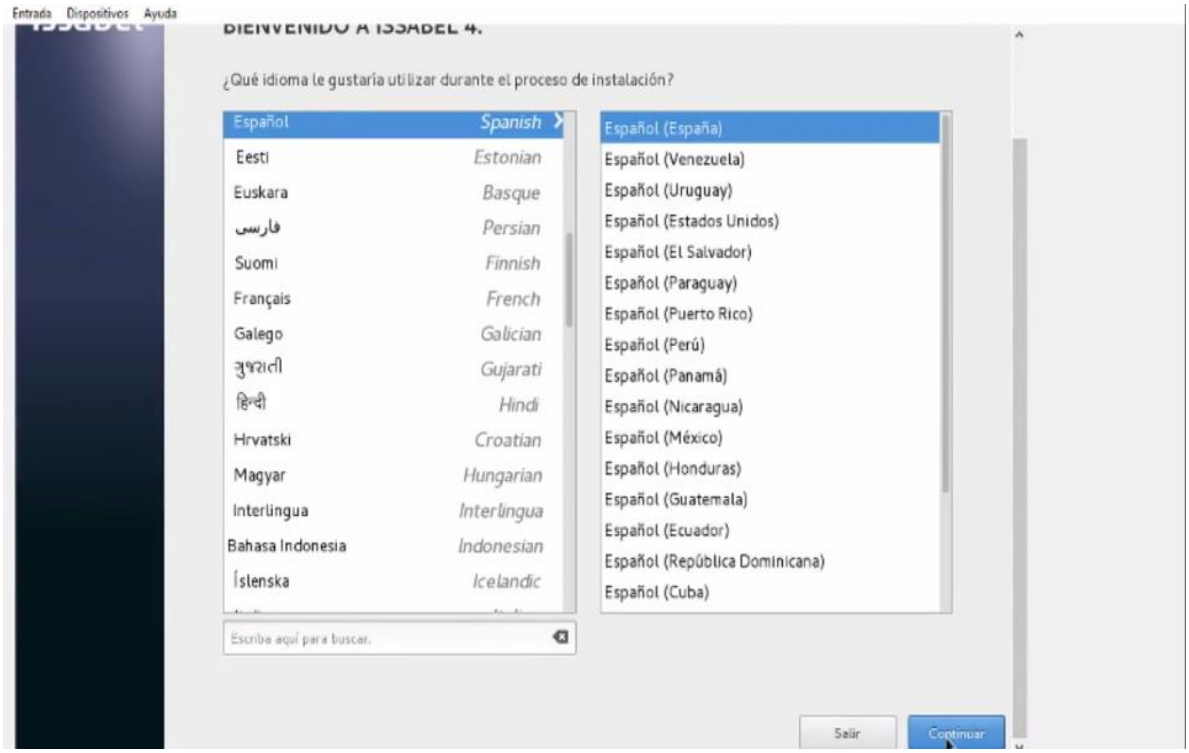
14	**Crear contraseñas robustas (que incluya distintos caracteres) para usuarios**	
	Longitud: Utiliza contraseñas que tengan al menos 12 caracteres. Cuanto más larga sea la contraseña, más difícil será de adivinar o crackear. Complejidad: Mezcla letras (mayúsculas y minúsculas), números, y caracteres especiales (como !, @, #, $, %). Cuanta más variedad de caracteres utilices, más segura será la contraseña. Evita información personal: Evita utilizar información personal obvia, como tu nombre, fecha de nacimiento, nombres de familiares o mascotas, o datos fácilmente accesibles en las redes sociales. Los atacantes pueden obtener esa información fácilmente. Evita secuencias o patrones obvios: No utilices secuencias de teclado como "qwerty" o "123456" ni patrones como "abcd1234" o "abcdabcd". Estos patrones son fáciles de adivinar. Evita contraseñas comunes: No uses contraseñas populares o comunes, como "password", "12345678" o "admin". Estas contraseñas son las primeras que los atacantes probarán. Contraseñas únicas: Utiliza contraseñas diferentes para cada cuenta que tengas. Si un atacante descubre una contraseña, no podrá acceder a todas tus cuentas. Evita información predecible: No utilices palabras del diccionario ni palabras relacionadas con tu tema de interés. Los atacantes utilizan programas que prueban miles de palabras en poco tiempo. Considera utilizar frases: En lugar de una sola palabra, considera utilizar una frase memorable y fácil de recordar. Por ejemplo, "MiPrimerCocheFueUnFordRojo". Actualización periódica: Cambia tus contraseñas regularmente. Es recomendable hacerlo cada 3 a 6 meses para mantener la seguridad de tus cuentas. Utiliza un gestor de contraseñas: Considera utilizar un gestor de contraseñas para generar y almacenar tus contraseñas de forma segura. Los gestores de contraseñas también pueden ayudarte a recordar contraseñas complejas sin tener que anotarlas.	
15	**Utilizar SRTP**	
	Verifica el soporte de SRTP: Asegúrate de que el software o servicio que utilizas para tus comunicaciones admita SRTP. Esto puede incluir clientes VoIP, softphones, gateways, PBXs u otros dispositivos relacionados. Consulta la documentación del proveedor o las especificaciones del software para confirmar si es compatible con SRTP. Configura el software o dispositivo: Accede a la configuración del software o dispositivo que utilizas para tus comunicaciones. Busca las opciones de seguridad o cifrado, donde podrás habilitar SRTP. Puedes encontrar estas configuraciones en la sección de preferencias, configuración de llamadas o configuración de cuentas, dependiendo del software o dispositivo específico que estés utilizando. Genera claves y certificados: Para establecer la seguridad en las comunicaciones SRTP, se requiere el uso de claves y certificados criptográficos. Puedes generar tus propias claves y certificados utilizando herramientas como OpenSSL o utilizar servicios de certificados confiables. Sigue los procedimientos recomendados para generar claves y certificados seguros. Intercambia claves y certificados: Para garantizar la autenticación y seguridad en la comunicación SRTP, debes intercambiar las claves y certificados generados con los demás participantes de la comunicación. Esto puede implicar compartir claves públicas o certificados para establecer una conexión segura entre los extremos. Realiza llamadas seguras: Una vez que hayas configurado SRTP y hayas intercambiado las claves y certificados necesarios, puedes realizar llamadas de voz o video seguras. Asegúrate de que todas las partes involucradas en la comunicación tengan configurado SRTP y estén utilizando claves y certificados válidos.	

16	**Restrinjir las direcciones IP** Si deseas restringir direcciones IP en un entorno de red local, una forma común de hacerlo es a través de la configuración del enrutador. Aquí tienes un método general para restringir direcciones IP en un enrutador: Accede a la configuración del enrutador: Abre un navegador web e ingresa la dirección IP predeterminada del enrutador en la barra de direcciones. Por lo general, la dirección IP es algo como "192.168.0.1" o "192.168.1.1". Consulta el manual del enrutador o comunícate con el fabricante si no estás seguro de la dirección IP. Inicia sesión en el enrutador: Ingresa el nombre de usuario y la contraseña para acceder a la configuración del enrutador. Si no has cambiado estas credenciales, es posible que encuentres las credenciales predeterminadas en el manual del enrutador o en la parte posterior del dispositivo. Encuentra la sección de filtrado de direcciones IP: La ubicación exacta puede variar según el enrutador, pero generalmente encontrarás esta configuración en la sección "Firewall" o "Filtrado". Busca opciones como "Filtrado de direcciones IP" o "Control de acceso". Configura las reglas de restricción de direcciones IP: Una vez que hayas encontrado la sección correspondiente, podrás agregar reglas para restringir direcciones IP. Puedes configurar reglas para bloquear direcciones IP específicas o rangos de direcciones IP. Ingresa la dirección IP que deseas bloquear y guarda la configuración. Aplica los cambios y reinicia el enrutador: Una vez que hayas configurado las reglas de restricción de direcciones IP, guarda los cambios y reinicia el enrutador para que las nuevas configuraciones surtan efecto.	
17	**Conseguir un buen firewall (Meraki, Sonicwall)** Cisco Meraki Firewall: Gestión basada en la nube para una configuración y administración sencillas. Funciones de seguridad avanzadas, como filtrado de contenido, prevención de intrusiones y protección contra malware. Integración con otros dispositivos de red Meraki para una administración más unificada. SonicWall Firewall: Enfoque en la seguridad de red con características como prevención de intrusiones, prevención de amenazas avanzadas y filtrado de contenido. Escalabilidad para adaptarse a diferentes necesidades de rendimiento. Herramientas de gestión centralizada para una configuración y monitoreo más sencillos. Al elegir un firewall, considera factores como el tamaño de tu red, el nivel de seguridad requerido y el presupuesto. Investiga las especificaciones técnicas, las características de seguridad, el soporte técnico y las reseñas de usuarios para tomar una decisión informada. Otras marcas de firewall, como Fortinet, Palo Alto Networks y Check Point, también ofrecen soluciones de seguridad de red que podrías considerar.	

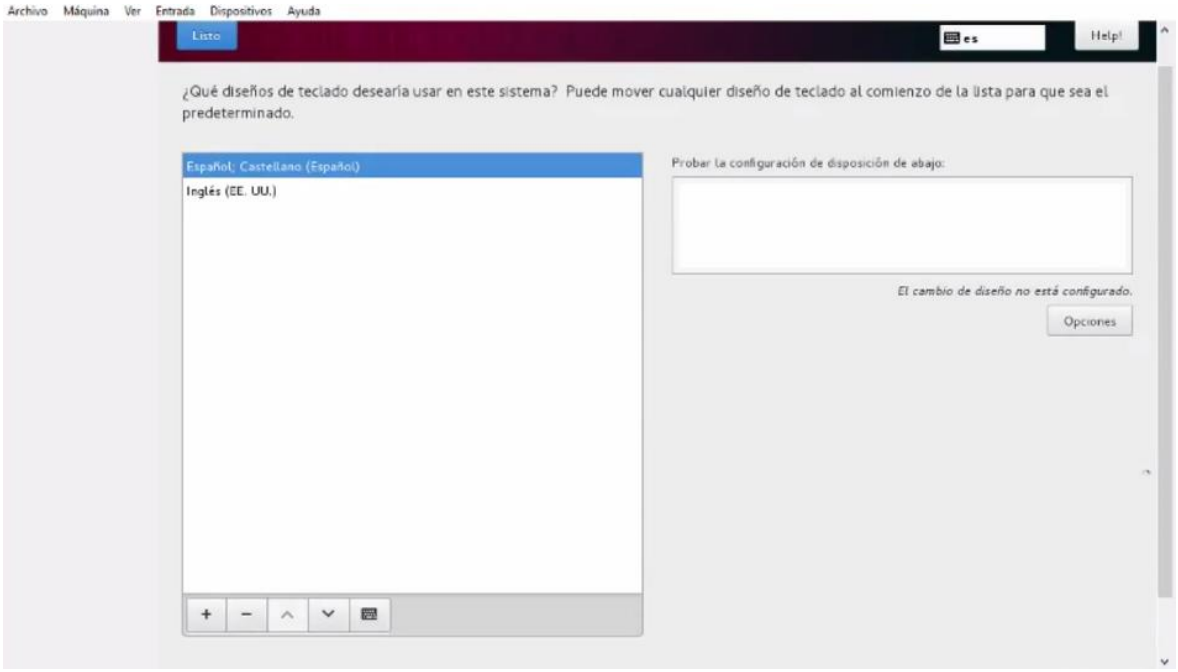
Fuente: Elaboración propia de los autores.

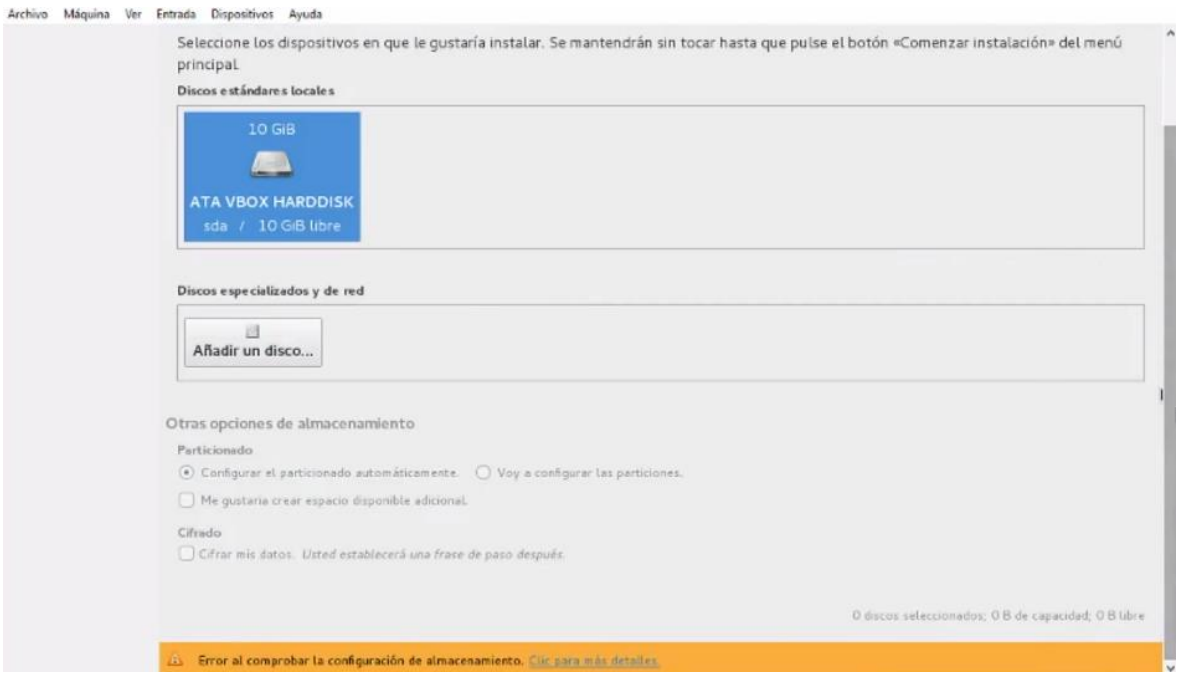
A continuación, se muestra el proceso de instalación de Issabel

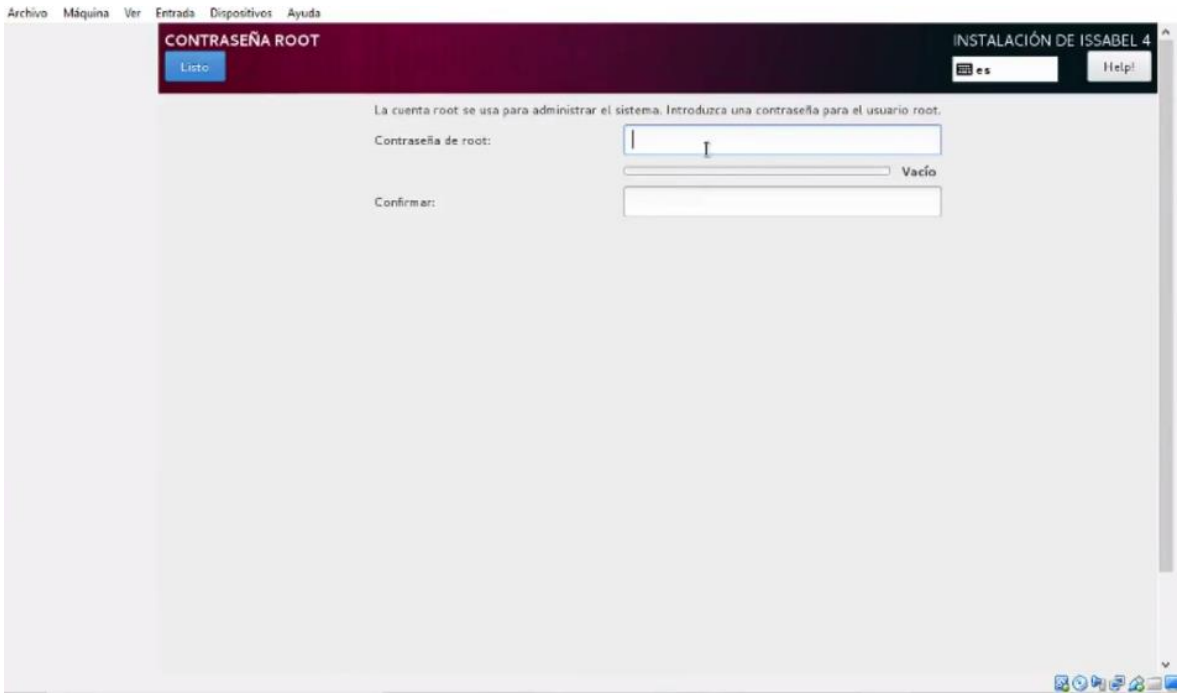


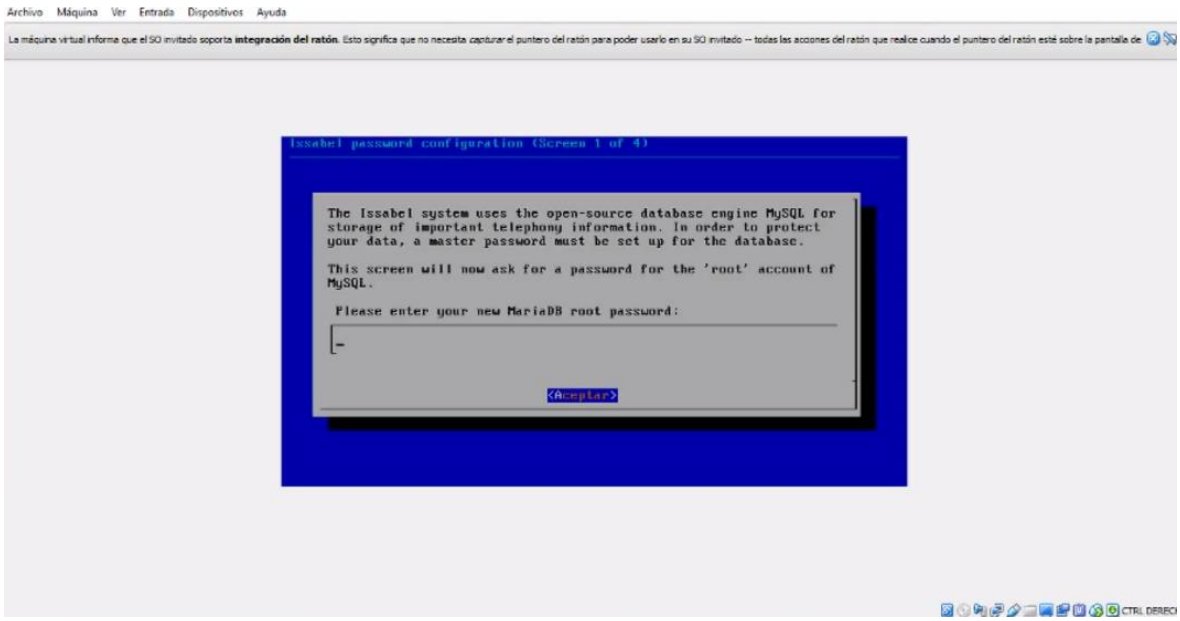

Entrada Dispositivos Ayuda
BIENVENIDO A ISSABEL 4.
¿Qué idioma le gustaría utilizar durante el proceso de instalación?
Español Spanish
Eesti Estonian
Euskara Basque
فارسی Persian
Suomi Finnish
Français French
Galego Galician
ગુજરાતી Gujarati
हिन्दी Hindi
Hrvatski Croatian
Magyar Hungarian
Interlingua Interlingua
Bahasa Indonesia Indonesian
Íslenska Icelandic
Escriba aquí para buscar.
Español (España)
Español (Venezuela)
Español (Uruguay)
Español (Estados Unidos)
Español (El Salvador)
Español (Paraguay)
Español (Puerto Rico)
Español (Perú)
Español (Panamá)
Español (Nicaragua)
Español (México)
Español (Honduras)
Español (Guatemala)
Español (Ecuador)
Español (República Dominicana)
Español (Cuba)
Salir
Continuar

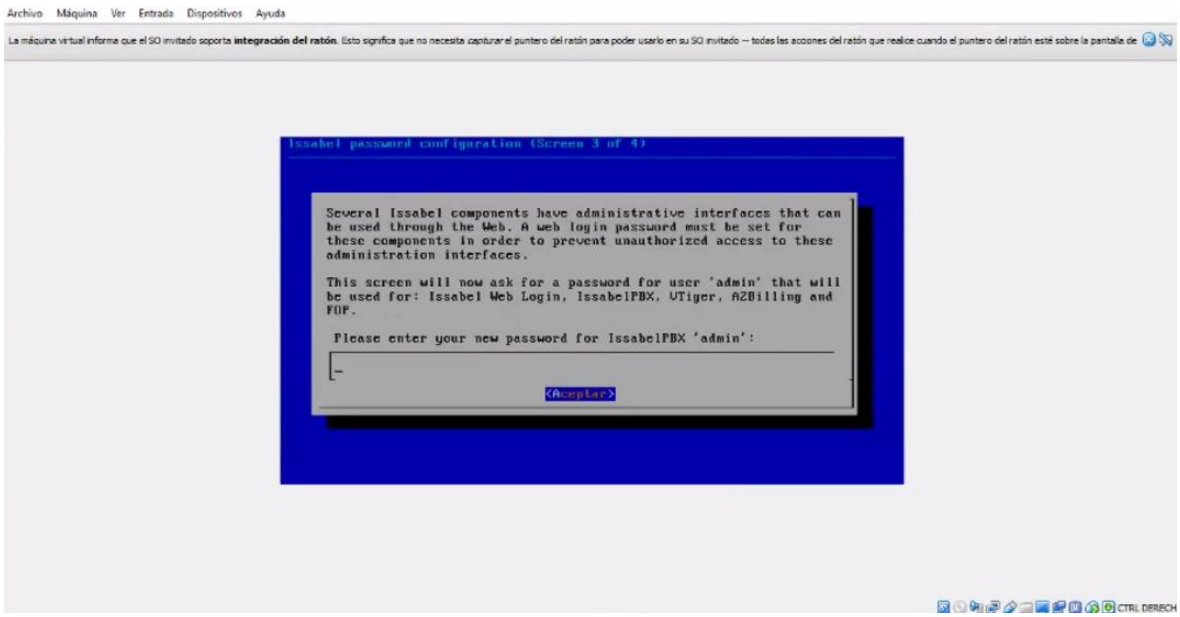

Issabel
us
Help!
REGIONALIZACIÓN
FECHA & HORA
huso horario América/Nueva York
TECLADO
Inglés (EE. UU.)
SOPORTE DE IDIOMA
Español (España)
SECURITY
SECURITY POLICY
Ningún perfil seleccionado
SOFTWARE
ORIGEN DE INSTALACIÓN
Medios locales
SELECCIÓN DE SOFTWARE
Instalacion de Issabel
SISTEMA
DESTINO DE LA INSTALACIÓN
No se seleccionó ningún disco
KDUMP
Kdump esta inhabilitado

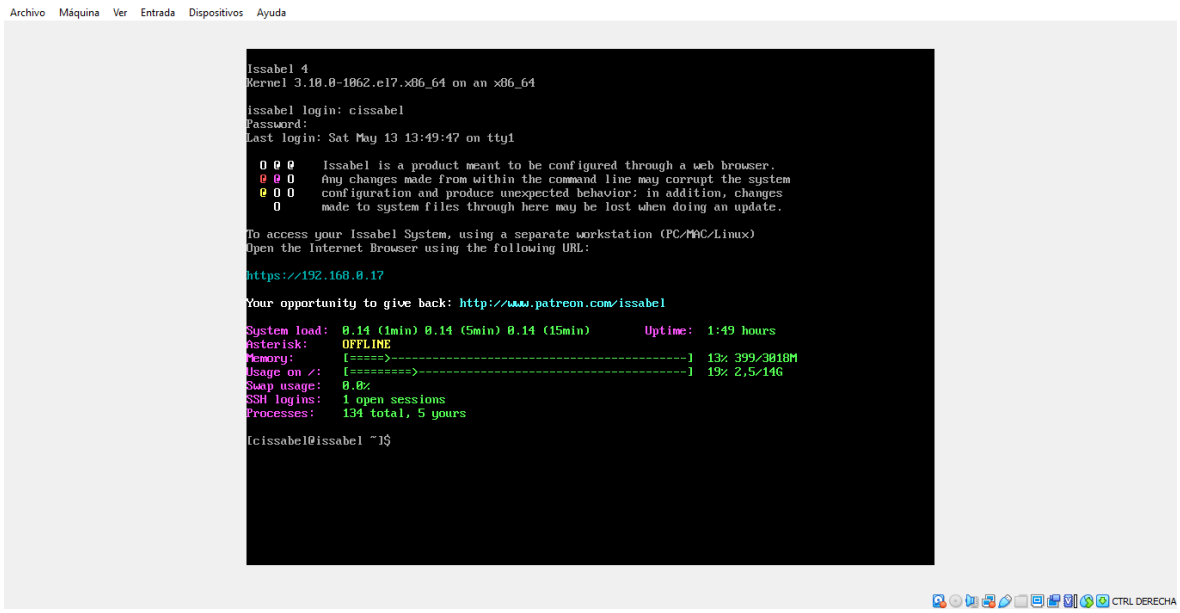

Archivo Máquina Ver Entrada Dispositivos Ayuda
Listo
es
Help!
¿Qué diseños de teclado desearía usar en este sistema? Puede mover cualquier diseño de teclado al comienzo de la lista para que sea el predeterminado.
Español; Castellano (Español)
Inglés (EE. UU.)
Probar la configuración de disposición de abajo:
El cambio de diseño no está configurado.
Opciones


Archivo Máquina Ver Entrada Dispositivos Ayuda
Seleccione los dispositivos en que le gustaría instalar. Se mantendrán sin tocar hasta que pulse el botón «Comenzar instalación» del menú principal.
Discos estándares locales
10 GiB
ATA VBOX HARDDISK
sda / 10 GiB libre
Discos especializados y de red
Añadir un disco...
Otras opciones de almacenamiento
Particionado
Configurar el particionado automáticamente.
Voy a configurar las particiones.
Me gustaría crear espacio disponible adicional.
Cifrado
Cifrar mis datos. Usted establecerá una frase de paso después.
0 discos seleccionados; 0 B de capacidad; 0 B libre
Error al comprobar la configuración de almacenamiento. Clic para más detalles.

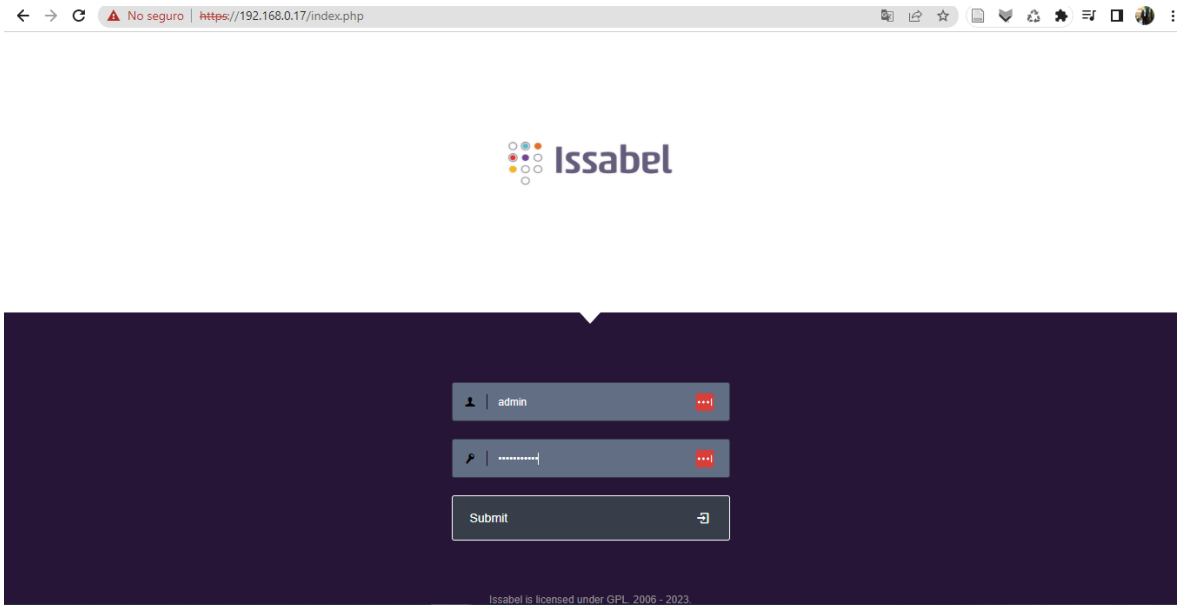

Archivo Máquina Ver Entrada Dispositivos Ayuda
CONTRASEÑA ROOT
Listo
INSTALACIÓN DE ISSABEL 4
es
Help!
La cuenta root se usa para administrar el sistema. Introduzca una contraseña para el usuario root.
Contraseña de root:
Vacío
Confirmar:

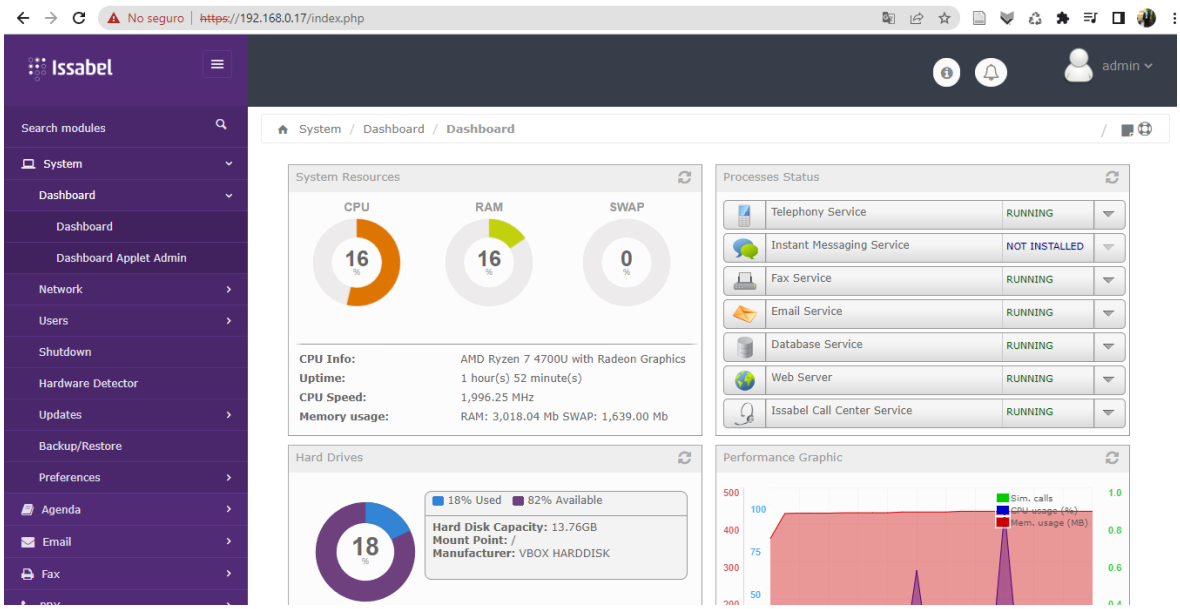

Archivo Máquina Ver Entrada Dispositivos Ayuda
La máquina virtual informa que el SO invitado soporta integración del ratón. Esto significa que no necesita capturar el puntero del ratón para poder usarlo en su SO invitado -- todas las acciones del ratón que realice cuando el puntero del ratón esté sobre la pantalla de
Issabel password configuration (Screen 1 of 4)
The Issabel system uses the open-source database engine MySQL for storage of important telephony information. In order to protect your data, a master password must be set up for the database.
This screen will now ask for a password for the 'root' account of MySQL.
Please enter your new MariaDB root password:
<Aceptar>
CTRL DERECH

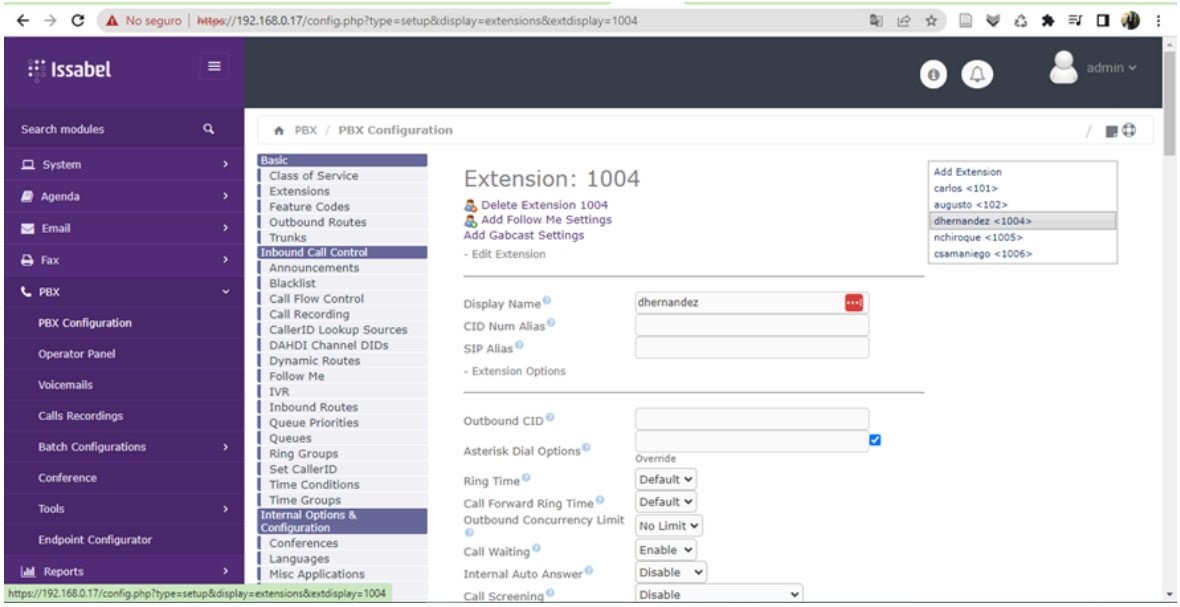


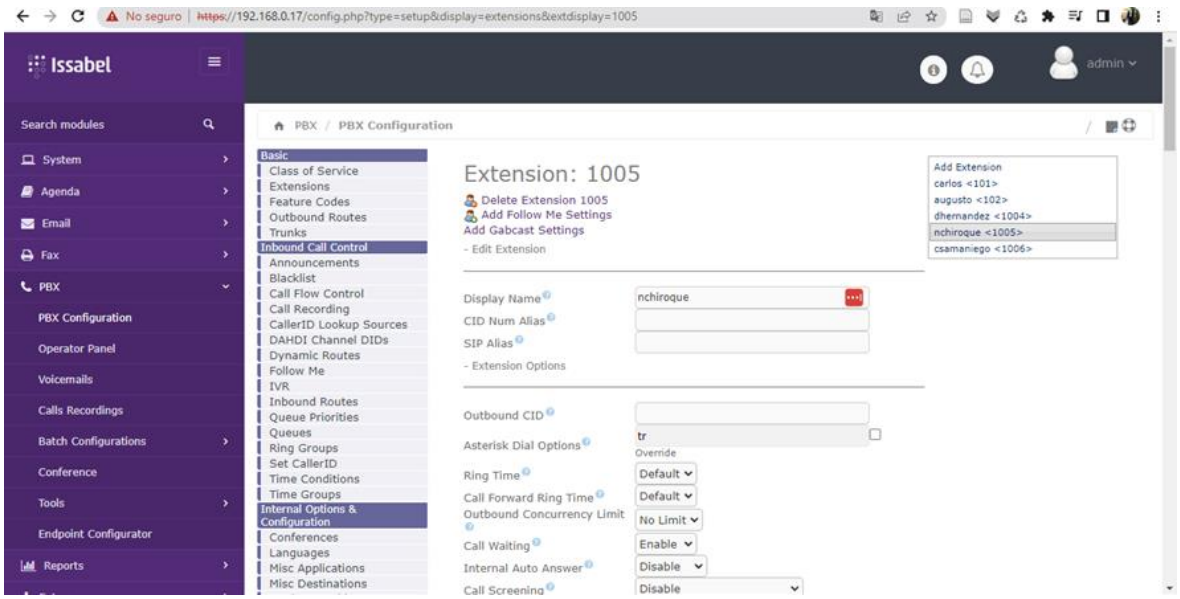


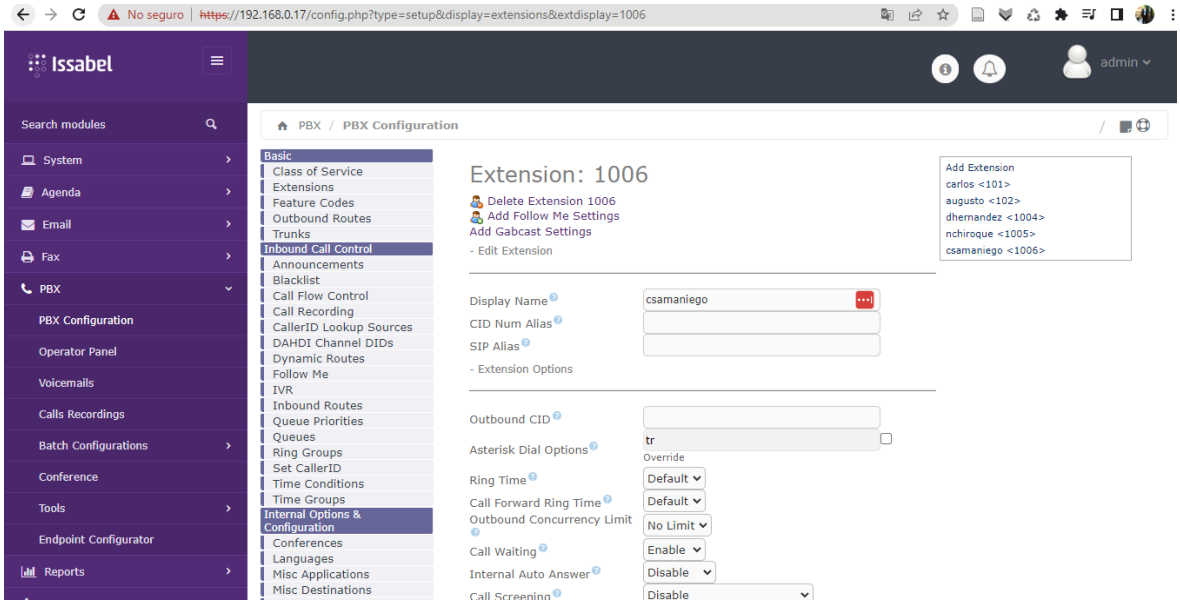
Después de realizar la instalación de Issabel el software arroja una dirección ip, esta dirección la colocamos en el navegador, esto nos permite crear la extensiones y los usuarios.

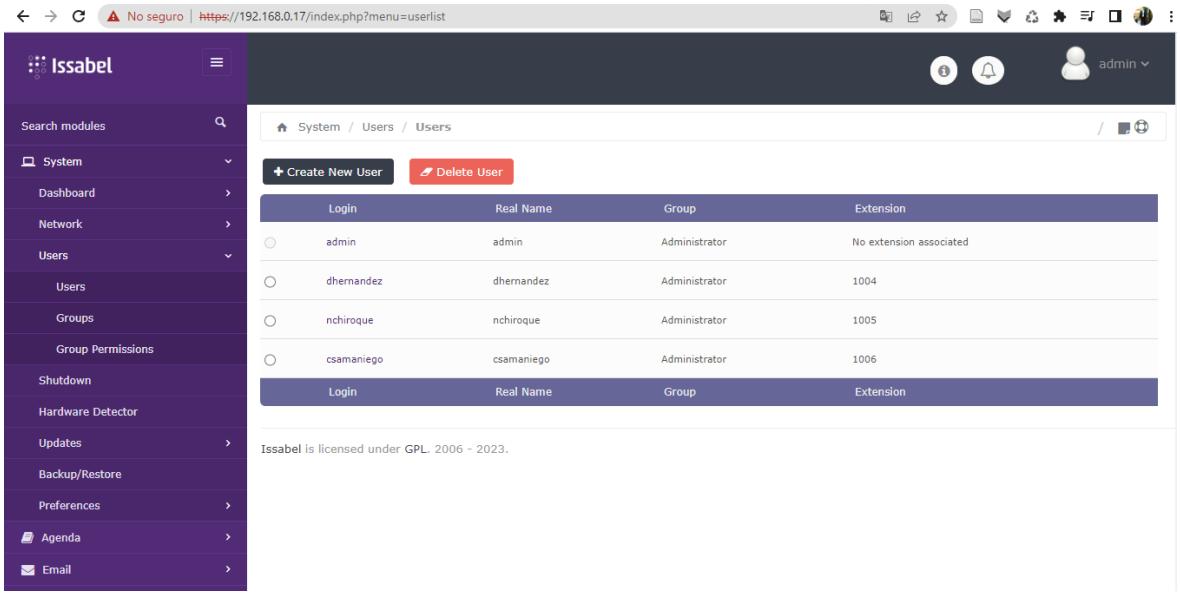

No seguro | https://192.168.0.17/index.php
Issabel
admin
Submit
Issabel is licensed under GPL. 2006 - 2023.


No seguro | https://192.168.0.17/index.php
Issabel
admin
Search modules
System
Dashboard
Dashboard
Dashboard Applet Admin
Network
Users
Shutdown
Hardware Detector
Updates
Backup/Restore
Preferences
Agenda
Email
Fax
System / Dashboard / Dashboard
System Resources
CPU
16
RAM
16
SWAP
0
CPU Info: AMD Ryzen 7 4700U with Radeon Graphics
Uptime: 1 hour(s) 52 minute(s)
CPU Speed: 1,996.25 MHz
Memory usage: RAM: 3,018.04 Mb SWAP: 1,639.00 Mb
Processes Status
Telephony Service RUNNING
Instant Messaging Service NOT INSTALLED
Fax Service RUNNING
Email Service RUNNING
Database Service RUNNING
Web Server RUNNING
Issabel Call Center Service RUNNING
Hard Drives
18
18% Used 82% Available
Hard Disk Capacity: 13.76GB
Mount Point: /
Manufacturer: VBOX HARDDISK
Performance Graphic
Sim. calls
CPU usage (%)
Mem. usage (MB)


No seguro | https://192.168.0.17/config.php?type=setup&display=extensions&extdisplay=1004
Issabel
admin
Search modules
System
Agenda
Email
Fax
PBX
PBX Configuration
Operator Panel
Voicemails
Calls Recordings
Batch Configurations
Conference
Tools
Endpoint Configurator
Reports
PBX / PBX Configuration
Basic
Class of Service
Extensions
Feature Codes
Outbound Routes
Trunks
Inbound Call Control
Announcements
Blacklist
Call Flow Control
Call Recording
CallerID Lookup Sources
DAHDI Channel DIDs
Dynamic Routes
Follow Me
IVR
Inbound Routes
Queue Priorities
Queues
Ring Groups
Set CallerID
Time Conditions
Time Groups
Internal Options & Configuration
Conferences
Languages
Misc Applications
Extension: 1004
Delete Extension 1004
Add Follow Me Settings
Add Gabcast Settings
- Edit Extension
Add Extension
carlos <101>
augusto <102>
dhernandez <1004>
nchiroque <1005>
csamaniego <1006>
Display Name
dhernandez
CID Num Alias
SIP Alias
- Extension Options
Outbound CID
Asterisk Dial Options
Override
Ring Time
Default
Call Forward Ring Time
Default
Outbound Concurrency Limit
No Limit
Call Waiting
Enable
Internal Auto Answer
Disable
Call Screening
Disable
https://192.168.0.17/config.php?type=setup&display=extensions&extdisplay=1004


No seguro | https://192.168.0.17/config.php?type=setup&display=extensions&extdisplay=1005
Issabel
admin
Search modules
System
Agenda
Email
Fax
PBX
PBX Configuration
Operator Panel
Voicemails
Calls Recordings
Batch Configurations
Conference
Tools
Endpoint Configurator
Reports
PBX / PBX Configuration
Basic
Class of Service
Extensions
Feature Codes
Outbound Routes
Trunks
Inbound Call Control
Announcements
Blacklist
Call Flow Control
Call Recording
CallerID Lookup Sources
DAHDI Channel DIDs
Dynamic Routes
Follow Me
IVR
Inbound Routes
Queue Priorities
Queues
Ring Groups
Set CallerID
Time Conditions
Time Groups
Internal Options & Configuration
Conferences
Languages
Misc Applications
Misc Destinations
Extension: 1005
Delete Extension 1005
Add Follow Me Settings
Add Gabcast Settings
- Edit Extension
Add Extension
carlos <101>
augusto <102>
dhernandez <1004>
nchiroque <1005>
csamaniego <1006>
Display Name
nchiroque
CID Num Alias
SIP Alias
- Extension Options
Outbound CID
Asterisk Dial Options
tr
Override
Ring Time
Default
Call Forward Ring Time
Default
Outbound Concurrency Limit
No Limit
Call Waiting
Enable
Internal Auto Answer
Disable
Call Screening
Disable

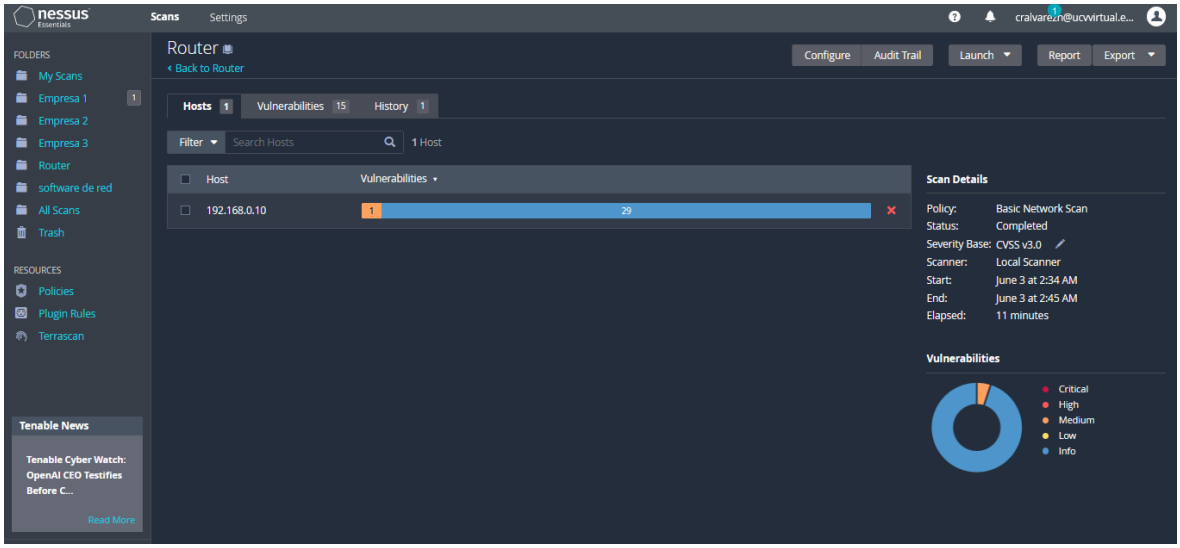




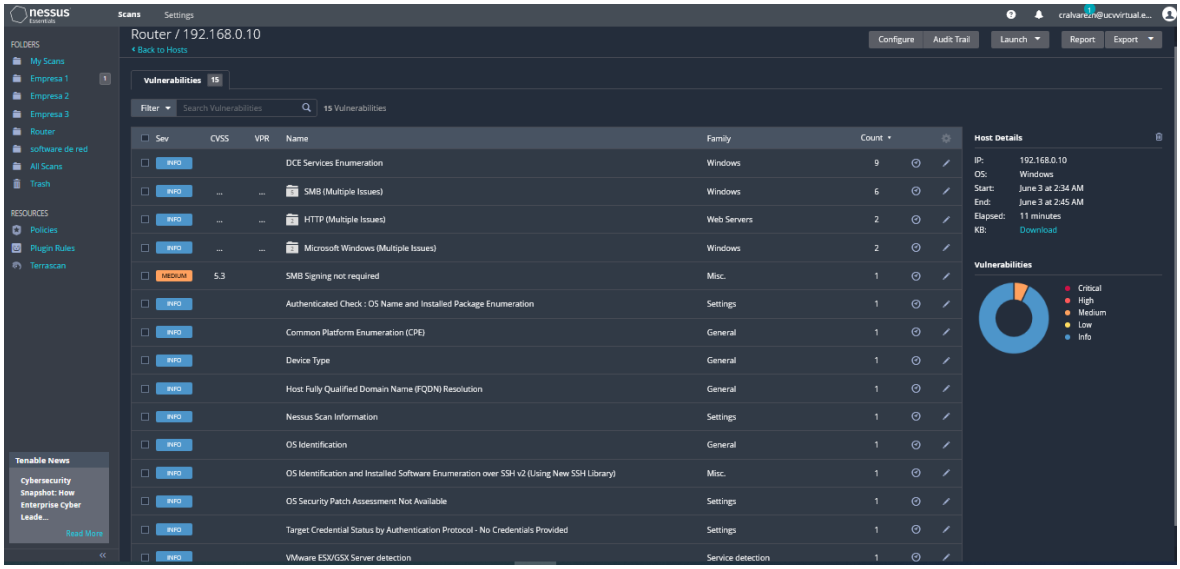
Luego de tener Issabel instalamos el software Kali Linux el cual nos permitirá realizar simulaciones de hacking ético.

Previo a realizar hacking ético tenemos que ver las vulnerabilidades de la voip. Para realizar este proceso primero debemos realizar ping al ip intervenir

para poder saber la cantidad de vulnerabilidades que hay en distinta configuraciones de VoiP utilizamos en software Nessus, este nos permite revelar con qué vulnerabilidades existe según la configuración que realicemos.

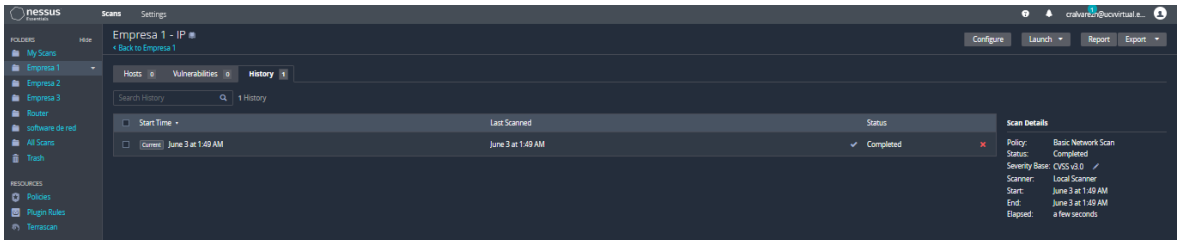


Como primer escenario analizamos el router, en el cual nos arroja 15 vulnerabilidades donde una de ellas es medianamente vulnerable y otras 29 son manejables.

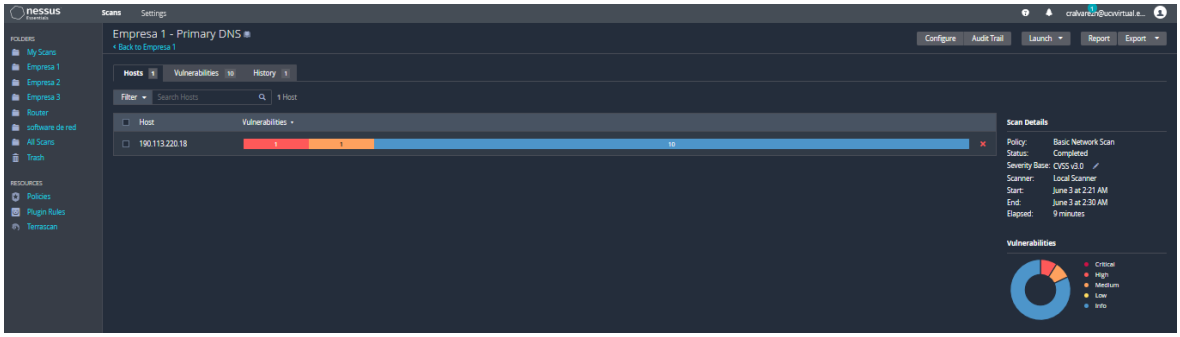


En esta imagen se puede visualizar de manera detallada las vulnerabilidades.

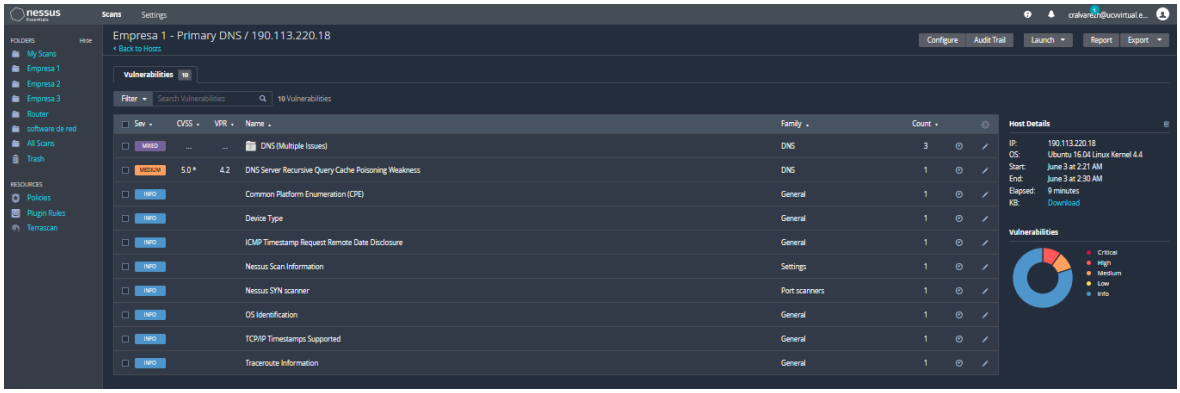
Empresa 1



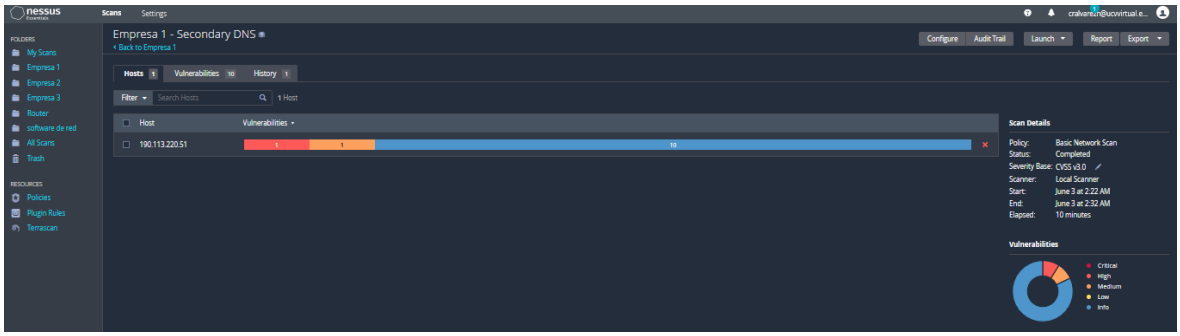
En la primera empresa simulada, analizamos la IP en la cual nos arroja 0 vulnerabilidades.



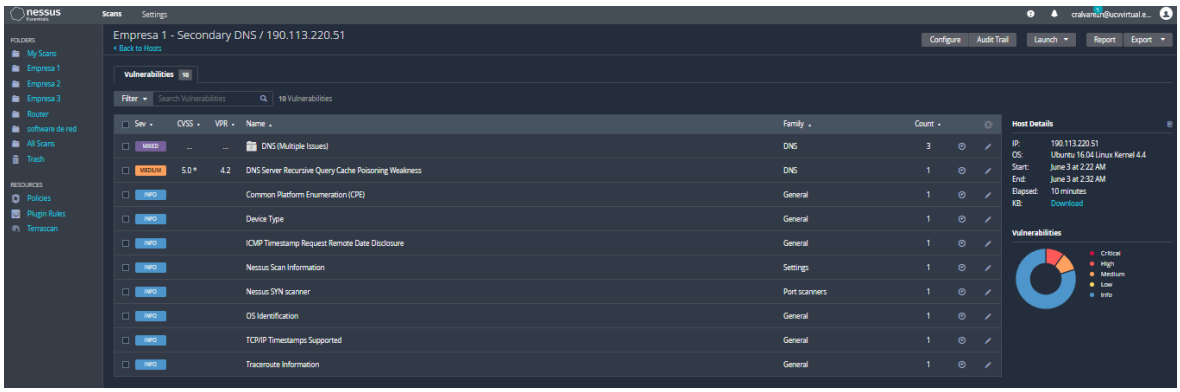
Analizamos el DNS Primario en la primera empresa en cual no arroja 10 vulnerabilidades. podemos observar que se obtiene 1 vulnerabilidad crítica y otra en categoría grande.



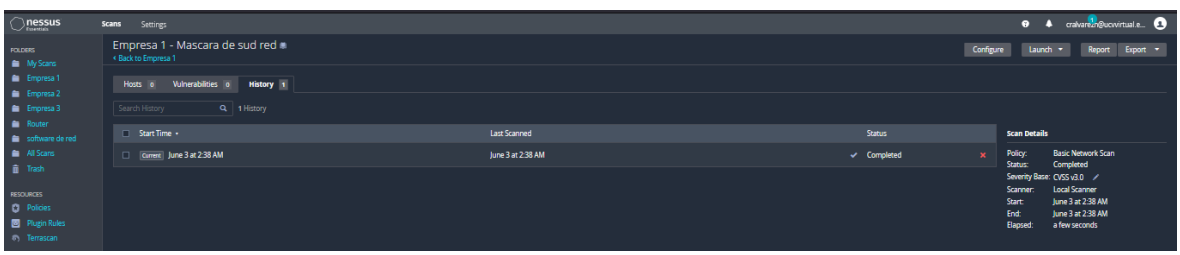
En esta imagen se puede observar cada una de las vulnerabilidades mostradas anteriormente.



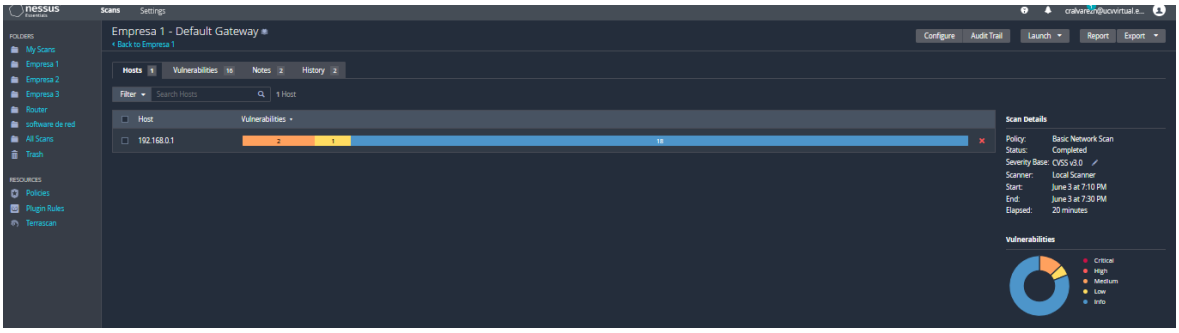
Analizamos el DNS Secundario en la primera empresa en cual no arroja 10 vulnerabilidades. podemos observar que se obtiene 1 vulnerabilidad crítica y otra en categoría grande.



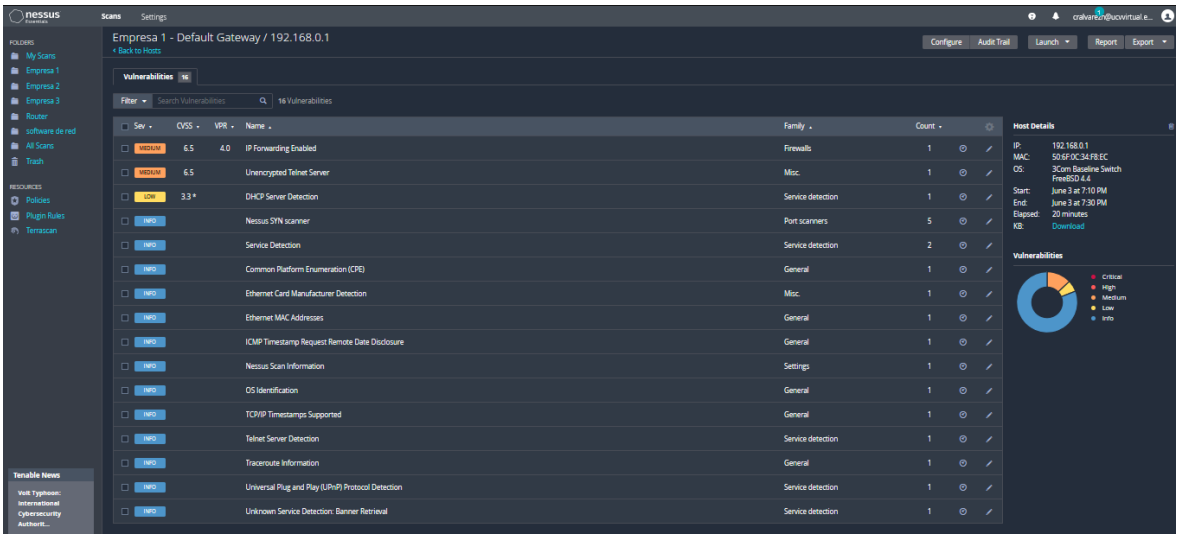
En esta imagen se puede observar cada una de las vulnerabilidades mostradas anteriormente.



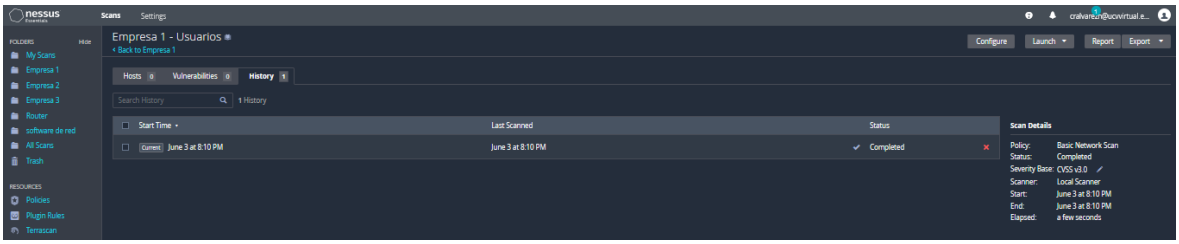
En la empresa 1 podemos observar que en la máscara de subred no hay vulnerabilidades.



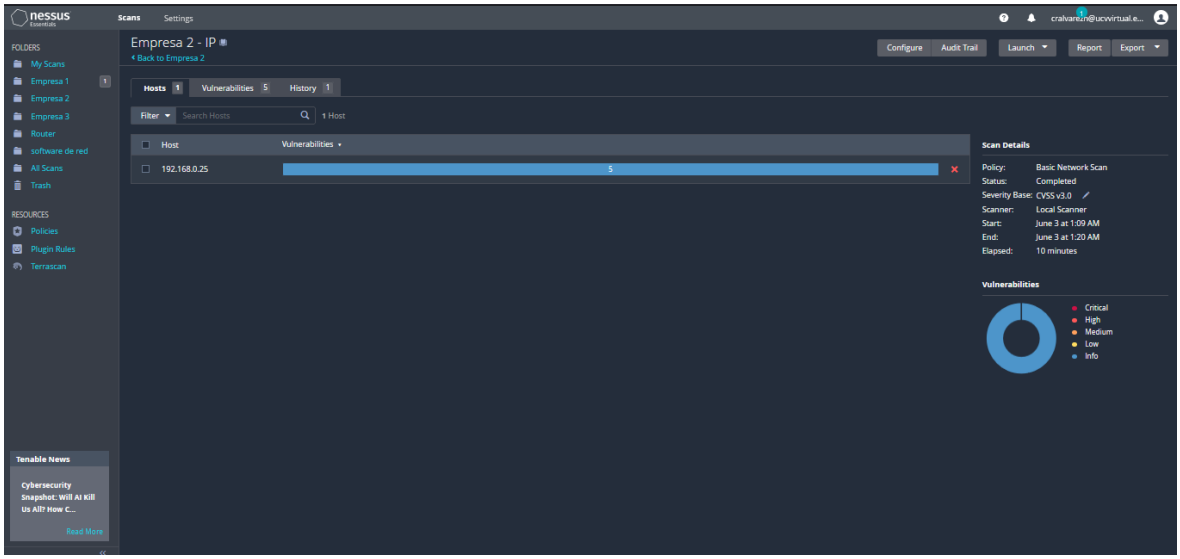
Analizamos el Gateway en la primera empresa en cual no arroja 18 vulnerabilidades. Podemos observar que se obtiene 1 vulnerabilidad baja y dos en mediana.



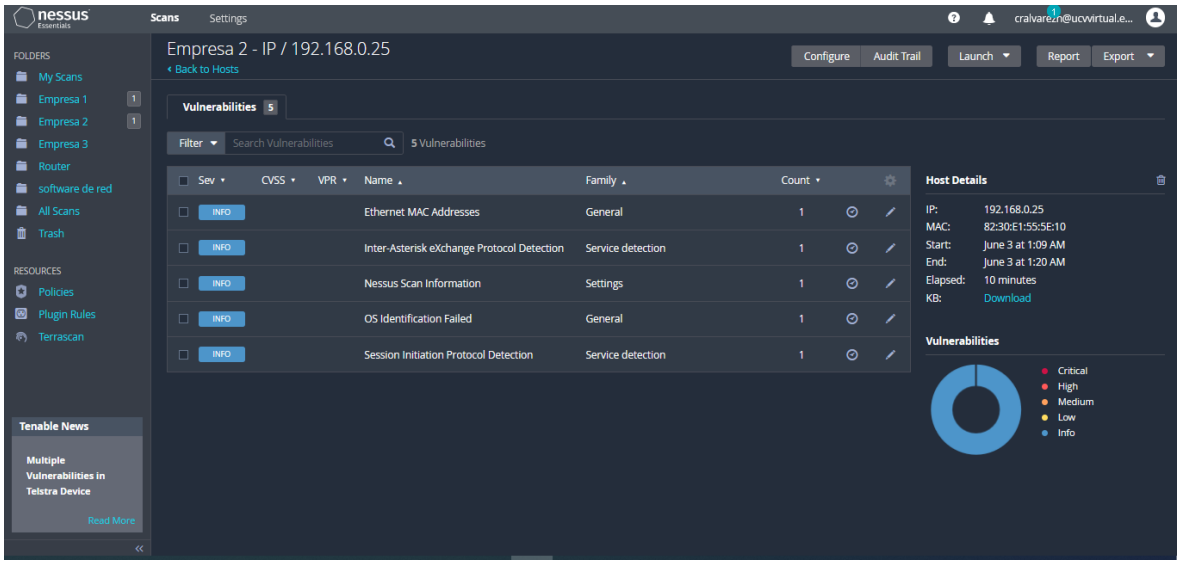
En esta imagen se puede observar cada una de las vulnerabilidades mostradas anteriormente.



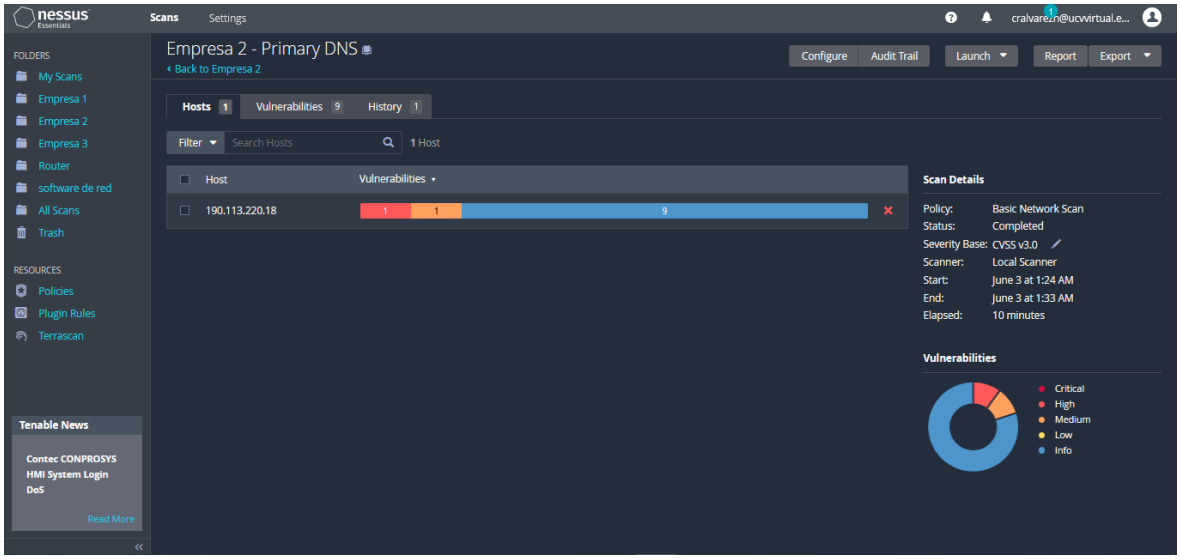
En esta imagen se puede observar más a detalle cada vulnerabilidad.



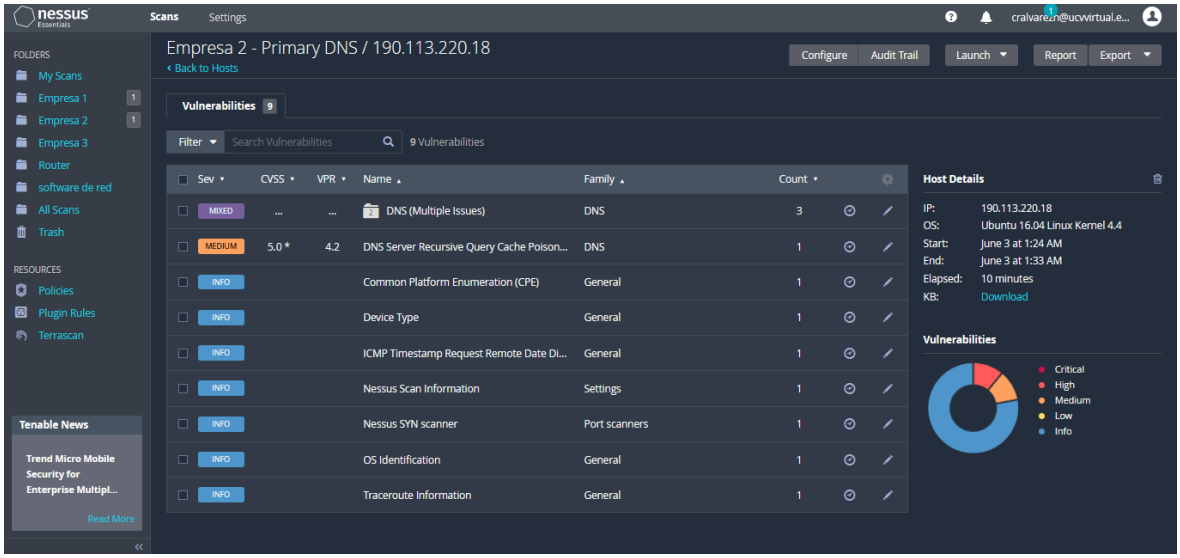
En este segundo escenario se puede analizar el la IP, donde se observa que son 5 las vulnerabilidades, las cuales son manejables según el software.



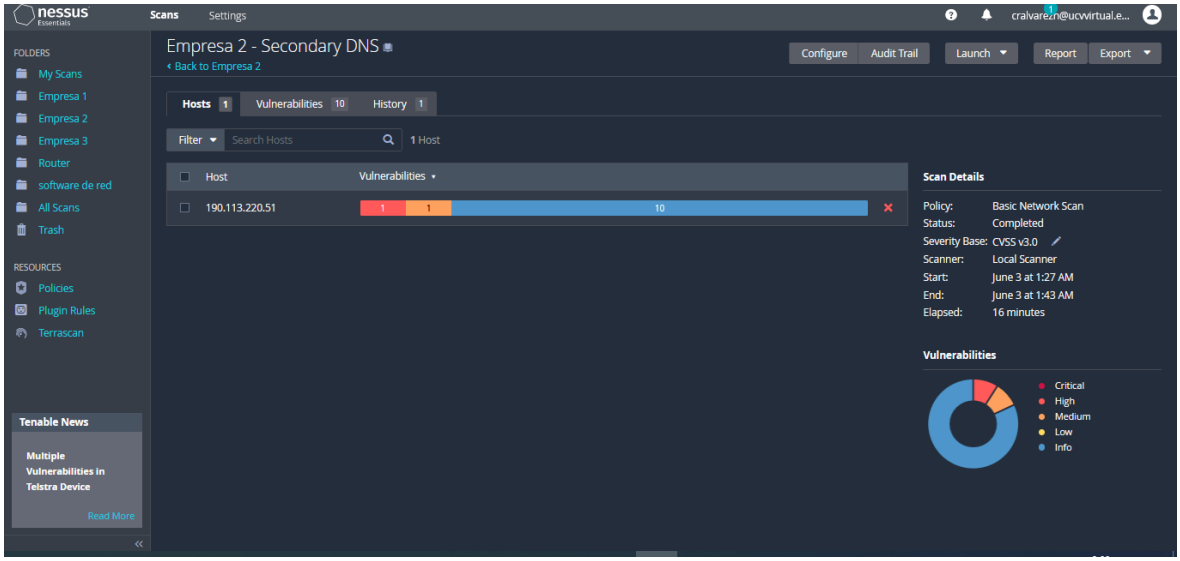
En esta imagen podemos observar el detalle de cada vulnerabilidad.



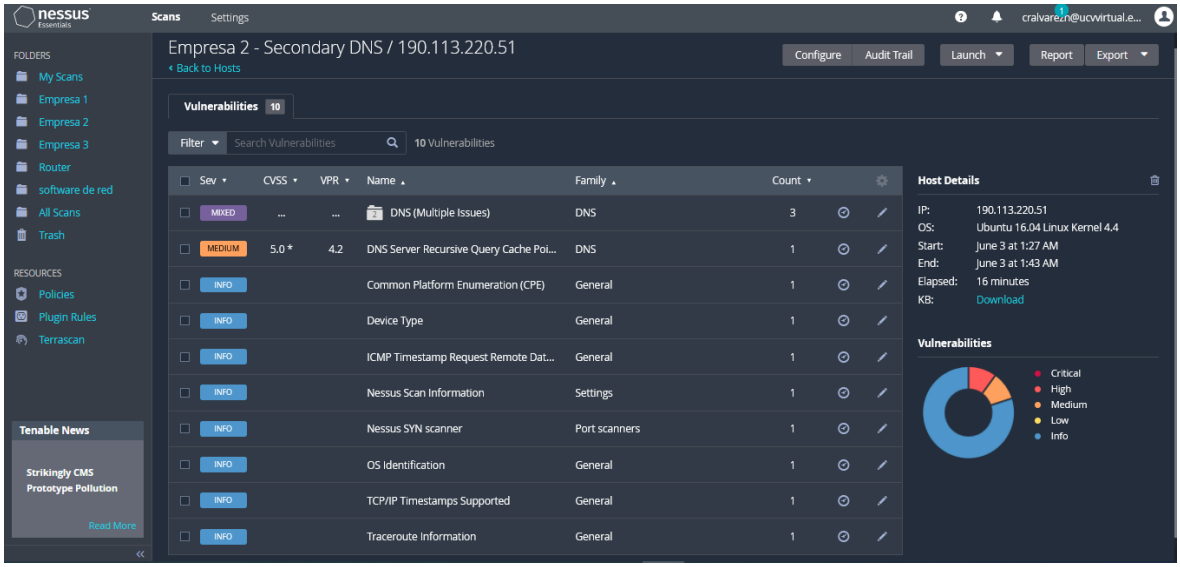
Analizamos el DNS primario la segunda empresa en cual no arroja 9 vulnerabilidades. Podemos observar que se obtiene 1 vulnerabilidad baja y dos en mediana.



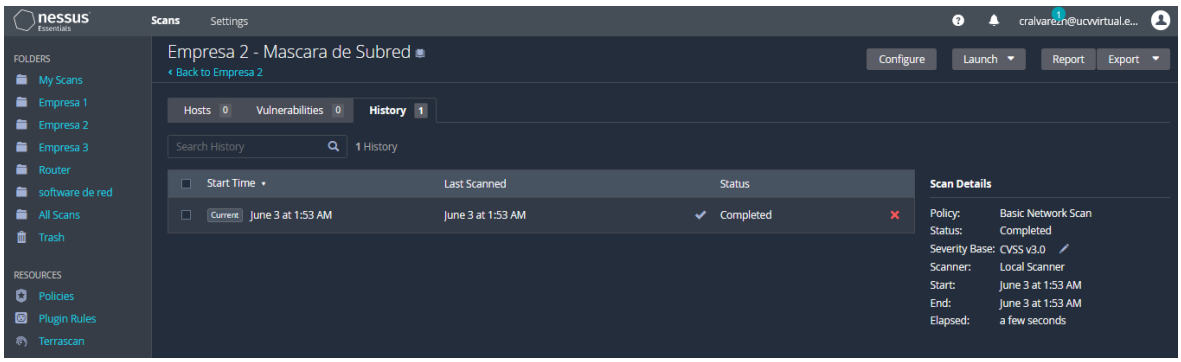
En esta imagen podemos observar el detalle de cada vulnerabilidad.



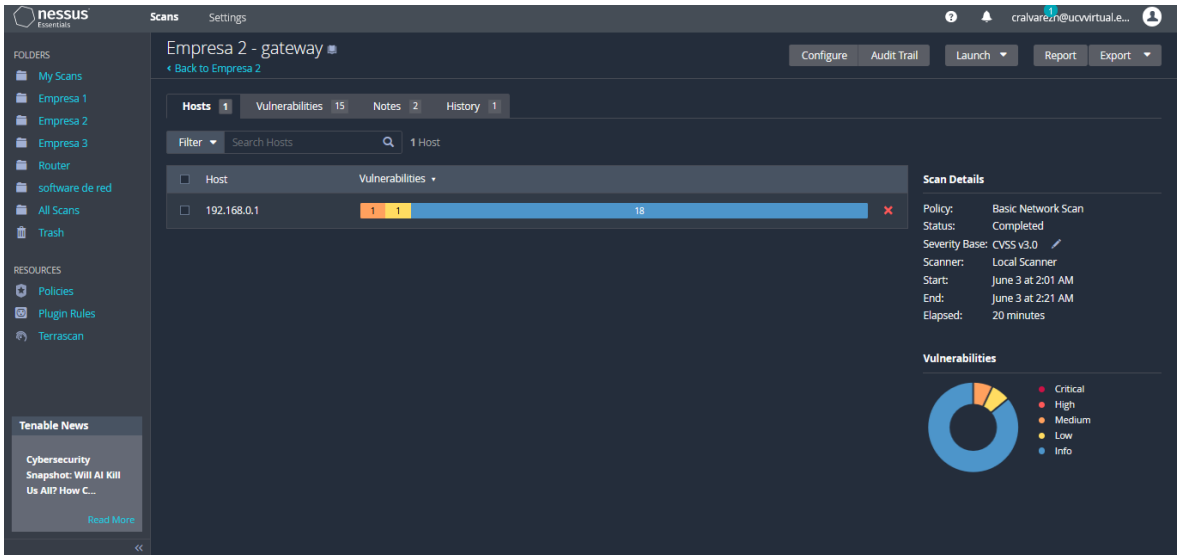
Analizamos el DNS secundario de la segunda empresa en cual no arroja 9 vulnerabilidades. Podemos observar que se obtiene 1 vulnerabilidad baja y dos en mediana.



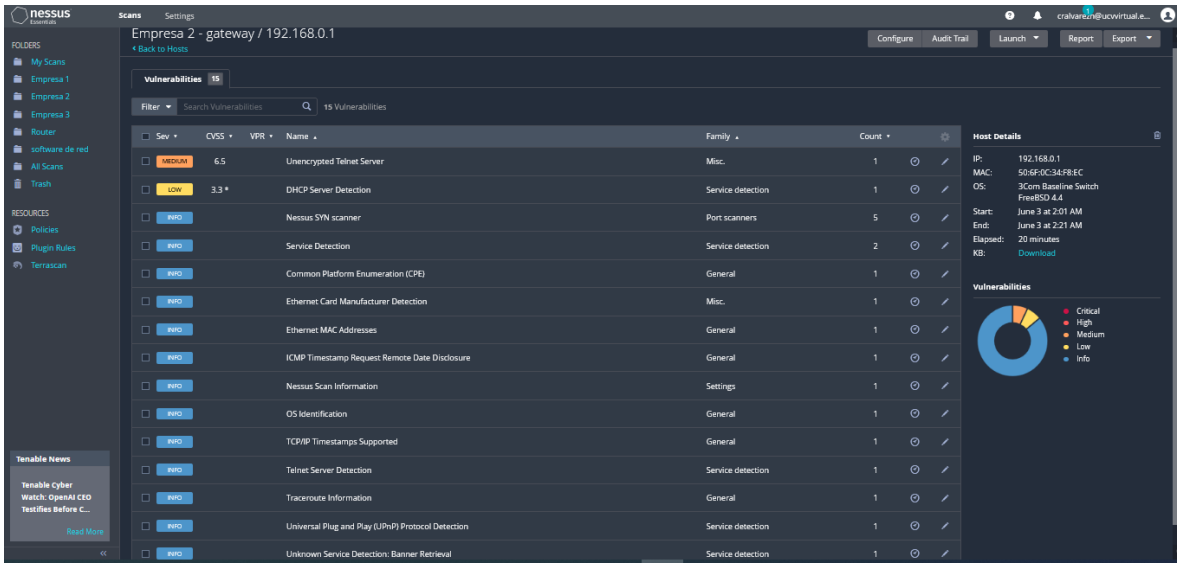
En esta imagen podemos observar el detalle de cada vulnerabilidad.



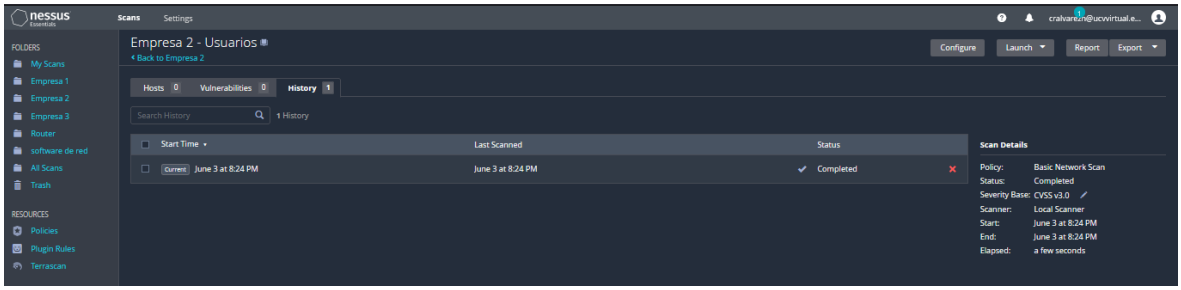
En la empresa 2 podemos observar que en la máscara de subred no hay vulnerabilidades.

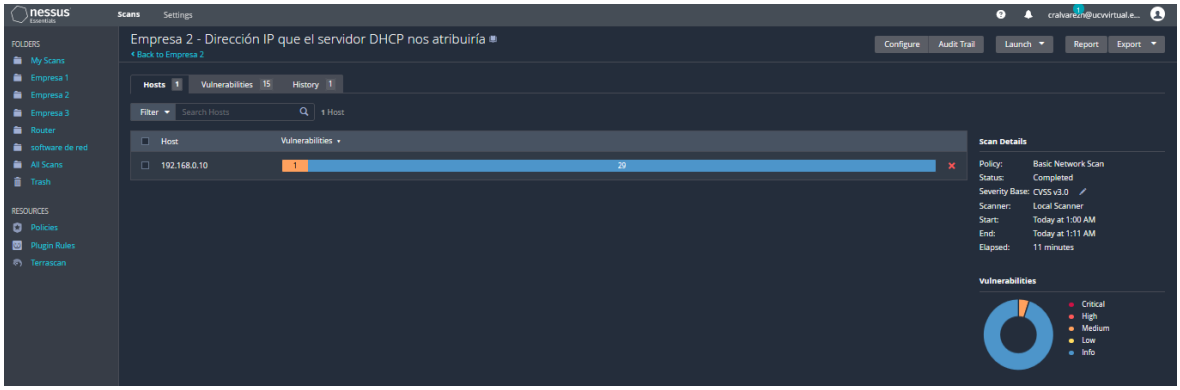


Analizamos el Gateway de la segunda empresa en cual no arroja 15 vulnerabilidades, 1 en estado medio y otro en estado bajo.

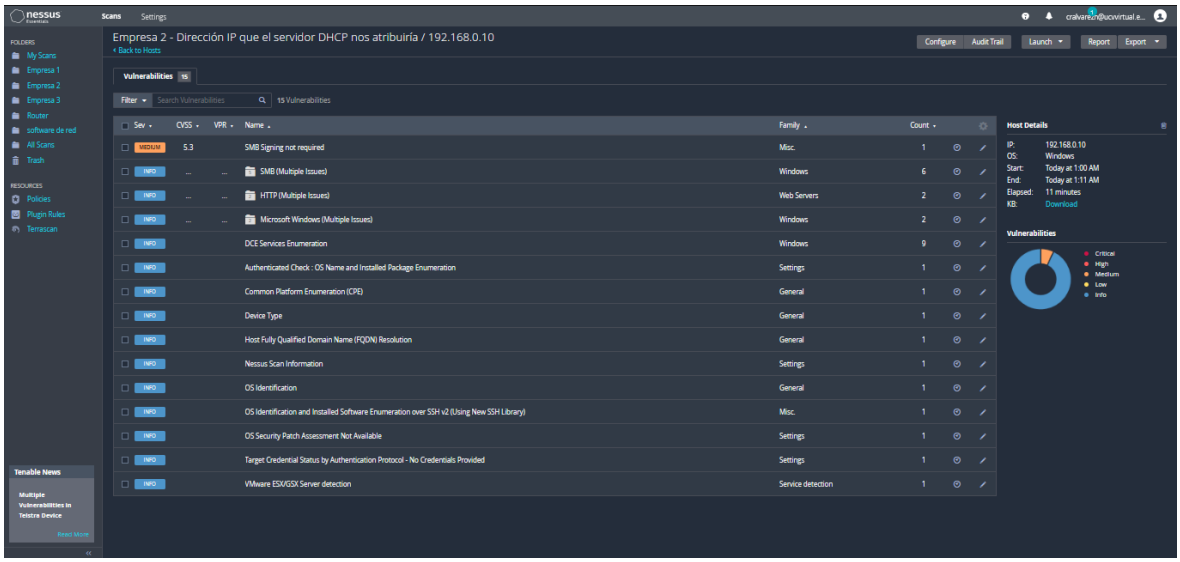


En esta imagen podemos observar el detalle de cada vulnerabilidad.





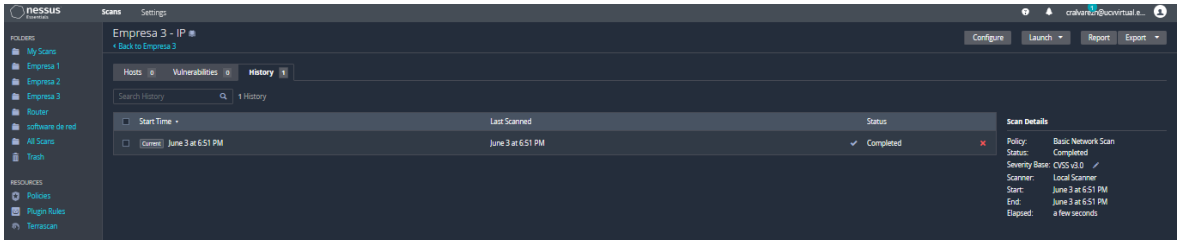
Analizamos la IP de la segunda empresa en cual no arroja 15 vulnerabilidades, 1 en estado medio.



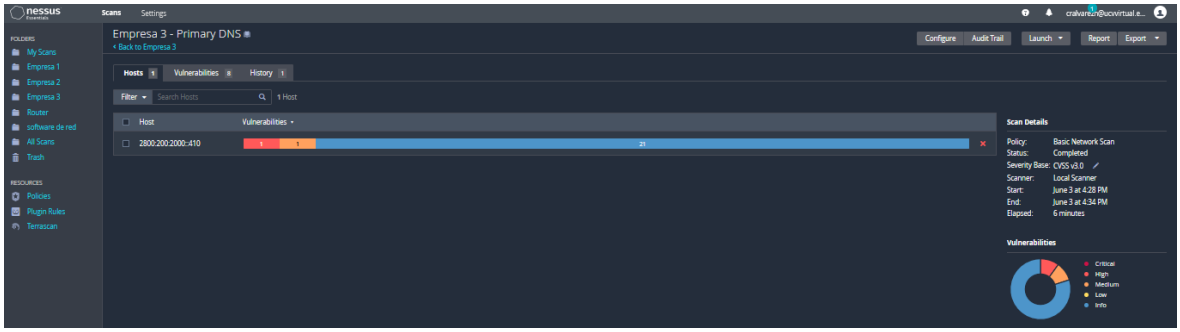
En esta imagen podemos observar el detalle de cada vulnerabilidad.

Empresa 3

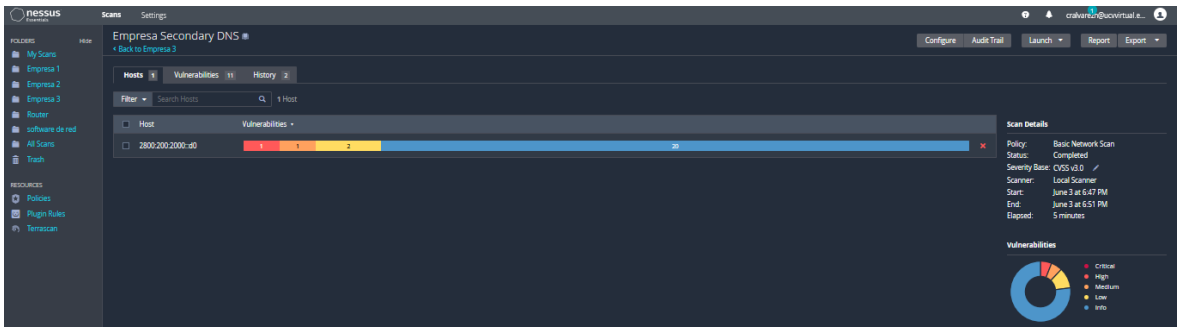
IP

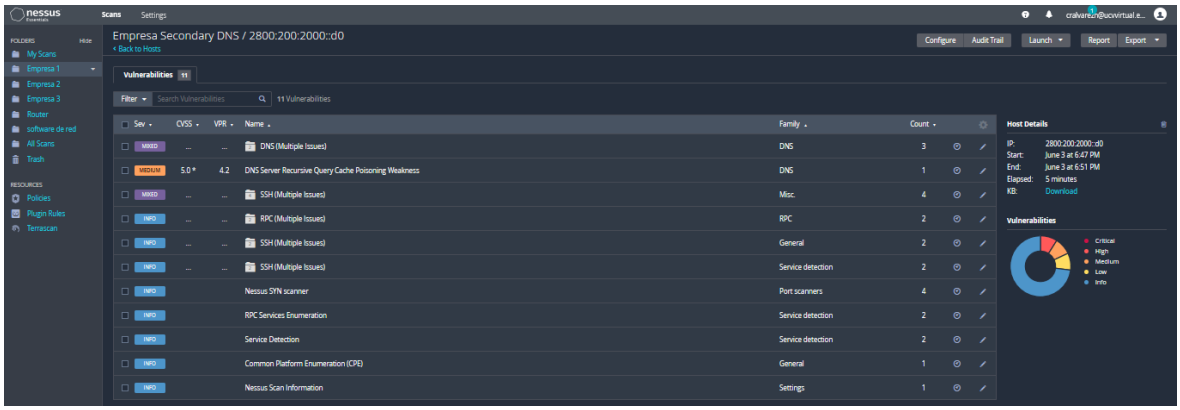


Primary DNS



Secondary DNS





Máscara subred