MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

Evaluar la efectividad en las Políticas de la seguridad y cifrado de los protocolos H.323 y SIP con SSL para redes VoIP.

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por la estudiante:
Johnny Gerardo BARRIGA ARIZABALA

Bajo la dirección de:
Rayner Stalyn DURANGO ESPINOZA.

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador
Mayo del 2019

Evaluar la efectividad en las Políticas de la seguridad y cifrado de los protocolos H.323 y SIP con SSL para redes VoIP.

Johnny Gerardo BARRIGA ARIZABALA[1]
Rayner Stalyn DURANGO ESPINOZA[2]

Resumen

La documentación pertinente aborda la temática de seguridad en sistemas Voz sobre protocolo de Internet, desde una perspectiva teórica, cognitiva y analítica mediante una encuesta efectuada a 100 expertos en seguridad digital en las principales empresas de Machala con el objeto de medir la efectividad en las políticas de protección gestadas en los estándares H.323 y SIP.
Se ejecuta una revisión literaria al compilar criterios de autores entendidos en la materia, en torno a las premisas, cualidades, parámetros o reactivos que caracterizan a las reglamentaciones citadas; la metodología aplicada es Delphi y descriptiva sustentada en un análisis descriptivo, gracias a las correlaciones prestadas por el software SPSS.
La finalidad de la investigación es diferenciar cuál estándar es mejor en términos de seguridad, a la vez medir el grado de resguardo que ofrece el sistema VoIP, verificar cuáles variables son las más relevantes al garantizar la fidelidad, calidad e integridad en los paquetes de datos; también se destacan recomendaciones u observaciones que permiten optimizar las potencialidades en el uso de sistemas digitales acorde a las tendencias contemporáneas de las prestaciones tecnológicas, afines al campo de las telecomunicaciones.

Palabras clave: VoIP, seguridad, evaluación, políticas, H.323-SIP.

Abstract

The relevant documentation addresses the issue of security in Voice over Internet protocol systems, from a theoretical, cognitive and analytical perspective through a survey conducted to 100 experts in digital security in the main companies of Machala in order to measure the effectiveness of policies of protection gestadas in the H.323 and SIP estandàres.
A literary revision is executed when compiling criteria of authors understood in the matter, around the premises, qualities, parameters or reagents that characterize the cited regulations; the applied methodology is Delphi and descriptive based on a descriptive analysis, thanks to the correlations provided by the SPSS software.
The purpose of the research is to differentiate which standard is better in terms of security, while measuring the degree of protection offered by the VoIP system, verifying which variables are the most relevant to ensure fidelity, quality and integrity in the data packages ; recommendations or observations are also highlighted that allow optimizing the potential in the use of digital systems according to contemporary trends in technological performance, related to the field of telecommunications.

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail correo jgbarriga@uees.edu.ec.
[2] Magíster en Seguridad Informática Aplicada. Director de la Maestría en Auditoría en Tecnologías de la Información Universidad Espíritu Santo-Ecuador.

INTRODUCCIÓN

La necesidad de las empresas y personas en comunicarse al menor tiempo posible, garantizar la integridad de la comunicación utilizando redes de datos; provoca mayores requerimientos de infraestructura tecnológica que las solventa; gestionando alternativas como la VoIP (voz sobre protocolo de internet) que permite cubrir con fluidez la necesidad de comunicación, utilizando protocolos como H.323, SIP y SSL. Así, el objetivo general de este documento es determinar la influencia de las políticas de la seguridad y cifrado de los protocolos H.323 y SIP con SSL para redes VoIP, por lo tanto, se realiza un análisis de varios autores que permitan generar una tabla para evaluar la efectividad de los protocolos, comparar estudios, así como analizar los indicadores que determinen cual es más efectivo al evaluar sus políticas de seguridad. Se opta por la metodología Delphi por ser de carácter sistemática e integrar la perspectiva teórica al medir la efectividad en las políticas de seguridad, por medio de una encuesta valorada en un cuadro informativo de las preguntas y justificado en un análisis abductivo; además, el tipo de investigación es exploratorio, la técnica de marco grupal facilita ampliar conocimientos trabajando de manera ágil al presentar resultados inmediatos, se contrasta con las opiniones de los expertos encuestados para conocer la factibilidad de las medidas de seguridad en respuestas a las vulnerabilidades afines a los sistemas VoIP.

La versatilidad, seguridad, agilidad son las bases contemporáneas en las redes de comunicación, el principal beneficio de esta tecnología es la posibilidad de crear redes multimedia con facilidad; por lo tanto, la vulnerabilidad de las redes VoIP es superior, comparado con redes de datos ya que tienen que transmitir datos en tiempo real, para asegurar la transmisión de voz, se pueden utilizar diferentes métodos y protocolos en varios niveles de comunicación y en distintas partes de la red. La seguridad de la comunicación de voz requiere inevitablemente estabilidad en los protocolos de señalización y transmisión (Mazalek, Vranova, & Stankova, 2015).

Durante los últimos años, las redes VoIP ha revolucionado el campo de las comunicaciones de voz debido a sus ventajas de costo y flexibilidad. Debido a este aumento continuo en el uso de esta tecnología, existe un mayor interés en la disponibilidad de soluciones biométricas, como el reconocimiento de identidad del usuario, identificación del idioma, identificación del género, estimación de la edad, etc., los cuales proporciona diversos servicios a través de Internet; de hecho, la sencillez de uso y aplicación de esas soluciones les garantiza una amplia gama de aplicaciones, como es el caso forense, servicios de banca a distancia como: e-banking, m-banking, servicios de comercio electrónico, por ejemplo, el control del acceso a recursos protegidos y servicios web. (Jamal, 2015).

Sin embargo, la complejidad de la arquitectura del sistema H.323, brinda un plan de control de transmisión de llamadas fiable, por lo tanto, hace al sistema más estable y seguro (Nikoukar, Hwang, Liem, & Lin, 2015).

Los sistemas de información están frecuentemente expuestos a diversos tipos de amenazas, sus efectos varían considerablemente: algunos inciden en la confidencialidad o integridad de los datos mientras que otros afectan la disponibilidad de un sistema (Jouini, Rabai, & Aissa, 2014).

MARCO TEÓRICO

En esta sección se compilan los criterios conceptuales capaces de direccionar el entendimiento de la temática, desde la visión del autor basada en una indagación bibliográfica para argumentar el escrito.

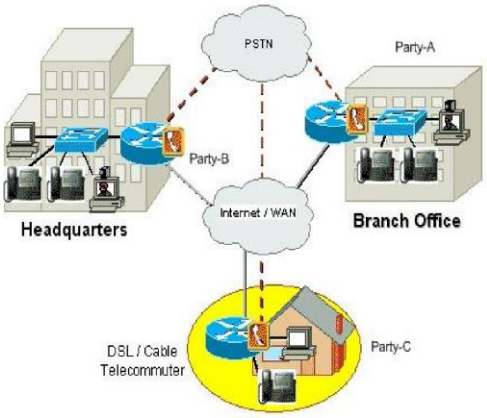
VoIP

Voz sobre IP, son paquetes de datos que viajan en forma digital para transmitir voz, esta tecnología utiliza protocolos como reglas para

intercambiar señales de voz en la red IP (Saad Saleh a, 2014).

VoIP permite realizar llamadas telefónicas usando protocolos de internet en lugar de la telefonía convencional, la misma que permite reducir costos de comunicación en las empresas (Chuquitarco, Villegas, Jácome, & Castillo, 2017). Una de sus bondades es utilizar una gran cantidad de protocolos al establecer comunicación, de los cuales vamos a revisar el H.323 y SIP. Así mismo, es necesario mantener canales de comunicación cifrados, esto se logra utilizando protocolos criptográficos como SSL que permiten establecer conexiones seguras, en las redes manteniendo la confidencialidad, integridad y autenticación de los datos (Costales, 2015). Además, las redes VoIP permiten integrar servidores IP Elastix que es un software de código libre que permite instalar centrales telefónicas para comunicación VoIP; también soporta protocolos H.323 y SIP (Landívar Edgar, 2015).

Figura 1: Esquema de llamada VoIP



Fuente: (Dakur & Dakur, 2015)

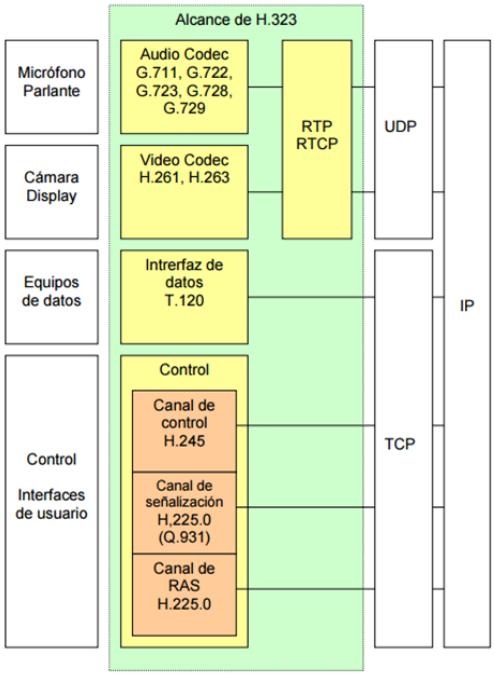
Una vez realizada la conexión, esta puede ser de cuatro tipos: texto, video, audio o una combinación de los tres, y el envío de estos datos se lo puede realizar mediante TCP y UDP. Por la cantidad de información que maneja esta clase de servicio, las posibilidades de tener problema de sobrecarga en los servidores son altos (Montazerolghaem, Shekofteh, Khojaste, Naghibzadeh, & Yaghmaee-M, 2014).

Protocolo H.323

Es un conjunto de reglas cuya señalización desempeña un papel importante, gracias a que establece las llamadas a través de Internet, lo cual permite al componente de red comunicarse una con otra, configurar y cerrar llamadas. Para establecer la sesión multimedia a través de telefonía IP, el protocolo H.323 es capaz de soportar sesiones de audio, video y datos a través del sistema VoIP. Para establecer una sesión multimedia entre usuarios, H.323 se completa primero con la operación de los usuarios y los registra a través del protocolo de Registro de Admisión y Estado (RAS). Después de registrar a los usuarios, H.323 realiza la señalización con respecto a la disposición de la llamada y desmontaje a través del protocolo H.225, el cual es el responsable de las negociaciones de la capacidad terminal y control de llamadas a través del protocolo H.245 (Singh, Singh, Singh, & Khan, 2014).

El protocolo H.323 integra estándares H.224, H.245 con la finalidad de facultar comunicación multimedia a través de la red VoIP. Además, este protocolo adopta el estándar RPT (Protocolo de Transporte en tiempo Real) el mismo que permite comunicaciones de audio y video en redes IP (Guaña-Moya & Muirragui-Irrazábal, 2018), en la figura 1 se expresa tanto la arquitectura como recomendación para la transmisión de datos en H.323.

Figura 2: Arquitectura de un terminal H.323



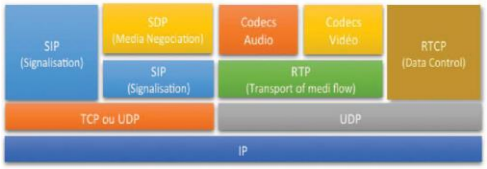
Fuente: (Joskowicz José, 2015)

El sistema H.323 define varios elementos de comunicación como Terminales, Unidades de Control Multipunto, Gateways, Gatekeepers y Elementos Frontera basado en Internet para ofrecer comunicación multimedia con capacidad de procesamiento y análisis. H.323 tiene siete fases en una llamada y puede soportar componentes para intercambiar mensaje o servicios suplementarios entre sí. Lo siguiente, son seis pasos de funcionalidad básica de H.323: la disposición de la llamada, comunicación inicial y el intercambio de capacidades, comunicación audiovisual, llamada estable con RTP, llamada de servicio de intercambio de medios y terminación de llamadas.

Protocolo SIP.

El uso de estándares abiertos, como el protocolo SIP, permite la interoperabilidad y facilita la producción de un gran número de soluciones, varias de las cuales también son gratuitas (Barry, Tamgno, Lishou, & Maleka, 2017).

Figura 3: Estructura del protocolo SIP

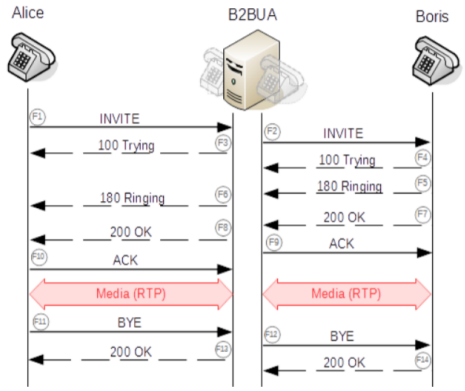


Fuente: (Barry et al., 2017)

De acuerdo a (Molina-Izurieta & Pazmiño-Ramírez, 2017) el desarrollo del SIP (Session Initiation Protocol) permite dar valor agregado a la telefonía IP, en base a que ofrece servicio de mensajería instantánea, envío de correos electrónicos y video llamadas, esto es una de las cualidades que lo diferencia de la telefonía tradicional, facilitando su adaptación a tareas cotidianas e instituciones capitalistas al optimizar sus potencialidades integrando versatilidad a las comunicaciones en forma horizontal o vertical. Este protocolo fue desarrollado por IETF (Internet Engineering Task Force) como una alternativa de H.323. Así mismo, en SIP las comunicaciones son enviadas como texto plano esto lo diferencia de H.323 (Joskowicz José, 2015). En la figura 3 se observa un ejemplo SIP de cómo se intercambia información entre el usuario y el servidor.

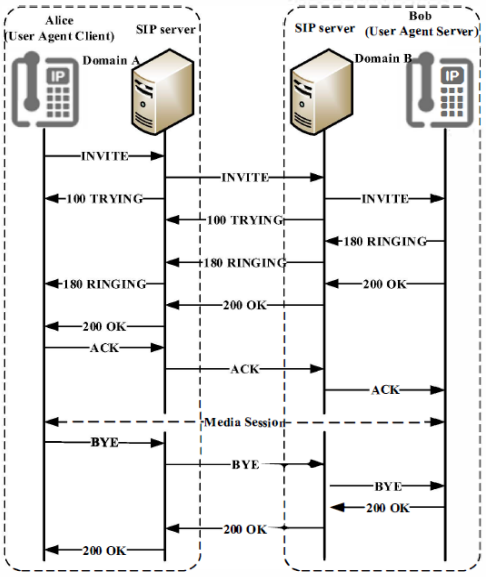
Comentario [IaP1]:

Figura 4: Ejemplo de comunicación SIP



Fuente: (Martínez, 2017)

Figura 5: Flujo de mensajes para establecer la conexión en SIP



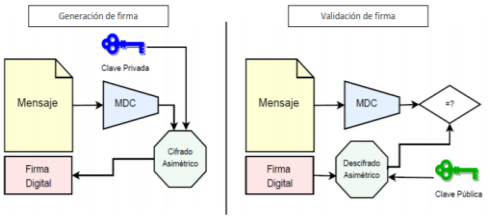
Fuente: (Hosseinpour, Seno, Moghaddam, & Roshkhari, 2016)

Aunque existen varios protocolos de señalización, a menudo el Protocolo de Inicio de Sesión (SIP) se utiliza para la señalización en VoIP. SIP es un protocolo de capa de aplicación que se utiliza para iniciar, modificar y finalizar sesiones multimedia entre los usuarios, teniendo en cuenta el texto y la simplicidad del protocolo SIP, los atacantes pueden realizar fácilmente diferentes tipos de ataques contra este protocolo (Hosseinpour et al., 2016).

Criptografía

Escuchar conversaciones de VoIP basada en SIP pudo haber sido bastante difícil en el pasado, pero con la tecnología de analizadores de protocolos o sniffer de paquetes de hoy en día, el ataque informático (hacking) se convierte en una práctica relativamente fácil. Sin ninguna duda, el escuchar a escondidas podría ser muy perjudicial, generando graves pérdidas en los negocios y en la industria por sus consecuencias. Dado que SIP necesita métodos más eficientes para realizar autenticación mutua en un entorno de red inseguro, se decide usar Criptografía de la Curva Elíptica (ECC), la cual, proporciona un tamaño de clave más pequeño que cualquier otro criptosistema y tiene cálculos más rápidos que la mitad los otros sistemas de clave pública en los mismos niveles de seguridad, ECC es adecuado para ser utilizado para la autenticación de mayor seguridad. (Thuayabat, 2015).

Figura 6: Firma digital en transferencia de datos



Fuente: (Ayllón, 2016)

El protocolo SIP presenta la autenticación de peticiones a través de un esquema de desafío-respuesta (challenge-response) llamado HTTP Digest Authentication que se hereda del protocolo HTTP, pero este protocolo de autenticación es vulnerable a diferentes tipos de ataques (Ahangari, Moghaddam, & Seno, 2016).

Seguridad informática.

Los experimentos prácticos son esenciales para la educación en seguridad de redes; las soluciones de laboratorio existentes requieren un esfuerzo significativo para construir, configurar y mantener, a menudo no admiten reconfigurabilidad, flexibilidad y escalabilidad (Xu, Huang, & Tsai, 2014).

Según (Pesantez, Aucancela, Auncancela, & Mantilla, 2017) la seguridad es “la cualidad o estado de estar libre de peligro”, es decir, protección contra los adversarios (aquellos que nos puede hacer daño tanto de forma intencionada como involuntaria). El objetivo principal de las políticas de seguridad informática es la de tratar de minimizar los

riesgos sobre los recursos informáticos y garantizar así la continuidad de las operaciones de la organización al tiempo que se administra dicho riesgo informático a un cierto costo aceptable. El objetivo secundario de la seguridad informática consiste en garantizar que los documentos, registros y archivos informáticos de la organización mantengan siempre su confiabilidad total, debido a que la privacidad respecto a información personal es considerada un complemento de los derechos humanos (Carvajal, 2018).

La seguridad informática es el área que se encarga de las metodologías, procesos y procedimientos para salvaguardar la información y datos confidenciales de una organización. Dichos procesos se estructuran a través de estándares, normas metodologías y protocolos para minimizar los riesgos en la empresa. Por ende, la seguridad informática es uno de los grandes retos a implementar, puesto que no es posible implementarla en un 100%, siendo imperiosa la aplicación de metodologías, infraestructura y estándares adecuados, permiten obtener un mayor grado de seguridad, mitigando algunos errores que se puede prevenir (Guzmán García & Tabora Bedoya, 2015).

Las cuestiones de seguridad relacionadas con VoIP, tales como: procesos de autenticación, asegura que cada participante de la conversación sean las personas correctas, el proceso de integridad, verificará y validará si los datos y el contenido de la conversación son comprometidos mientras se transportaban entre el remitente y el receptor. La privacidad se garantiza mediante el cifrado y el método de descifrado para proteger los datos de la intercepción y la alteración (Ghazali, Al-Nuaimy, Al-Ataby, & Al-Taee, 2016).

Según Gil (2012) describe a la seguridad de las redes VoIP como una tecnología que hereda protocolos ya existentes en las redes de datos. La figura 3 muestra como la seguridad de VoiP, está construida por varias capas. En consecuencia, las empresas deben mantener seguridad en varios niveles para proteger sus bases de datos. Es decir, evitar cualquier ataque informático que puede realizarse a través de las redes IP, se analiza desde una perspectiva holística como es apreciado en la figura 5.

Figura 7. Seguridad de las Redes VoIP

Fuente: (Borbúa, Herrera, & Ch, 2017)

SSL

En la actualidad, tener una comunicación cifrada se ha convertido en una prioridad dentro de las redes VoIP, dentro de este método de seguridad hay ventajas como desventajas. Se entiende como comunicación segura al servicio que brinda protección contra personas indeseadas que pueden estar escuchando, y mejorar la fiabilidad del envío de datos entre hosts (Husák, Cermák, Jirsík, & Celeda, 2015).

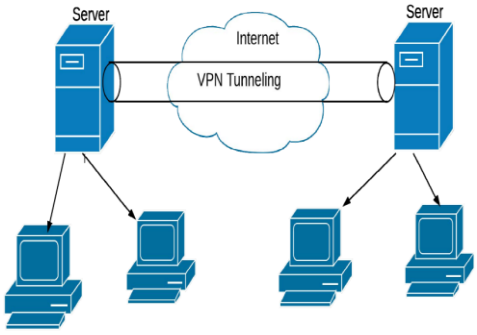
SSL es un protocolo criptográfico que proporciona una comunicación segura entre dos partes, a través de Internet, mediante encapsulación y el cifrado de datos en la capa de aplicación (Korczyński & Duda, 2014). SSL (Secure Socket Layer) proporcionar autenticación por identidad, confidencialidad en los datos e integridad de servicios dentro de comunicaciones basadas en red TCP/IP, cuenta con la tecnología de clave pública, por lo tanto, el pirata informático no interviene entre la comunicación desde el cliente al servidor de servicios o viceversa. Con el paso del tiempo se

ha convertido en una marca de seguridad en cualquier tipo de comunicación en Internet (Hao, Jia, Cui, Xin, & Meng, 2014).

TLS (Seguridad en Capa de Transporte) es la última versión de SSL, el cual se ha descubierto vulnerabilidades. La característica principal de TLS es la autenticación por medio de certificado digital, además de otros atributos como el no repudio, integridad de datos y protección de repetición. Actualmente permite asegurar protocolos como HTTP, SMTP, FTP (Husák et al., 2015).

Otra ventaja de SSL, es la compatibilidad con VPN, estas tecnologías van de la mano, brindando una conexión segura entre punto y punto (Gurung & Kim, 2015).

Figura 8: Ejemplo de VPN

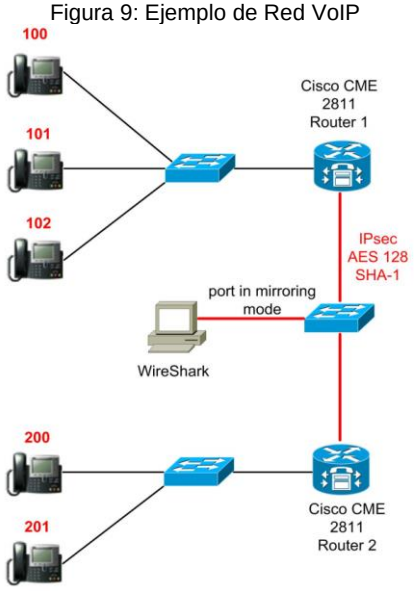


Fuente: (Gurung & Kim, 2015)

Redes

Las redes modernas de hoy en día, no solo están destinadas a transmitir información enteramente de datos simples, ahora con la tecnología de VoIP marca un comienzo de la modernización de las redes de comunicación, con la capacidad de transmitir datos multimedia a cualquier parte del mundo. En la Figura 6 se observa una conexión básica de telefonía IP con tecnología Cisco (Mazalek et al., 2015).

Figura 9: Ejemplo de Red VoIP



Fuente: (Mazalek et al., 2015)

Asterisk

Es software que se utiliza para hacer un sistema como IP-PBX y perciben el sistema VOIP que está apoyado por varios protocolos de los cuales SIP es uno de ellos (Karotiya, Wyawahare, & Haridas, 2016).

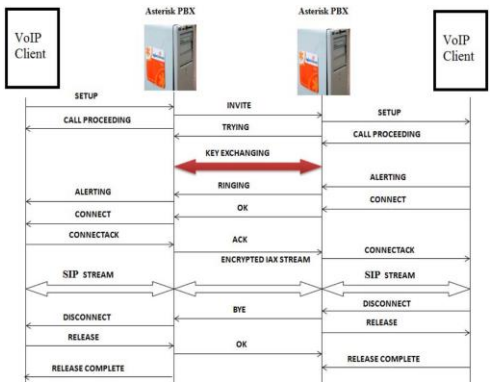
Asterisk al ser una aplicación de software libre, brinda mucho más funcionalidades y servicios, por lo tanto, en el momento de administrar una central PBX, se destacan algunas ventajas de este sistema, las cuales son:

- Grabaciones del sistema
- Rutas entrantes
- Operadoras automáticas
- Extensiones

Entre otras características, como permitir su implementación sobre sistemas operativos

Linux, minimizando el presupuesto inicial, debido a esto, el personal al frente del proyecto deben tener conceptos avanzados de programación y VoIP (Compromisos, Desafíos, & Educación, 2016).

Figura 10: Sistema basado en Asterisk PBX



Fuente: (Arjun & Ashok, 2014)

Elastix

Elastix es una plataforma unificada de comunicación, combina algunos conjuntos de software disponibles para PBX, basados en Asterisk y todo esto administrable desde una única interfaz gráfica. Por consiguiente, Elastix proporciona facilidades en el momento de configurar diferentes parámetros VoIP, especialmente para aquellos usuarios que no están acostumbrados a Linux y protocolos VoIP implementados en Asterisk (Lukša, Fajt, & Krhen, 2014).

Este sistema utiliza una base de datos CDR que es un Registro de Detalles de Llamadas, el cual se encuentra dentro del paquete de herramientas de Elastix, facilita el control de llamadas, actualizándose automáticamente. Algunos de los datos que se guardar en el CDR son ID de la llamada, origen, destino y fecha de la llamada (Barghi, Hossein, Moghadam, & Roshtkhari, 2014).

Bases de datos

Bases de datos una es una colección integrada de información almacenada en distintos tipos de registro, de forma que sean accesibles para múltiples aplicaciones. La interrelación de los registros se obtiene de las relaciones entre los datos no de su lugar de almacenamiento físico (Greiner Laura., 2014). Actualmente, y debido al avance tecnológico en el campo de la informática y la electrónica, la mayoría de las empresas cuentan con sistemas gestores de bases de datos para mantener la información en formato digital, las mismas que, ofrecen un amplio rango de soluciones informáticas al problema del almacenamiento de la información. Resumiendo lo que es una base de datos según (Tintín-Perdomo, Caiza-Caizabuano, & Caicedo-Altamirano, 2018) “Una base de datos es un conjunto de datos configurados en una red, siendo accesibles por los sistemas de aplicación de alguna empresa dada”.

Existen programas denominados sistema de gestión de bases de datos (SGBD), que permiten almacenar y posteriormente manipular los datos de forma rápida y estructurada. La definición según (IES Luis Vélez de Guevara, 2018) “conjunto de elementos software con capacidad de definir, mantener y utilizar una base de datos”. También se determina las funciones fundamentales de los SGBD que son las de actualizar, eliminar, crear y obtener la estructura asociada al esquema lógico de una base de datos.

Además, la clasificación de las bases de datos se puede definir de acuerdo a su modelo de administración. Básicamente un modelo de datos es una descripción de algo conocido como contenedor de datos, así como de los métodos que sirven para la manipulación de los datos. Estos modelos de datos no son cosas físicas, sino que son abstracciones que en definitiva permiten la instalación e implementación de un eficiente sistema de base de datos; por lo general se refieren a algoritmos, y conceptos matemáticos. Algunos de los modelos utilizados con mayor frecuencia en las bases de datos son: jerárquicas, de red, transaccionales, relacionales,

multidimensionales, documentales, Bases de datos deductivos. El conocimiento de que modelos de datos son utilizados en Sistemas de Gestión de Bases de Datos determina cómo debe estructurarse un diseño y las formas en que se representarán las relaciones entre la información (Greiner L., 2014).

Normas y estándares

Actualmente VoIP es una tecnología empleada a nivel mundial para transmitir información multimedio en tiempo real, pero también tiene sus limitaciones, por ejemplo, severos problemas en enviar voz sin perder paquetes, por lo tanto, la estructura de VoIP debe tener más garantías. Para realizar una evaluación de la calidad de voz, existen dos métodos principales: el primero se llama método subjetivo, el cual, se apoya en oyentes humanos que dan una opinión sobre la calidad de voz. El segundo lleva como nombre: método objetivo, es un software que mide la calidad de voz, pero solo está disponible para la lengua extranjera inglés (Daengsi, Khitmoh, & Wuttidittachotti, 2015).

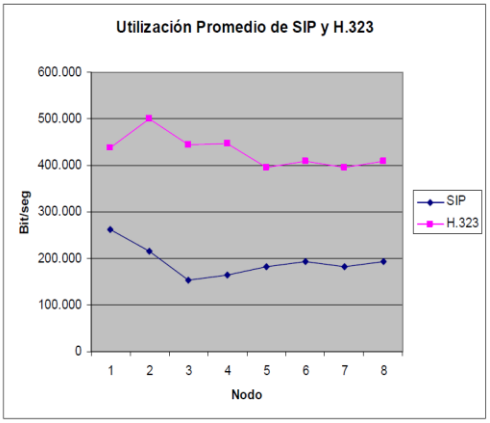
Según el ámbito de las telecomunicaciones, son un conglomerado de reglas que caracterizan los procesos afines a toma de decisiones e instrucciones al garantizar la seguridad en una labor (Valle, 2017). Así mismo, estas deben promulgarse y difundirse desde el momento de la inducción o reinducción del trabajador al puesto de trabajo, con el fin de evitar daños que puedan derivarse como consecuencia de la ejecución de un trabajo.

Por lo tanto, se deben realizar controles de ingeniería que sirvan para rediseñar los procesos de las normas de seguridad de las bases de datos, así mismo, la buena distribución de las áreas de trabajo y contar con instalaciones adecuadas dentro de la empresa. Además, en la realización de los trabajos pueden concurrir una gran variedad de posibles situaciones y circunstancias que las reglamentaciones oficiales no pueden abarcar. Lo que hace que la normativa legal, en muchos casos sea insuficiente, puesto que no puede descender a las condiciones de trabajo concretas que se dan en cada industria, o enfocada a cada necesidad que urge en el medio de las telecomunicaciones en especial afines a las bondades digitales, que carecen de un marco regulatorio nacional retroalimentado al desarrollo de nuevas tecnologías (Sánchez, 2016).

Según las normas (ISO, 2018), la información es un activo vital para el éxito y la continuidad en el mercado de cualquier empresa. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para las empresas. De modo que, para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización. ISO/IEC 27000 es un conjunto de estándares desarrollados o en fase de desarrollo por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de empresa, pública o privada, grande o pequeña.

La utilización de los protocolos no solo depende de sus virtudes, sino de las cualidades que demanda el proyecto; en breves rasgos H.323 es más completo, mientras que SIP es más versátil/simple al desarrollar redes VoIP.

Figura 11: Uso de estándares para redes VoIP



Fuente: (Orellana, 2006)

Así, en este apartado se resumen las distintas normas que componen la serie ISO 27000 y se indica cómo puede una empresa implantar un sistema de gestión de seguridad de la información (SGSI) basado en ISO 27001. ISO/IEC 27001 publicada el 15 de octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. En esta norma, se enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles, la empresa deberá argumentar sólidamente la no aplicabilidad de los controles no implementados (ISO 27000, 2012).

Además, la norma ISO 27001, es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información (Casas & Pérez-Cépeda, 2016), con base en esta definición se deduce que al implementar este sistema la empresa tendrá conocimiento de cuál es su estado de seguridad, de poder tomar medidas para mitigar los riesgos, también tienen la opción de controlar y evaluar si esas medidas fueron efectivas o no, esto conlleva al mejoramiento continuo.

Seguridad en base de datos

La metodología que se debe aplicar en las normas de seguridad de las bases de datos es proteger la información de ataques maliciosos, la causa por lo que se presentan errores en la seguridad de base es por la falla de procedimientos sencillos que a pasar el tiempo se convierten en grandes inconvenientes que afectan en lo concerniente a la seguridad de la información. Desde este punto de vista, se debe concientizar a todos los elementos que conforman las empresas, sobre la importancia de mantener normas de seguridad informática (Navarro Bustos, Jairo René, 2014).
Por lo tanto, para comenzar un análisis de la seguridad de los datos, se necesita establecer conceptos básicos de seguridad informática. Pues, según (Almeida Freire, 2017) se la define generalmente ..”toda acción destinada a salvaguardar la disponibilidad, acceso e integridad de información, proteger de la revelación no autorizada, de la modificación, su destrucción accidental o intencional, e incapacidad para procesar datos”, pero se debe manejar un concepto más amplio en el que se incluyan tanto los procedimientos como maneras de preservar la información, por lo que se podría añadir que…se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios” (Arcentales-Fernández & Caycedo-Casas, 2017).

Políticas de seguridad informática

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de

información. Estos riesgos que se enfrentan han llevado a que se desarrolle un documento de directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de las empresas (Arístides Dasso, 2018).

Las principales falencias en seguridad en redes VoIp se resumen en la tabla 1.

Tabla 1. Vulnerabilidades en sistemas VoIP

CAPA	VULNERABILIDAD
Políticas y consejos	Contraseñas débiles Accesos indebidos
Seguridad Física	Degeneración de equipos Falta de rigor en control de personal
Seguridad en red	Distribute Denial of service IMCP inalcanzable SYN Floods Variedad de floods
Servicios	DOS Inyección SQL
Sistema operativo	Malas configuraciones Gusanos y virus Bobnet
Protocolos VoIP	Fraudes SPAM Phishing Fuzzing Flodds Secuestro de sesiones Intercepciones de llamadas

Fuente: (Vásquez Costales, 2013)

Actualmente la mayoría de las empresas están realizando inversiones para crear directrices de seguridad informáticas para implantarlas en documentos que definan las reglas de las mismas, muy pocas empresas alcanzan el éxito, ya que una de las barreras que se enfrenta es tratar de conseguir que los altos ejecutivos ejecuten estas políticas y hacerles ver la necesidad y beneficios que implican contar con buenas políticas de seguridad informática. Finalmente, podemos decir que contar con políticas de seguridad informática ayuda a minimizar los riesgos en la pérdida de información de las empresas.

METODOLOGÍA

Se aprecia que la naturaleza de la investigación es dinámica e interdisciplinaria, exigiendo un método sistematizado que faculte estudiar de forma holística las variables que describen la eficacia en políticas de seguridad, en virtud de las potencialidades afines a VoIp; se opta por DELPHI gracias a que permite establecer objetivos, concretar y sintetizar datos mediante procesos comparativos conjugados en un análisis abductivo.

Los procesos empleados son:

Análisis Abductivo: Permite sumar conocimiento mediante conjeturas tomadas de otros autores, bajo un mismo contexto que establezca nuevas relaciones entre las variables estudiadas (Ambrosio, Año 2018).

Matriz Comparativa: Es una síntesis de las diferentes virtudes tangibles en forma cualitativa o cuantitativa, en VoIP permite sintetizar objetivos en forma apreciable al lector (Wilches-Cortina, Cardona-Peña, & Tello-Portillo, 2017).

Estadístico descriptivo: Consiste en interpretar series de datos, a través de medidas de tendencia para inferir el comportamiento de las variables e inhibir relaciones convergentes entre las premisas expuestas en el análisis (Acosta, Pacheco, Jiménez, & Ochoa, 2018).

Delphi: Es un proceso sistemático que permite identificar variables, elaborar instrumentos de valoración, analizar en forma objetiva mediante opiniones de profesionales entendidos en la materia e integrar saberes progresivamente al retroalimentar los resultados, hasta argumentar las conjeturas planteadas en la investigación (M.E. García-Ruiz, 2018).

Tabla 2. Matriz comparativa entre protocolos de VoIP en torno a seguridad

Parámetro	Calidad	Cifrado	Detección
H.323	Alta	alta	Regular
SIP	alta	Regular	Regular
Cita	(Sonwane & Chandavarkar, 2013)	(V.Srihari & Kalpana, 2014)	(Filip Rezac & Bajakova, 2016)

Fuente: Elaboración Propia

El emplear protocolos como el SIP reduce posibilidades de ataques y espionaje, pero se debe conjugar con otras alternativas a modo escalable para prevenir del todo posibles infiltraciones, una solución es cifrar los paquetes de datos en tiempo real (Leonardo Carjaval & Rawa, 2016).

Tabla 3. Principales falencias en SIP

Ataque	Espionaje	Intromisión
Resultados	Hackeo	Hombre en medio
Vulnerabilidades	Fallo en seteo	Virus, claves
Contra medidas	Protocolos en tiempo real	Cifrado asimétrico

Fuente: (Rehman & Abbasi, 2014)

La encuesta se encuentra dirigida a los responsables de la seguridad en sistemas VoIP, en las principales empresas tanto públicas como privadas de la ciudad de Machala; radiodifusoras, instituciones educativas, entidades bancarias, cooperativas de transporte, proveedoras de tecnologías/servicios o comercio donde gestiones necesidades IP a través de multimedia.
La encuesta planteada, se deriva de una serie de preguntas denotadas en trabajos similares; orientadas a evaluar las premisas propuesta en este escrito tomando como muestra a 100 encuestados, debido al tamaño de la población y que se requiere criterio de expertos, cuyo juicio deriva de su pericia e integró desempeño en el área.

Tabla 4: Reactivos usados en la encuesta

Pregunta 1	¿Indique qué protocolos utiliza en su paquetería VoIP?
Pregunta 2	¿Aplican cifrado en contraseñas/caracteres o combinaciones complejas?
Pregunta 3	¿Indique cuales vulnerabilidades físicas registra con mayor riesgo y frecuencia?
Pregunta 4	¿Cuáles amenazas considera de mayor prioridad en la seguridad de red?
Pregunta 5	¿Cuál protocolo considera Ud. que brinda mejor protección para detectar bonet, gusanos, virus o malas configuraciones?
Pregunta 6	¿Cuál de las siguientes vulnerabilidades considera más perniciosa para los servicios VoIP?
Pregunta 7	¿Cuenta con los medios para inspeccionar la paquetería de datos en tiempo real en el servicio VoIP?
Pregunta 8	¿Con qué protocolo experimenta mayor flexibilidad y escalabilidad en enlaces multimedia?
Pregunta 9	¿Qué protocolo facilita el cifrado de paquetería en llamadas VoIP?
Pregunta 10	¿Qué medidas de protección, configuraciones o herramientas para garantizar la seguridad en servicio VoIP?

Fuente: (SantaCruz, 2008)

ANÁLISIS DE RESULTADOS

En función de las opiniones registradas y deducciones estimadas mediante la estadística descriptiva se tiene:

Tabla 5: Tabulación de la encuesta

No	OPCIONES	%
1	SIP	35
	H.323	65
2	SI	70
	NO	30
3	Control al personal	50
	Degeneración de equipos	30
	Accesos indebidos	20
4	DDOS	20
	SYN Floods	10
	Inyección SQL	40
	Hackeos	30
5	H.323	68
	SIP	32
6	SPAM	4
	Phising	30
	Fuzzing	6
	Floods	12
	Secuestro de sesiones	20
	Intercepción de llamadas	28
7	SI	40
	NO	60
8	H.323	75
	SIP	25
9	H.323	70
	SIP	30
10	Red fast flux	7
	Encriptado de paquetes	18
	Redes privadas	40
	Contraseñas fuertes	35

Fuente: Elaboración Propia

La mayoría prefiere al protocolo H.323 gracias a sus bondades destinadas a la seguridad, mayores prestaciones, aunque mayor grado de complejidad en contraste con el estándar SIP; en cuestiones de cifrado el 70% lo prefieren, por ser una solución versátil, económica y factible; además los protocolos como H.323 incorpora módulos que facilitan el encriptado de datos.

El protocolo H.323 posee mejores características en términos de seguridad, como cifrado, escalabilidad, señalización y enrutamiento de paquetería, esto lo hace más tedioso; pero a su vez más flexible que el SIP al resguardar la integridad de datos, esto no opaca la facilidades que presta el servicio VoIP por ser entendible para el lenguaje humano y su capacidad de amalgamar nuevas implementaciones digitales; además el protocolo

H.323 es abarcativo e integrador recogiendo y amalgamando bondades de otros estándares, gracias a esto el 68% lo considera más favorable; sin embargo también es complejo dificultando las configuraciones pero facilitando la detección de amenazas, en contraste con el SIP que da una solución rápida pero descuida la protección frente agentes externos.

El protocolo SIP es adaptable y compatible con H.323, difieren en su grado de respaldo a datos, por ello es más efectivo usar H.323 para encriptar datos en los paquetes, al realizar configuraciones de mayor complejidad; el SIP favorece una solución rentable y óptima, pero descuida la seguridad al soportar redes de grandes áreas o empresas con múltiples sucursales/departamentos.
En lo referente a vulnerabilidades el 40% de la población, considera los ataques SQL como más peligrosos, debido a que son letales para cualquier sistema IP, aproximadamente un tercio piensa que los hackeos son las amenazas de mayor intensidad, en un rango menor el DDOS y SYN Floods; un aspecto a tener en cuenta es que la ausencia detonante para efectuar el ataque no es motivo para descuidar la seguridad; gracias a que la mayoría de ataques como phishing e intercepciones derivan de desatenciones; el 20% competen a secuestro de sesiones por terceros, 12% saturación de la red y en menor relevancia el SPAM por publicidad o anuncios vía internet.

La auditoría interna/retroalimentar la seguridad es un principio clave de prevención, por ello el 60% realiza inspecciones para asegurar que no sufran sabotaje u otros ataques; esto evidencia que a más de la infraestructura tecnológica hace falta cultura en la seguridad digital y protección de información personal o institucional. Los sistemas informáticos ostentan seguridad, en torno a la ética de sus operadores, por lo tanto, la mitad de dicha labor es capacidad/regular/controlar al personal; en un 30% de los casos mantener en óptimas condiciones a los equipos y accesos no autorizados.

La forma más factible de contrarrestar las falencias, resultó ser las redes privadas evitando ataques externos; medidas como cambio periódico de dominio IP o encriptado son menos empleadas por ser más complicadas/costosas por demandar un conocimiento especial sobre la temática; por ende se opta en un 35% contraseñas fuertes como medio eficiente; en general el empoderamiento institucional es clave al evitar falencias en la seguridad; debido a que el factor humano no es predecible ni responde a políticas de seguridad, salvo su propio criterio en comparación con la sinergia colectiva que posee la tecnología digital.

CONCLUSIONES

Los protocolos otorgan cierto grado de seguridad en relación a las potencialidades del sistema, sin embargo, se hallan condicionados por el nivel de seguridad física, lógica e interfaces que facultan la comunicación VoIP, gracias a que por sí solos los estándares no derogan confiabilidad sino la integración de todos sus componentes en forma conjunta y transparente.

El protocolo H.323 es una reglamentación más completa a la vez que compleja, brinda mejores prestaciones en contraste con sencillez y agilidad que ofrece SIP; en términos de protección H.323 presta mayor eficacia al ser más versátil en cuestiones de cifrado e interconectividad de servicios multimedia.

Se observa en la relación entre variables que actualmente existe poca tecnificación y concientización sobre la relevancia de la seguridad en sistemas informáticos, haciendo hincapié en la comunicación digital; debido a la falta de casos o percances que demanden su fortificación en torno a las bondades VoIP.

En función de las encuestas se nota que el protocolo H.323 es mejor, gracias a cuestiones de tamaño de red e integra mejores potencialidades al proteger la paquetería de datos; también se evidencia que es requerido una actualización en bondades tecnológicas afines a los servicios voz y datos, capacitar al personal e integrar programas de auditoría para dinamizar el sistema de seguridad de toda la infraestructura informática.

Las vulnerabilidades de mayor riesgo son las humanas; seguidas por espionaje, inyección SQL, phishing e intentos de hackeo ya sea por virus, botnet u otro agente externo; esto demuestra que la seguridad va más allá del protocolo exigiendo hoy en día un estudio, capaz de armonizar calidad, prestaciones, relación beneficio/costo en sistemas IP.

Referencias Bibliográficas

Acosta, R. H., Pacheco, K. P., Jiménez, F. R., & Ochoa, G. V. (2018). Análisis Estadístico Descriptivo e Inferencial de la Velocidad y Dirección del viento en la Costa Caribe Colombiana. Espacios, 3-15.

Ahangari, F. M. (2016). A new SIP authentication scheme by incorporation of elliptic curve cryptography with ticket server. 2nd International Congress on Technology. Communication and Knowledge, ICTCK, 447-454.

Almeida Freire, A. L. (2017). La ciberseguridad, y su incidencia en las políticas de la seguridad de la información de la armada del Ecuador. Universidad de las Fuerzas Armadas ESPE, 306-323.

Ambrosio, M. E. (Año 2018). Diagnóstico en Psicoanálisis: ¿Lógica Abductiva? II Congreso Internacional de Psicología - V Congreso Nacional de Psicología "Ciencia y Profesión" (págs. 448-456). Anuario de Investigaciones de la Facultad de Psicología.

Arcentales-Fernández, D. A., & Caycedo-Casas, X. (2017). Auditoría informática: un enfoque efectivo. Dominio de las Ciencias Vol. 3, 157-173.

Aristides Dasso, A. F. (2018). Evaluación de la Seguridad en Sistemas Informáticos. Universidad Nacional de San Luis - XX Workshop de Investigadores en Ciencias de la Computación, 1016-1020.

Arjun, A. &. (2014). Real Time Implementation of Elliptic Curve Cryptography Over a Open. Hefei: Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT).

Ayllón, A. J. (2016). Criptografía y Seguridad en WhatsApp. Madrid: UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA.

Ayoub, B., Jamal, K., & Arsalane, Z. (2015). An Analysis and Comparative Evaluation of MFCC Variants for Speaker Identification over VoIP Networks. 2015 World Congress on Information Technology and Computer Applications (WCITCA). Hammamet, Tunisia.

Barghi, F. H. (2014). A comprehensive SPIT detection and prevention framework based on reputation model on call communication patterns. Iranian Conference on Intelligent Systems ICIS, 188-193.

Barry, M. A. (2017). Challenges of integrating a VoIP communication system on a VSAT network. 19th International Conference on Advanced Communication Technology (ICACT), 275-281.

Borbúa, R. V., Herrera, L. R., & Ch, R. P. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. URVIO, Revista Latinoamericana de Estudios de Seguridad, 31-45.

Carvajal, E. T. (2018). TECNOLOGÍAS, SEGURIDAD INFORMÁTICA Y DERECHOS HUMANOS. IUS ET SCIENTIA (ISSN: 2444-8478) 2018, Vol.4, nº 1, 19-39.

Casas, J. B., & Pérez-Cépeda, M. (2016). El ISO 9001 y TQM en las empresas de Ecuador. GCG Globalización, competitividad y gobernabilidad, 153-176.

Chuquitarco, M., Villegas, J., Jácome, D., & Castillo, J. (2017). Topología experimental de red con máquinas virtuales para la Interoperabilidad entre plataformas de voz IP multimarca bajo Norma ISO 27002:2005. Revista Publicando, 4 No 11, 20-41.

Costales, P. V. (2015). Análisis del protocolo SSL y su aplicación en el aseguramiento de tráfico de VoIP frente a los ataques de Eavesdropping. Obtenido de http://dspace.espoch.edu.ec/handle/123456789/4030

Daengsi, T. K. (2015). VoIP quality measurement: subjective VoIP quality estimation model for G. 711 and G. 729 based on native Thai users. Multimedia Systems. . Obtenido de https://doi.org/10.1007/s00530-015-0468-3

Dakur, A., & Dakur, S. (2015). Eavesdropping and Interception Security Hole and Its solution over VoIP Service. 2014 IEEE Global Conference on Wireless Computing and Networking (GCWCN) (págs. 6-10). Lonavala, India: IEEE.

Estrada, J. C. (2016). Seguridad de la Telefonía IP en Ecuador: Análisis en Internet. ENFOQUE UTE, 25-40.

Filip Rezac, J. R., & Bajakova, Z. (2016). Analysis of the IP Telephony Security

Issues Using Automatic Neural Network Classifier. 2016 24th International Conference on Software, Telecommunications and Computer Networks (SoftCOM). Split, Croatia: IEEE.

Ghazali, A. J.-N.-A.-T. (2016). Building IPv6 based tunneling mechanisms for VoIP security. 13th International Multi-Conference on Systems, Signals and Devices, SSD, (págs. 171-176).

Guaña-Moya, J., & Muirragui-Irrazábal, V. (2018). Servicios y aplicaciones de voz sobre ip utilizando el estándar H.323. Polo del Conocimiento, 343-355.

Gurung, S. &. (2015). Healthcare Privacy: How Secure Are the VOIP/Video-Conferencing Tools for PHI Data? Proceedings. Aesthetic Plastic Jorunal, 574-579.

Guzmán García, A. &. (2015). Diseño de un Sistema de gestión de la seguridad informática - SGSI - para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá s través de la auditoría. Medellín: Universidad Abierta y a Distancia.

Hao, Y. J. (2014). OpenSSL heart bleed: Security management of implements of basic protocols. Proceedings. 9th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (págs. 520-524). GUANGZHOU, 3PGCIC.

Hernández, J. M., López, C. A., & Acosta, C. A. (2016). ROPUESTA DE UNA PIZARRA ASTERISK EN LA UNIVERSIDAD DE CIENFUEGOS. Compromisos, T., Desafíos, R. Y., & Educación, D. E. L. A., 210-217.

Hosseinpour, M. S. (2016). Modeling SIP normal traffic to detect and prevent SIP-VoIP flooding attacks using fuzzy logic. 6th International Conference on Computer and Knowledge Engineering, ICCKE. Mashhad: IEEE EXPLORED.

Husák, M. Č. (2015). Network-based HTTPS client identification using SSL/TLS fingerprinting. Proceedings. 10th International Conference on Availability, Reliability and Security, (págs. 389-396). https://doi.org/10.1.

IES Luis Vélez de Guevara. (2018). Gestión de Bases de Datos, Versiòn 1.0. Sevilla: Departamento de informàtica.

ISO. (febrero de 2018). 27000:2018. Obtenido de https://www.iso.org/standard/73906.html

Jouini, M. R. (2014). Classification of security threats in information systems. Procedia Computer Science, 32, 489-496.

Karotiya, N. A. (2016). Review paper on point to point communication with the use of power over Ethernet based on VOIP system on asterisk. 2nd International Conference on Advances in Electrical, Ele. Tokyo University of Information Sciences.

Korczyński, M. &. (2014). Markov chain fingerprinting to classify encrypted traffic. IEEE INFOCOM, 781-789.

Le Xu, D. H. (2014). Cloud-based virtual laboratory for network security education. IEEE Transactions on Education, 57(3), 145-150.

Leonardo Carjaval, L. C., & Rawa, D. (2016). Detecting unprotect SIP Based voice over IP traffic. 4TH international symposium on digital forenses and security (págs. 25-27). IEEE.

Lukša, D. F. (2014). Sound quality assessment in VOIP environment. 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2014 (págs. 1066-1070). Opatija, Croatia.: Institute of Electrical and Electronics Engineers (IEEE).

M.E. GARCÍA-RUIZ, F. L.-A. (2018). Aplicación del metodo delphi en el diseño de una investigación cuantitativa sobre el fenómeno FABLAB. EMPIRIA. Revista de Metodología de Ciencias Sociales. N.o 40, 129-166.

Martínez, E. U. (2017). Infraestructura de señalización para proporcionar servicios audiovisuales en un emulador de redes. Léganes: Universidad Carlos III de Madrid.

Mazalek, A. V. (2015). Analysis of the impact of IPSec on performance characteristics of VoIP networks and voice quality. ICMT 2015 - International Conference on Military Technologies 2015. Brno, Czech Republic: https://ieeexplore.ieee.org/document/7153703.

Molina-Izurieta, R. E., & Pazmiño-Ramírez, J. E. (2017). Diseño de un servicio PBX hospedado en un servidor virtual privado VPS en la nube para uso de

empresas pymes que no cuentan con servicios de telefonías de VoIP. Dominio de las Ciencias Vol. 3, núm. 2, 866-889.

Montazerolghaem, A. S.-M. (2014). A novel load scheduling for session initiation protocol networks. 4th International Conference on Computer and Knowledge Engineering, ICCK (págs. 1-15). Hongbo Jiang: Huazhong University of Science and Technology.

Nikoukar, A., Hwang, I.-S., Liem, A. T., & Lin, Y.-H. (2015). Local-Aware H.323-based VoIP service in EPON. Proceedings. 5th International Conference on Electrical Engineering and Informatics: Bridging the Knowledge between Academic, Industry, and Commun. Denpasar, Indonesia: https://ieeexplore.ieee.org/document/7352581.

Orellana, G. R. (2006). Análisis de seguridad de transferencia de VoIP y desempeño de los protocolos en redes con clientes inalámbricos. Guayaquil: ESCUELA SUPERIOR POLITÈCNICA DEL LITORAL.

Pesantez, D. F., Aucancela, J. K., Auncancela, A. L., & Mantilla, C. E. (2017). Modelo de Seguridad contra ataques de denegación de servicio para tráfico SIP. Revista Tecnológica ESPOL, 167-178.

Rehman, U. U., & Abbasi, A. G. (2014). Security Analysis of VoIP Architecture for Identifying SIP Vulnerabilities. Conference: Emerging Technologies (ICET), 2014 10th International Conference on (págs. 87-93). Islamabad, Pakistan: IEEE.

Saad Saleh a, ⇑. Z. (2014). Improving QoS of IPTV and VoIP over IEEE 802.11n. Computers and Electrical Engineering, 2-20.

SÁNCHEZ, J. L. (2016). ANÁLISIS REGULATORIO Y COMERCIAL PARA EL DESARROLLO DE SERVICIO DE CLOUD COMPUTING PARA LA PROVINCIA DE EL ORO – ECUADOR. Guayaquil: ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL.

SantaCruz, M. S. (2008). Diseño de una infraestructura de red convergente para la empresa Uniphone S.A. Quito; Ecuador: Escuela Politècnica Nacional.

Singh, H. P. (2014). VoIP: State of art for global connectivity - A critical review. Journal of Network and Computer Applications, 37(1), 365-379.

Sonwane, G. D., & Chandavarkar, M. B. (2013). Security Analysis of Session Initiation Protocol in IPv4 and IPv6 based VoIP network. 2013 Second International Conference on Advanced Computing, Networking and Security (págs. 187-192). IEEE.

Thuayabat, N., Tangwongsan, S., & University, M. (2015). A security model of voice eavesdropping protection over SIP-based VoIP with XTR cryptography. Proceedings of the 2015 12th International Joint Conference on Computer Science and Software Engineering, JCSSE 2015. (págs. 207-211). http://repository.li.mahidol.ac.th/dspace/handle/123456789/35819.

Tintín-Perdomo, V. P., Caiza-Caizabuano, J. R., & Caicedo-Altamirano, F. S. (2018). Arquitectura de redes de información. Principios y conceptos. Dominio de las Ciencias, 103-122.

V.Srihari, & Kalpana, P. (2014). Security Aspects of SIP based VoIP Networks: A Survey. 2nd International Conference on Current Trends in Engineering and Technology, ICCTET'14 (págs. 143-150). Coimbatore, India: IEEE Conference Number - 33344.

VALLE, C. J. (2017). *ESTUDIO DEL COMPORTAMIENTO DE UN SERVIDOR DE VoIP BASADO EN RASPBERRY PI Y SU INCIDENCIA EN LA COBERTURA PARA CLIENTES MÓVILES EN REDES WiFi.* Guayaquil: ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL.

Vásquez Costales, P. (2013). *Análisis del protocolo SSL y su aplicación en el aseguramiento de tráfico de VoIP frente a los ataques de Eavesdropping.* Riobamba: Escuela Superior Politécnica de Chimborazo.

Villavicencio-Caparó Ebingen, A.-C. M., Mireya, C.-L. K.-C., Karla, Z.-O., & Frank, W.-C. (2017). EL TAMAÑO MUESTRAL PARA LA TESIS. ¿CUÁNTAS PERSONAS DEBO ENCUESTAR? *OACTIVA UC Cuenca. Vol. 2, No. 1*, 59-62.

Wilches-Cortina, J. R., Cardona-Peña, J. A., & Tello-Portillo, y. J. (2017). A VoIP call classifier for carrier grade based on

Support Vector Machines. *Revista DYNA, 84(202)*, 75-83.