



Universidad Tecnológica ECOTEC Facultad de Ingenierías

Título del trabajo:

Implementación de un sistema de telefonía VoIP con política de QoS para mejorar la comunicación empresarial de SEPRIVZAM CIA.

Línea De Investigación:

Tecnologías de la Información y la Comunicación

Modalidad de titulación:

Propuesta Tecnológica

Carrera:

Ingeniería en Sistemas

Título a obtener:

Ingeniero en sistemas con énfasis en Administración de redes

Autor (a):

Leonardo Manuel Fariño Díaz

Tutor (a):

PhD. Marcos Espinoza Mina

Samborondón – Ecuador

2023

Dedicatoria

Dedico esta tesis a Dios, porque la inspiración divina siempre me guía por el buen camino de todo corazón. Gracias a Dios por darme la fuerza y sabiduría para realizar este proyecto. A mis padres, su amor incondicional, apoyo y sacrificio ha sido un pilar fundamental en mi camino, gracias por creer en mí, por sus palabras de aliento y por ser mi ejemplo de constancia. Este logro también demuestra su amor y dedicación. A mi esposa, por ser mi roca, su inquebrantable apoyo y paciencia es mi mayor motivación. Gracias por su comprensión durante mi ausencia y por ser mi mayor inspiración para alcanzar mis sueños. Su cariño y aliento han hecho que cada paso de este viaje sea significativo, por su aguante y amor eterno. Esta tesis no hubiera sido posible sin su amor, ánimo y confianza en mí. Espero que esta dedicatoria te haga sentir lo importante que eres en mi vida y lo agradecido que estoy por todo lo que has hecho por mí.

Dedico este trabajo también a mis estimados maestros, su conocimiento, orientación y tutoría fueron esenciales en mi aprendizaje. Gracias por compartir su sabiduría, por desafiarme a crecer y por darme las herramientas para enfrentar los desafíos intelectuales. Su dedicación ha dejado una huella imborrable en mi camino.

Hoy, con humildad y gratitud, dedico esta tesis a cada uno de ustedes. Su influencia y apoyo fueron esenciales para mi éxito académico. Que esta dedicatoria refleje mi profundo aprecio y reconocimiento de su importancia para mi vida.

Agradecimiento

Quiero expresar mi más profunda gratitud a Dios. Estoy agradecido de tenerlo como guía y fuente de fortaleza en cada paso de este viaje educativo. Tu amor y sabiduría me han sostenido y me han dado la confianza para perseverar en los momentos difíciles. A mis queridos padres, su inmenso apoyo y constante amor ha sido mi mayor motivación. Gracias por creer en mí, darme las oportunidades que necesito y apoyarme para hacer realidad mis sueños. Para mi amada esposa, su apoyo y comprensión infinitos han sido mi mayor fortaleza. Gracias por estar a mi lado, animándome en los momentos difíciles y siendo mi fiel compañera en este camino de desarrollo. Estimados maestros, MSc. Ana María Arellano, MSc. Erika Asensio, MSc. Manuel Ramírez, MSc. Antonio Rodríguez, MSc. David Benavides, PhD. Alejandra Colina y PhD. Marcos Espinoza, tu conocimiento, dedicación y guía han sido fundamentales para mi desarrollo académico. Gracias por compartir sus experiencias, por desafiarme a alcanzar mi máximo potencial y por brindarme las herramientas que necesito para completar desafíos académicos. Les agradezco sinceramente a todos por su contribución a mi desarrollo académico y personal. Sus enseñanzas y apoyo han tenido un impacto duradero en mi vida y el éxito de este logro.

Que este agradecimiento exprese mi más profundo respeto y gratitud a cada uno de ustedes, y que celebremos muchos éxitos juntos en el futuro.

Certificado de Revisión final



ANEXO N° 14

CERTIFICADO DE APROBACIÓN DEL TUTOR PARA LA PRESENTACIÓN A REVISIÓN DEL TRABAJO DE TITULACIÓN

Samborondón, 09 de Julio de 2023

Magister
Erika Ascencio Jordán
Decana de la Facultad
Ingeniería.
Universidad Tecnológica ECOTEC

De mis consideraciones:

Implementación de un sistema de telefonía VoIP con política de QoS para mejorar la comunicación empresarial de SEPRIVZAM CIA. según su modalidad Propuesta Tecnológica; fue revisado, siendo su contenido original en su totalidad, así como el cumplimiento de los requerimientos establecidos en la guía para la elaboración del trabajo de titulación, Por lo que se autoriza a: Fariño Díaz Leonardo Manuel, para que proceda a su presentación para la revisión de los miembros del tribunal de sustentación.

ATENTAMENTE,



PhD. Marco Espinoza Mina

Tutor

Certificado de Coincidencias de Plagio



CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS

Habiendo sido nombrado PhD. Marco Espinoza Mina, tutor del trabajo de titulación "Implementación de un sistema de telefonía VoIP con política de QoS para mejorar la comunicación empresarial de SEPRIVZAM CIA." elaborado por Sr. Leonardo Manuel Fariño Díaz con mi respectiva supervisión como requerimiento parcial para la obtención del título de Ingeniero en sistemas con énfasis en Administración de redes.

Se informa que el mismo ha resultado tener un porcentaje de coincidencias 4 (%) el mismo que se puede verificar en el siguiente link: (copiar y pegar el https del resultado). Adicional se adjunta print de pantalla de dicho resultado.

CERTIFICADO DE ANÁLISIS
Original

Implementación de un sistema de telefonía VoIP con política de QoS para mejorar la comunicación empresarial de SEPRIVZAM CIA.

4% Coincidencias
+ Se. Tienen entre paréntesis los porcentajes por coincidencia.
Se. Tienen en negrilla.

Documento: TITULO DE INGENIERO EN SISTEMAS CON ENFASIS EN ADMINISTRACION DE REDES
Tamaño del documento original: 1534 NPT
Autor: LEONARDO MANUEL FARIÑO DIAZ

Supervisor: LEONARDO MANUEL ESPINOZA MINA
Fecha de depósito: 07/02/2023
Tipo de carga: NPT (Administración)
Fecha de fin de análisis: 07/02/2023

Sumario de palabras: 21,228
Número de palabras: 108,001

Métrica de las coincidencias en el documento

Fuentes
Fuentes principales detectadas

Nº	Descripción	Similitud	Utilización	Estado actualizado
1	Implementación de un sistema de telefonía VoIP con política de QoS para mejorar la comunicación empresarial de SEPRIVZAM CIA.	4.0%		Fecha de depósito: 07/02/2023
2	Implementación de un sistema de telefonía VoIP con política de QoS para mejorar la comunicación empresarial de SEPRIVZAM CIA.	4.0%		Fecha de depósito: 07/02/2023
3	Implementación de un sistema de telefonía VoIP con política de QoS para mejorar la comunicación empresarial de SEPRIVZAM CIA.	4.0%		Fecha de depósito: 07/02/2023
4	Implementación de un sistema de telefonía VoIP con política de QoS para mejorar la comunicación empresarial de SEPRIVZAM CIA.	4.0%		Fecha de depósito: 07/02/2023



FIRMA DEL TUTOR
PhD. Marco Espinoza Mina

Resumen

El presente trabajo de titulación trata sobre el problema del control de llamadas telefónicas en la empresa SEPRIVZAM CIA, la cual carece de un sistema de grabación de llamadas para mejorar la comunicación entre colaboradores. Esta falta de control puede generar malentendidos y problemas de servicio entre ellos. La solución recomendada es implementar un sistema telefónico VoIP con políticas de calidad de servicio (QoS) basado en seguridad. Esto implicará pasar del actual sistema de telefonía analógica a un sistema digital basado en VoIP, ofreciendo beneficios como mayor control, menores costos y flexibilidad en la gestión de las comunicaciones. Para ello se utilizó una metodología del Project Management Institute (PMI) lo que permite un enfoque de satisfacción en las necesidades y expectativas de las partes interesadas del proyecto, e incrementar las probabilidades de éxito del proyecto. Adicionalmente, se aplicaron técnicas de investigación como entrevistas y encuesta con el objetivo de obtener información necesaria para alcanzar los objetivos planteados. Se utilizó un computador como servidor de Voice over Internet Protocol (VoIP), con la implementación de la central telefónica Issabel, Private Branch Exchange (PBX) y la adopción de políticas de QoS, basadas en seguridad, que brinda una mayor escalabilidad y flexibilidad, adaptándose a las necesidades cambiantes de la empresa aportando un mayor control y seguimiento de las llamadas, mejorando la eficiencia, la calidad y seguridad del servicio de comunicación interna y externa. Las pruebas y validaciones realizadas demuestran que el sistema de telefonía VoIP con políticas de QoS basado en la seguridad de la empresa, cumple con los objetivos propuestos para mejorar su operación, calidad de servicio y rentabilidad, posicionándola de manera competitiva en el mercado actual.

Palabras claves: Issabel, QoS, comunicación, seguridad, políticas.

Abstract

The present degree work deals with the problem of telephone call control in the company SEPRIVZAM CIA, which lacks a call recording system to improve communication between employees. This lack of control can generate misunderstandings and service problems among them. The recommended solution is to implement a VoIP telephone system with security-based quality of service (QoS) policies. This will involve moving from the current analog telephone system to a digital VoIP-based system, offering benefits such as greater control, lower costs and flexibility in communications management. A Project Management Institute (PMI) methodology was used to achieve this, allowing a focus on satisfying the needs and expectations of the project's stakeholders and increasing the probability of project success. In addition, research techniques such as interviews and surveys were applied to obtain the information necessary to achieve the objectives set. A computer was used as a Voice over Internet Protocol (VoIP) server, with the implementation of the Issabel telephone exchange, Private Branch Exchange (PBX) and the adoption of QoS policies, based on security, which provides greater scalability and flexibility, adapting to the changing needs of the company, providing greater control and monitoring of calls, improving efficiency, quality and security of internal and external communication service. The tests and validations carried out show that the VoIP telephony system with QoS policies based on the company's security, meets the proposed objectives to improve its operation, quality of service and profitability, positioning it competitively in the current market.

Keywords: Issabel, QoS, communication, security, policies.

Índice

Dedicatoria	I
Agradecimiento	II
Certificado de Revisión final.....	III
Certificado de Coincidencias de Plagio	IV
Resumen	V
Abstract	VI
Índice	VII
Índice Tabla	XIV
Índice Figura	XIV
Introducción.....	1
Antecedentes	3
Planteamiento del problema	3
Pregunta Problemática.	5
Objetivo de la propuesta Tecnológica.....	5
Objetivo General.	5
Objetivos Específicos.	5

Alcance.....	5
Justificación.....	6
Capítulo 1	8
1. Marco Teórico	8
1.1 Comunicación	9
1.1.1 Comunicación Organizacional	9
1.2. Telefonía tradicional	10
1.3. Redes Computacionales	10
1.4. PBX VoIP	11
1.4. 1. Telefonía VoIP	11
1.4.2 Característica de VoIP.	13
1.4.3. Ventajas de VoIP.	14
1.4.4. Desventaja de VoIP	15
1.5. Issabel	16
1.5.1. Característica de Issabel	16
1.5.2. Comparación de Elastix con Issabel.....	17
1.6. Calidad de servicio (QoS)	19
1.6.1. Función de QoS	20

1.6.2. Beneficios de QoS	20
1.6.3. Implementación de QoS	22
1.6.4. Técnicas de QoS.....	23
1.6.5. Herramientas para evaluar QoS	23
1.6.6. TCPdump	24
1.6.7. NetworkMiner	24
1.6.8. Wireshark	24
1.6.9. Comparativas de herramientas de para medir los parámetros de QoS ...	25
1.7. Softphones	26
1.7.1 Funcionamiento de Softphone VoIP	26
1.7.2. Ventajas de utilizar un softphone VoIP	27
1.7.3. X-lite.....	28
1.7.4. 3CX.....	28
1.7.5. Zoiper.....	28
1.7.6. Linphone.....	28
1.7.7. Comparación de Softphone IP	29
Capítulo 2	30
2. Metodología del proceso de desarrollo de la propuesta tecnológica	30

2.1. Enfoque de la Investigación	31
2.1.1. Investigación Cualitativa.....	32
2.1.2. Investigación Cuantitativa	32
2.2. Métodos de Investigación.....	32
2.2.1. Investigación Descriptiva.....	33
2.2.2. Investigación Explicativa	33
2.3. Variables de Investigación.....	34
2.3.1. Variable Independiente	34
2.3.2. Variable Dependiente	35
2.4. Período y lugar donde se desarrolla la propuesta tecnológica	36
2.4.1. Periodo	36
2.4.2. Lugar.....	36
2.5. Universo y Muestra	37
2.5.1. Universo	37
2.5.2. Muestra.....	37
2.6. Métodos e Instrumento de la investigación	38
2.6.1. Entrevistas.....	39
2.6.2. Encuestas	40

2.7. Metodología de Desarrollo	40
Capítulo 3	42
3. Análisis e Interpretación de Resultados.....	42
3.1. Analizar e interpretar los resultados– Pregunta 1.....	43
3.2. Analizar e interpretar los resultados – Pregunta 2.....	43
3.3. Analizar e interpretar los resultados– Pregunta 3.....	44
3.5. Analizar e interpretar los resultados– Pregunta 5.....	45
3.6. Analizar e interpretar los resultados– Pregunta 6.....	45
3.7. Analizar e interpretar los resultados– Pregunta 7.....	46
CAPÍTULO 4	47
4. IMPLEMENTACIÓN DE LA SOLUCIÓN TECNOLÓGICA.....	47
4.1 Fase 1: Inicio	48
4.1.1. Estado de la Red De Área Local (LAN).....	48
4.1.2. Servidor	49
4.2. Fase 2: Planificación	50
4.3. Fase 3: Ejecución	50
4.3.1. Descarga e Instalación De Issabel	51
4.3.2. Creación de extensiones	54

4.3.4. Grupos de extensiones	55
4.3.4. Registros de llamadas	56
4.4. Fase 4: Supervisión y control.....	56
4.4.1. Pruebas de funcionamiento.....	57
4.4.2. Corrección de Códec de Software	57
4.4.3. Verificación de Vulnerabilidades en el Servidor	58
4.4.4. Configuración de herramientas de Vulnerabilidad	59
4.4.5. Rastrear llamadas con Wireshark.....	60
4.4.6. Reconocimiento del servidor	61
4.4.7. Aplicación de Política de QoS en Seguridad.....	62
4.4.8. Configuración de Firewall.....	63
4.4.9. Cambiar el puerto por defecto del servidor web	64
4.4.10. Configurar doble autenticación web	65
4.4.11. Configuración de servicio SSH.....	66
4.4.12. Configuración de Fail2ban	68
4.4.13. Configuración de ACL a nivel SIP	70
4.4.14. Alertas para llamadas internacionales	71
4.4.15. Alertas ante cambio de configuraciones.....	72

4.4.16. Certificación del servidor y Cliente	74
4.5. Fase 5: Cierre.	75
4.5.1. Distribución actual de la red LAN y servicios habilitados	76
4.5.2. Evaluación de resultados por experto en telefonía IP	77
4.5.3. Resultado de la implementación de las políticas QoS basado en seguridad	78
Conclusión.....	79
Recomendaciones	81
Bibliografía	82
Anexo	91
Anexo 1	91
5.1 Encuesta.....	91
Anexo 2.....	93
5.2 Entrevista.....	93
Anexo 3.....	96
5.3. Carta de autorización.....	96
Anexo 4.....	97
5.4. Cronograma de actividades.	97

Índice Tabla

Tabla 1. Comparativo de Servidor VoIP	18
Tabla 2. Comparativas de herramientas de para medir los parámetros de QoS	25
Tabla 3. Comparación de Softphone IP	29
Tabla 4. Variables de investigación.	35
Tabla 5. Resumen de departamentos, empleados, equipos y teléfonos.	37
Tabla 6. Resumen de departamentos, empleados, equipos, teléfonos y servicios de comunicaciones post implementación.	76

Índice Figura

Figura 1. Servicios de telefonía IP.	12
Figura 2. Beneficios de la tecnología VoIP.	15
Figura 3. Aplicando reglas con QoS	21
Figura 4. Fases básicas de desarrollo de proyectos	41
Figura 5. Departamento o área que pertenece	43
Figura 6. Características fundamentales para un sistema VoIP en SERVIZAM CIA.	44
Figura 7. Importancia de una QoS en las llamadas VoIP	44

Figura 8. Tipo de medidas necesarias para proteger las llamadas VoIP en el sistema	45
Figura 9. Nivel de disponibilidad en el sistema de VoIP	46
Figura 10. Funciones adicionales en el sistema de VoIP	46
Figura 11. Diagrama de red LAN de la empresa SEPRIVZAM.	48
Figura 12. Servidor que será usado para la propuesta tecnológica.....	50
Figura 13. Descarga del archivo de ISO de Issabel.	51
Figura 14. Instalación de Issabel en el computador	51
Figura 15. Configuración de Idioma de Issabel.....	52
Figura 16. Configuración del disco y versión de Issabel.	53
Figura 17. Configuración de la contraseña de usuario Root.	54
Figura 18. Creación de extensión	55
Figura 19. Configuración de Códec	58
Figura 20. Configuración de herramienta vulnerabilidad	60
Figura 21. Rastreo de llamada por el protocolo SIP	61
Figura 22. Búsqueda de puerto abierto por Nmap.....	62
Figura 23. Activación de Firewall	63
Figura 24. Cambio del puerto por defecto 443.....	65

Figura 25. Configurar doble autenticación web.....	66
Figura 26. Configuración de servicio SSH.....	67
Figura 27. Configuración de Fail2ban.....	68
Figura 28. Configuración de ACL a nivel SIP	70
Figura 29. Alertas para llamadas internacionales	71
Figura 30. Configuración de alerta de cambio	73
Figura 31. Diagrama de red LAN de la empresa SEPRIVZAM post Implementación	76

Introducción

En un mundo globalizado donde la tecnología ha avanzado claramente, la automatización de procesos ha avanzado significativamente, creando nuevos retos para las empresas. Según Koutroumpis & Llewellyn (2020), durante los últimos años, el uso y acceso a internet han sido percibidos en la sociedad, lo que ha provocado cambios trascendentales en la forma en que las personas se interrelacionan entre sí y se comunican, así como en el mercado que se ha transformado y evolucionado constantemente con productos y servicios más lucrativos. Además, las innovaciones digitales siguen evolucionando regularmente. De ahí que, existen áreas donde la tecnología no solo proporciona herramientas útiles, también ofrece una ventaja en términos de su capacidad de utilización.

De esta manera, la evolución de la telefonía ha recorrido un largo camino desde sus orígenes analógicos hasta su posterior conversión a la tecnología digital. Por ello, en 1877 Alexander Graham Bell diseñó y construyó el primer dispositivo capaz de transmitir sonido a distancia a través de señales eléctricas. Desde entonces, ha habido muchos avances y mejoras en la invención. Luego, en la década de 1960, aparecieron los teléfonos digitales en respuesta a la disminución de la calidad de la señal en largas distancias. Esta tecnología utiliza un canal digital para enviar la voz, previamente digitalizada en forma numérica, a un destino donde se convierte en una señal analógica.

Como consecuencia, hasta hace unos años, las redes de datos y las redes telefónicas coexistían, pero evolucionaron por separado debido a las tecnologías incompatibles que utilizan. Esta incompatibilidad técnica ya no existe. El desarrollo de la tecnología VoIP (Voice over IP) ha creado un sistema totalmente integrado de redes telefónicas y de datos (Cuadra, 2021). Es por esto que, el uso de centrales analógicas para gestionar las llamadas es considerado un sistema obsoleto para las empresas ya que limita en algunos aspectos como funcionalidad y escalabilidad al momento que se requiere.

Por lo tanto, la telefonía IP (telefonía sobre Protocolo de Internet) goza de un alto nivel de aceptación en las empresas debido a la facilidad de integración de todos los medios de comunicación, dispositivos de comunicación y servicios. De acuerdo a Quiroz (2018), la telefonía digital se refiere a la gestión de llamadas a través de enlaces digitales asegurando una mejor calidad de voz en distancias más largas gracias a la tecnología de telefonía VoIP brindando un servicio de bajo costo con muchas ventajas y beneficios sobre los teléfonos convencionales. Para implementar la telefonía digital, las centralitas deben gestionar las llamadas a través de un enlace digital.

Según a Júnior (2021) la telefonía digital requiere el intercambio de gestión de llamadas a través de enlaces digitales que garanticen una mejor calidad de voz en distancias más largas, ya que la telefonía VoIP ofrece un servicio de bajo costo con ventajas y desventajas más grande que una telefonía tradicional.

Otros hechos interesantes que se han destacado es que las empresas que migran a VoIP ahorran entre un 50 y 70%, las comunicaciones unificadas se reservan aproximadamente de 115 minutos diarios por trabajador, se tenía previsto que el mercado de servicios globales incrementará de 83 mil millones de dólares en 2015 a 140 mil millones para el año 2021, las telecomunicaciones están perdiendo un promedio de 700 mil usuarios de telefonía fija mensualmente (Tandel & Rughani, 2017).

Por otro lado, VoIP es la transmisión de voz a través de una red IP (Protocolo de Internet), una de las principales aplicaciones de Internet. Los servicios de VoIP de alta calidad se utilizan ampliamente en las redes IP. Estos servicios ayudan a los usuarios a trabajar de manera más eficiente y facilitan la comunicación diaria. Sin embargo, las redes IP solo ofrecen el mejor servicio posible, por lo que los problemas de calidad de servicio (QoS), como la pérdida de paquetes, el retraso y la inestabilidad, tienen un impacto significativo en la calidad de VoIP. Estas son pautas para mejorar el servicio definidas en función de aspectos relacionados con la red, como la saturación y la pérdida de paquetes.

Antecedentes

La empresa SEPRIVZAM es una compañía de Seguridad Privada que fue creada en el año 2021, la cual tiene como principal objetivo brindar servicios de seguridad física a urbanizaciones, locales, custodias, o personas que lo requieran. Dicha compañía, actualmente cuenta con un sistema telefónico analógico que permite la comunicación interna entre los empleados, este sistema tiene menor rendimiento, requiere mayor uso de recursos (infraestructura y pago de servicios), y el sistema telefónico tampoco tiene posibilidad de uso poder grabar llamadas y tener un mejor control. Hoy en día, la telefonía analógica se considera obsoleta frente a todos los recursos que ofrece la telefonía IP a bajo costo.

Planteamiento del problema

En el presente, la empresa SEPRIVZAM enfrenta un problema crítico al no poseer un sistema de grabación de llamadas telefónicas para la comunicación entre empleados. La falta de este sistema dificulta el control y seguimiento de las llamadas y puede dar lugar a malentendidos, errores y problemas en la atención al cliente. Además, la falta de registros precisos y completos hace que sea imposible revisar y calificar las llamadas, lo que dificulta la identificación de áreas de oportunidad y la implementación de mejoras en el servicio. En resumen, la falta de un sistema de grabación de llamadas en SEPRIVZAM se está convirtiendo en un grave problema que afecta sus operaciones, calidad de servicio y rentabilidad.

Hoy en día, con los avances tecnológicos y sistemas digitales que se posee, se tiene VoIP, que es un acrónimo de Voz sobre Protocolo de Internet (Voice Over Internet Protocol), el cual por sí mismo significa voz a través de internet, es decir, un sistema VoIP brindaría ventajas y beneficios contra el sistema tradicional, no obstante, esto no resolvería en su totalidad algunos inconvenientes que puede tener este sistema de comunicación. La empresa desea tener un mayor control de llamadas como monitoreando grabaciones, verificación de destinatario. Como resultado, se puede realizar una implementación de un sistema de VoIP

basándose en las políticas de QoS, esto hace referencia a la calidad de servicio (QoS) en las redes de comunicación. Por lo tanto, esto se refiere a la capacidad de la red para proporcionar un nivel consistente de servicio a diferentes tipos de tráfico.

Por este motivo se debe priorizar y asignar recursos en función de las necesidades de la aplicación y del usuario. Esta implementación brinda un excelente servicio y brinda importantes ventajas en el monitoreo de llamadas. Además de asegurar la eficiencia de la calidad a través de políticas de QoS. Debido a esto se debe optimizar el tráfico de la red a través de una gestión adecuada significa reducir la pérdida de paquetes, el retraso y la fluctuación, evitando así la degradación de la calidad. Lo mismo es válido para la evaluación de los parámetros de herramientas que utiliza el protocolo TCP/IP.

Por esta razón, se debe cambiar prioridades y asignar recursos en función de las necesidades de las aplicaciones y los usuarios. Esta implementación brindaría un buen servicio, generando una mayor ventaja al monitoreo de llamadas; además de garantizar una eficiencia de calidad por medio de políticas de QoS. De modo que, optimizando el tráfico de datos en la red a una gestión adecuada, implicaría una reducción en la pérdida de paquetes, latencia y jitter, evitando la degradación de calidad; así mismo, la evaluación de parámetros de herramientas que se emplean en el protocolo TCP/IP.

Adicionalmente, es importante mencionar que se pueden medir los parámetros requeridos para una correcta implementación de políticas QoS, con herramientas de software libre, como lo son: TCPdump, NetworkMiner y Wireshark, para mantener la red en óptimas condiciones y asegurando la calidad.

En definitiva, la implementación de un sistema de VoIP aplicando la política QoS es esencial para resolver el problema de control de llamadas de los empleados que no se obtiene un registro o grabaciones para evitar inconveniente con los clientes de la SEPRIVZAM.

Pregunta Problemática

¿Cómo se puede controlar las llamadas en la empresa SEPRIVZAM?

Objetivo de la propuesta Tecnológica

Objetivo General

Implementar un sistema VoIP basado en QoS aplicando parámetros en seguridad para la empresa SEPRIVZAM CIA.

Objetivos Específicos

- Describir los temas relacionados con los servicios del sistema VoIP, QoS y herramientas enfocadas en el monitoreo del protocolo TCP/IP.
- Identificar la situación actual de la empresa SEPRIVZAM mediante el levantamiento de información pertinente.
- Esquematizar un diseño de un servidor de VoIP con políticas QoS.
- Implementar el servidor VoIP de acuerdo con los requerimientos.
- Evaluar el rendimiento del servidor VoIP con las políticas QoS a través de herramientas de protocolo TCP/IP de acuerdo de las necesidades de la empresa.

Alcance

Se considera que la propuesta de implementación de un sistema VoIP en la empresa SEPRIVZAM es descriptivo y explicativo debido a lo siguiente:

- El alcance del proyecto es descriptivo y explicativo porque se pretende describir cada proceso y aclarar cada fenómeno que se presente y sus respectivas causas, las relaciones entre uno o más factores, etc.
- Mediante el método descriptivo se observa los pasos necesarios para implementar un sistema VoIP, pero para lograr una implementación efectiva se necesita información detallada sobre los objetivos y requisitos específicos del sistema.

- A través del método explicativo se puede observar la funcionalidad de los componentes a desarrollar en la tesis, lo que permite una mejor adaptación del sistema a las necesidades de la empresa. Además, el proceso de implementación puede variar según los requisitos específicos del sistema y la configuración de la red existente.
- Se infiere que, utilizar ambos métodos asegurar una implementación exitosa y adaptada a las necesidades de la empresa.

Justificación

El proyecto se presenta como una solución para el problema de control de llamadas telefónicas en la empresa SEPRIVZAM, basado en los teléfonos tradicionales actuales (analógicos). Este tipo de sistema tiene varias limitaciones, tales como: alto costo, falta de control, baja calidad y falta de flexibilidad en la gestión de la comunicación. Debido a estos problemas, muchas empresas ahora están migrando a la telefonía VoIP.

Razón por la cual, la solución propuesta es implementar un sistema de VoIP fundamentado en QoS, de esta manera se obtienen varias ventajas y beneficios como mejor control, la reducción de costos, escalabilidad, flexibilidad, funciones avanzadas o integraciones con otras aplicaciones.

Desde ese punto de vista, menciona SELLAN (2020) “Al implementar QoS en un IP PBX, se logra una mejor calidad de voz y video, lo que da como resultado un sistema telefónico confiable y económico”. Las características de QoS incluyen clasificación y marcado, para distinguir los tipos de tráfico en función del comportamiento de la red; En función de cada infraestructura, se pueden crear políticas para mejorar el rendimiento de la red (Criollo, 2020). De ahí que, se aplican las políticas basadas en QoS, las cuales garantizan la calidad del servicio VoIP que se evalúa a través de herramientas de software libre que están constantemente monitoreando aspectos como latencia, jitter y pérdida de paquetes.

Para la presente propuesta, se utiliza un servidor con sistema operativo Linux, por lo consiguiente para la instalación del servidor VoIP se utiliza un software

libre que es Issabel en su versión estable. De esta manera, se configuran las líneas correspondientes de la telefonía IP. Adicionalmente, el sistema VoIP ayuda en el manejo de softphones de software libre (o software de teléfonos) los cuales simulan el funcionamiento de un teléfono físico, simbolizando un ahorro considerando el hecho que muchas empresas alquilan o compran teléfonos físicos a un determinado fabricante. En las herramientas de evaluación de calidad de servicio, se usó software libre para evitar gastos excesivos. Entre las opciones seleccionadas se encuentran TCPdump, NetworkMiner y Wireshark, que permiten realizar esta tarea de manera efectiva y sin incurrir en costos elevados. Debido a esto, la implementación de un sistema de VoIP con políticas QoS en una empresa permite solucionar el mayor problema que presenta la empresa SEPRIVZAM, que es el control de llamadas.

CAPÍTULO 1

1. MARCO TEÓRICO

En el presente capítulo se exponen las diferentes definiciones y conceptos de autores, además de tipos y funciones de la telefonía VoIP, entre otros, con la finalidad de que contribuyan a un mejor entendimiento de los términos explicados a lo largo de este trabajo investigativo, dicho proceso se realizó por medio de una recopilación de estudios académicos, seleccionados de los distintos artículos de revistas científicas, sitios web y repositorios universitarios.

1.1 Comunicación

El proceso de comunicación implica la interacción entre dos partes con el objetivo de lograr el entendimiento mutuo. A nivel individual, las personas se comunican para una variedad de propósitos, como tomar decisiones, expresar opiniones, responder preguntas o intercambiar información. En un entorno profesional, la comunicación cobra aún más importancia ya que es necesaria para el buen funcionamiento de una empresa. Sin una comunicación efectiva entre los empleados, una empresa no puede funcionar de manera efectiva.

Según Alemany (2022), la comunicación no se limita a pasar mensajes del remitente al receptor, sino que requiere que el mensaje esté encriptado y que ambas partes entiendan y conozcan el código para una comunicación exitosa. Además, debe haber un medio físico para transmitir el mensaje, y el mensaje debe ser claro y significativo. Comprender estos componentes es fundamental para hacer llegar un mensaje de un punto a otro y para todo el proceso de comunicación.

1.1.1 Comunicación Organizacional

Según Carvalho (2021), la comunicación organizacional se refiere a una serie de métodos y acciones destinados a simplificar y acelerar la transmisión de mensajes entre los miembros de una organización, así como entre la organización y su entorno. También pretende influir en las opiniones, actitudes y comportamientos de los públicos internos y externos de la organización para lograr sus objetivos con mayor eficacia y eficiencia. La comunicación eficaz es esencial para que las organizaciones funcionen correctamente, y puede ayudar a generar confianza, aumentar la productividad y mejorar la moral de los

empleados. Algunos de los métodos utilizados en la comunicación organizativa son las reuniones, los memorandos, los informes, los correos electrónicos, los boletines y las plataformas de redes sociales.

1.2. Telefonía tradicional

La telefonía analógica convencional se basaba en la transmisión de voz a través de dos hilos de cobre, inventado por Alexander Graham Bell en 1876. La tecnología permitía la comunicación punto a punto entre dos dispositivos conectados físicamente, creando una comunicación pregunta-respuesta unidireccional. Para conectar dos o más dispositivos, se requiere una red en estrella, donde todos los dispositivos deben estar conectados físicamente entre sí. De acuerdo con Cano (2007) la telefonía analógica se aplica principalmente en proyectos donde el costo es más importante que la calidad y seguridad de los datos transmitidos, ya que realiza la misma función que un teléfono digital, pero a un bajo costo. Actualmente, la telefonía por Internet o VoIP está reemplazando rápidamente a una tecnología similar, ya que a lo largo de los años ha tenido éxito debido a los menores costos de implementación para las empresas.

1.3. Redes Computacionales

Acorde a Valverde (2017), las redes informáticas son sistemas de comunicación que posibilitan la transmisión de información entre distintos dispositivos conectados mediante un medio de transmisión, como cables o señales inalámbricas. Estas redes tienen múltiples usos, como compartir archivos, imprimir documentos, enviar correos electrónicos y acceder a Internet. Asimismo, las redes informáticas también pueden mejorar la seguridad y la eficiencia de las empresas.

Acorde a Muñoz (2022), los avances tecnológicos han reducido la relevancia de la distancia como barrera para la comunicación. De hecho, las redes informáticas han evolucionado con la gran cantidad de datos disponibles en Internet, lo que permite a las personas comunicarse con otras personas en todo el mundo en muy poco tiempo.

1.4. PBX VoIP

Los términos IP PBX y sistema telefónico VoIP se usan indistintamente para describir un sistema telefónico empresarial que utiliza el Protocolo de Internet (IP) para la transmisión de voz, de ahí el nombre Protocolo de Voz sobre Internet (VoIP). PBX, abreviatura de "Private Branch Exchange", es el componente de conmutación de su sistema telefónico privado.

Según Mohamed (2023), VoIP es la prestación de servicios de telefonía a través de Internet mediante una combinación de tecnologías de comunicación, métodos, protocolos y técnicas de transmisión. En lugar de líneas telefónicas analógicas, la VoIP facilita realizar llamadas de audio a través de redes IP como Internet.

De igual manera, Roy (2021) explica que la tecnología VoIP se encarga de la transferencia de voz en tiempo real mediante la comunicación de datos por Internet. Ésta, consiste en convertir la señal analógica de voz en paquetes digitales, los cuales son enviados desde el origen al destino y viceversa. Para lograr esto, se utiliza un códec para convertir la voz en datos digitales y luego se transmiten a través de Internet. En el extremo receptor, se realiza el proceso inverso, convirtiendo los datos digitales nuevamente en señal analógica y enviándolos al nodo de destino. VoIP es un sistema compuesto por diferentes componentes y es crucial evaluar su confiabilidad y seguridad en aplicaciones críticas.

1.4. 1. Telefonía VoIP

Las líneas telefónicas VoIP permiten la transmisión de audio a través de líneas de datos, y se utiliza el mecanismo de red llamado QoS para proporcionar un servicio telefónico confiable y con buena calidad de sonido. Gracias a las tecnologías basadas en protocolos IP, es posible realizar llamadas en líneas no orientadas a conexión, permitiendo la transferencia bidireccional de voz, video y multimedia simultáneamente.

A su vez, Kozma (2022) expone que, esencialmente, la Voz sobre Protocolo de Internet (VoIP) ayuda a realizar o recibir llamadas telefónicas a través de Internet en lugar de las líneas telefónicas tradicionales. Además, hay tres categorías principales de servicios VoIP: VoIP en la nube, VoIP en las instalaciones y VoIP residencial.

El protocolo VoIP, que permite la transmisión de voz, datos y vídeo por medio de una red convergente de alta velocidad, se aplica para los sistemas de telefonía basados en Internet. Por lo que, cualquier usuario con conexión a la red de datos puede hacer llamadas telefónicas mediante transmisión guiada o inalámbrica empleando este protocolo. De manera que, los usuarios de VoIP pueden llamar a otros que estén conectados a la red, ya sea a través de conexiones Wi-Fi o por cable.

Las conexiones VoIP pueden crear canales de comunicación con líneas telefónicas convencionales, redes celulares GSM, 4G, 4,5G y 5G, y otros sistemas de telefonía IP. Algunos servicios VoIP usan adaptadores que requieren un ordenador y un teléfono VoIP dedicado. El códec se utiliza para codificar señales de voz analógicas, y el audio resultante se encapsula en un paquete IP que se transfiere con la ayuda de una conexión a Internet en lugar de una línea telefónica normal.

Según Blass (2019), El concepto de telefonía IP surge a finales de los 90 cuando VocalTec, pionera en este campo, utilizó esta tecnología para realizar las primeras llamadas entre ordenadores a través de Internet. Con el tiempo, cada vez más empresas comenzaron a implementar proyectos relacionados con la telefonía IP. En el año 2000, esta tecnología ya representaba más del 3% del tráfico de voz. La figura 1 esquematiza el uso que hoy en día se le da a VoIP.

Figura 1. Servicios de telefonía IP.



Fuente: Tomado de Blass (2019).

1.4.2 Característica de VoIP

La central de telefonía IP se caracteriza por la capacidad de transmitir señales de voz con un ancho de banda reducido, lo que permite la transmisión de mensajes con un mínimo consumo de datos. Además, estos paquetes de datos pueden contener varios servicios, lo que reduce los costes económicos.

Según Packer (2018), La accesibilidad de un sistema VoIP es muy importante para los usuarios con discapacidad visual. Un estudio de usabilidad y una encuesta en línea de usuarios de VoIP con discapacidad visual exploraron la importancia de las funciones populares de VoIP y evaluaron la dificultad de usar estas funciones.

Como menciona Sellan (2020), además, los números telefónicos se depositan en la nube del operador de telecomunicaciones, lo que facilita realizar llamadas desde cualquier parte del mundo a través de una línea IP utilizando un teléfono inteligente o softphone, con la capacidad de tener un número telefónico de contacto de las Américas, Europa o cualquier continente.

De acuerdo a Matango (2019) la integración de una red de telefonía IP en la infraestructura de red de datos de una empresa no genera costos adicionales para realizar llamadas, ya que se combinan las redes de voz y datos en una sola red LAN.

1.4.3. Ventajas de VoIP

De acuerdo con Martínez (2018), la tecnología de VoIP ofrece varias ventajas en comparación con la telefonía tradicional. A continuación, se presentan algunas de las ventajas de VoIP:

- Costo: Una de las principales ventajas de VoIP es su bajo costo en comparación con la telefonía tradicional. Las llamadas de larga distancia y las llamadas internacionales son significativamente más baratas con VoIP.
- Flexibilidad: VoIP permite a los usuarios realizar llamadas desde cualquier lugar con una conexión a Internet, lo que significa que no están limitados por la ubicación geográfica.
- Funcionalidades avanzadas: VoIP ofrece una amplia gama de funcionalidades avanzadas, como correo de voz, llamada en espera, transferencia de llamadas y conferencias telefónicas, que no están disponibles en la telefonía tradicional.
- Integración: VoIP se puede integrar fácilmente con otras aplicaciones de comunicación, como correo electrónico y mensajería instantánea, lo que permite una mayor eficiencia y productividad.
- Calidad de voz mejorada: La calidad de voz en las llamadas de VoIP ha mejorado significativamente en los últimos años, lo que significa que las llamadas son más claras y nítidas.
- Escalabilidad: VoIP es altamente escalable y se puede adaptar fácilmente a las necesidades cambiantes de una empresa.

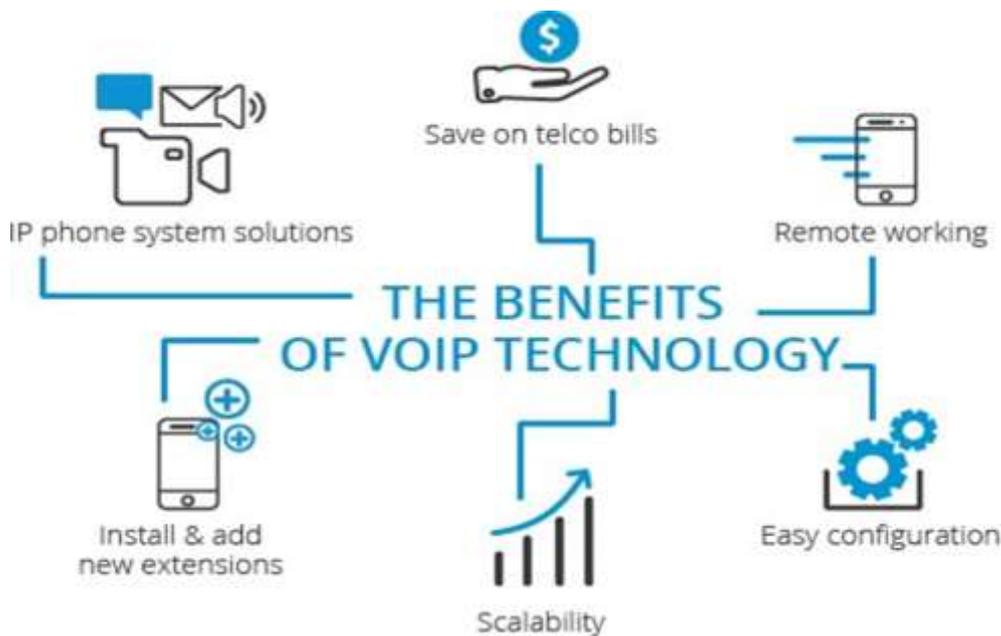
Según Terrenos (2022), La principal ventaja de un teléfono IP radica en su ventaja económica, ya que es significativamente más económico que una línea tradicional, eliminando la necesidad de un teléfono fijo. Además, brinda la posibilidad de realizar llamadas gratuitas o usar datos móviles a cualquier persona con la misma aplicación, eliminando así las barreras geográficas y los costos asociados a las comunicaciones telefónicas con personas lejanas.

Las empresas pueden mejorar el servicio al cliente con aplicaciones que mejoran la productividad y la eficiencia de los agentes. Los clientes también pueden

comunicarse con la empresa a través de varios canales, incluidas las llamadas gratuitas al centro de contacto.

En base a lo anterior, los servicios de VoIP pueden brindar una excelente calidad de llamadas con baja latencia en conexiones de Internet de alta velocidad. La figura 2 ilustra los beneficios discutidos hasta ahora.

Figura 2. Beneficios de la tecnología VoIP.



Fuente: Tomado de 3CX (2021).

1.4.4. Desventaja de VoIP

De acuerdo Kozma (2022), las soluciones de VoIP presentan algunas desventajas que se debe considerar. Una de ellas es la necesidad de contar con una conexión a Internet sólida y confiable, ya que la calidad de las llamadas puede verse afectada en caso contrario. Sin embargo, en situaciones de cortes de energía inesperados, los teléfonos convencionales aún tienen ventaja, ya que las líneas telefónicas suelen seguir funcionando mientras que el servicio de Internet puede no estar disponible.

Aunque la tecnología VoIP es vulnerable a los ataques de red y otros riesgos de seguridad, la mayoría de los proveedores de servicios y sistemas de software confiables cuentan con medidas de seguridad para prevenir dichas

vulnerabilidades. Estos incluyen ataques de denegación de servicio (DOS) o bloqueo de llamadas.

1.5. Issabel

Según la página de Issabel (2019), es una plataforma que simplifica la administración de los canales de comunicación de su negocio, integrando una central telefónica (VoIP) con correo electrónico, CRM, fax, videoconferencia, grabación de llamadas, analíticas y otras funcionalidades.

Issabel es una plataforma de comunicaciones unificadas de código abierto que combina varias funciones en una sola plataforma. Está construida en base a Asterisk de Digium the Asterisk Company, e integra PBX, correo electrónico y tareas de colaboración, así como un servidor de base de datos. El objetivo principal de Issabel es hacer que su plataforma evolucione y se adapte a cualquier necesidad propuesta. Esta plataforma se basa en la filosofía de código abierto, y la comunidad es el elemento principal ya que, sin ellos, Issabel no existiría. Transformándose en uno de los últimos proyectos de comunicaciones unificadas de código abierto, gracias al esfuerzo y contribución de su comunidad.

De acuerdo a Castillo (2020), es un software de código abierto y está licenciado bajo la Licencia Pública General de GNU. En la actualidad, ISSABEL es compatible con dos arquitecturas: Intel x86-compatible (32 bits) e Intel x86-64-compatible (64 bits). ISSABEL se ejecuta en una plataforma Linux con Asterisk, y utiliza otros paquetes que se administran fácilmente a través de una interfaz de usuario web. La distribución de Linux en la que se basa ISSABEL es CentOS, que ofrece compatibilidad binaria con Red Hat Enterprise Linux.

1.5.1. Característica de Issabel

Acorde a Issabel (2019), especifica las características del sistema que son:

- PBX: Integración de PBX para hacer y recibir llamadas, transferir llamadas, conferencias y otras funcionalidades telefónicas.
- Correo electrónico: Integración de correo electrónico para enviar y recibir correos electrónicos desde la plataforma.

- Mensajería instantánea: Integración de mensajería instantánea para la comunicación en tiempo real a través de chat.
- Colaboración: Herramientas de colaboración como calendarios compartidos, tareas y notas.
- Monitor de recursos del sistema: Herramienta para monitorear y analizar el uso de recursos del sistema.
- Administración vía Web: Configuración y administración de la plataforma a través de una interfaz web fácil de usar.
- Configurador de parámetros de red: Configuración de parámetros de red como IP, máscara de subred y puerta de enlace.
- Control de apagado y encendido de central vía web: Posibilidad de controlar el encendido y apagado del sistema desde la interfaz web.
- Soporte para backup y restore a través de web: Herramienta para hacer copias de seguridad y restaurar la plataforma en caso de fallos.
- Soporte para configuración de fechas en el servidor, horas y zonas horarias: Configuración de fechas, horas y zonas horarias en la plataforma para adaptarse a las necesidades de la organización.

1.5.2. Comparación de Elastix con Issabel

La elección entre Elastix e Issabel como plataforma de comunicaciones unificadas depende en gran medida de las necesidades y preferencias individuales de cada usuario. Si se busca una mayor personalización y flexibilidad en opciones y módulos, junto con una interfaz web fácil de administrar, Elastix puede ser la opción ideal. Asimismo, su amplia comunidad de usuarios ofrece soporte y solución de problemas.

Por el contrario, Issabel posee una interfaz de usuario más amigable e intuitiva, una mayor integración con servicios de terceros y herramientas de colaboración, junto con un enfoque en la seguridad y privacidad de los datos. Esto puede ser especialmente atractivo para aquellos que buscan una solución más segura.

En última instancia, es importante evaluar cuidadosamente las características y funcionalidades de cada plataforma, antes de tomar una decisión, estas se detallan en la tabla 1.

Tabla 1. Comparativo de Servidor VoIP

Característica	Elastix	Issabel
Licencia	GPL	GPL
Basado en	Asterisk	Asterisk
Interfaz de usuario	Interfaz web personalizable	Interfaz de usuario más intuitiva
Personalización	Mayor flexibilidad en personalización	Menor flexibilidad en personalización
Integración	Menor integración con herramientas de colaboración	Mayor integración con servicios de terceros y herramientas de colaboración
Administración	Interfaz web fácil de usar	Interfaz web fácil de usar
Soporte y comunidad	Comunidad activa y amplia base de usuarios	Comunidad activa y amplia base de usuarios
Seguridad y privacidad	Enfoque en seguridad y privacidad de los datos	Enfoque en seguridad y privacidad de los datos
Funcionalidades	Básicas y avanzadas de comunicaciones unificadas	Básicas y avanzadas de comunicaciones unificadas

Fuente: Elaboración propia (2023).

1.6. Calidad de servicio (QoS)

Es un término utilizado para describir la capacidad de una red para brindar una experiencia de usuario satisfactoria en términos de rendimiento y confiabilidad. Básicamente, QoS se refiere a una serie de tecnologías que ayudan a administrar el tráfico de datos para minimizar la pérdida de paquetes, la latencia y la inestabilidad. Estos problemas pueden ocurrir en cualquier red, pero son especialmente graves en las redes que están congestionadas o tienen una gran demanda.

QoS es un método proactivo que se utiliza para garantizar que los usuarios tengan acceso a los recursos de la red cuando lo necesiten. Esto se hace estableciendo prioridades para tipos específicos de datos en la red.

Acorde con Roy (2021) declara que, debido a la participación de diferentes tipos de aplicaciones de red en el sistema VoIP, la calidad del servicio es una gran demanda. Los paquetes de voz deben llegar desde el origen hasta el destino junto con la calidad de la transmisión. La pérdida de paquetes, el jitter, la latencia y el retraso son los principales problemas que permanecen en la red VoIP. La comunicación en tiempo real, como VoIP, requiere un bajo nivel de latencia en la red con el fin de realizar un alto nivel de calidad de voz y video.

De acuerdo a ManageEngine (2022), al administrar los recursos de la red de esta manera, QoS puede mejorar en gran medida el rendimiento de la red y brindar una experiencia de usuario más satisfactoria. Del mismo modo, QoS puede ayudar a garantizar que los servicios críticos, como los sistemas de control de procesos industriales o los sistemas de monitoreo de seguridad, tengan el ancho de banda y la capacidad de red necesarios para funcionar correctamente con frecuencia.

De acuerdo con esto, Kumar (2021) menciona que, se ha trabajado en el desarrollo de protocolos de enrutamiento y técnicas de QoS que abordan aspectos relacionados con paquetes y estándares de comunicación inalámbrica. También se han evaluado parámetros que afectan la calidad de audio o video en la comunicación de voz sobre IP en redes de malla inalámbricas, como la pérdida

de paquetes, el jitter y el retardo. Por ende, se han propuesto modelos para analizar la pérdida de paquetes, uno de los parámetros de QoS, y se ha realizado un análisis del jitter y la pérdida de paquetes en el tráfico de VoIP.

1.6.1. Función de QoS

Acorde con TechTarget (2021), las herramientas de calidad de servicio se encargan de la tarea de dar prioridad a los paquetes de datos para maximizar el uso del ancho de banda disponible en una red limitada. Esto significa que la red tiene una capacidad específica para transportar información en un intervalo de tiempo determinado. Por lo tanto, las herramientas de QoS gestionan la priorización de los paquetes de manera que el ancho de banda se utilice de forma óptima para brindar el mejor servicio de Internet posible dentro de ese intervalo de tiempo establecido.

Las herramientas de QoS se encargan de priorizar estos paquetes para aprovechar de manera efectiva el ancho de banda limitado en la red. Dado que la red solo puede transportar una cantidad limitada de información en un tiempo determinado. En resumen, QoS es esencial para optimizar el rendimiento de la red al distribuir el ancho de banda de manera equitativa y eficiente.

1.6.2. Beneficios de QoS

La calidad de servicio (QoS) brinda distintos beneficios significativos para las organizaciones, siendo el principal de ellos la garantía de disponibilidad de la red y de las aplicaciones que se ejecutan en ella. Asimismo, QoS permite una transferencia de datos eficiente y segura a través de la red, lo que significa que las organizaciones pueden utilizar su ancho de banda actual de manera más eficiente, sin tener que actualizar la infraestructura de red para expandir su capacidad.

Entre los beneficios específicos de QoS, se encuentran:

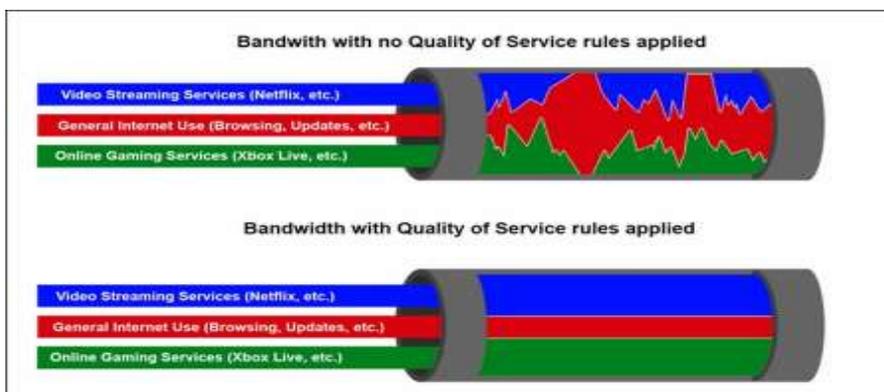
- Proporcionar recursos necesarios para las aplicaciones críticas.
- Permitir una mejor gestión del tráfico por parte de los administradores de red.

- Reducción de costos al no tener que invertir en nueva infraestructura de red.
- Mejora en la experiencia del usuario.

Según Strzeciwiłk (2021), los estándares de QoS exigidos en las redes basadas en IP utilizadas para la transmisión de voz (VoIP) son altamente exigentes debido a que cualquier degradación en la calidad de una llamada es percibida de inmediato por el usuario final. Esta cuestión es de gran importancia, puesto que, señala el creciente aumento en la proporción de aplicaciones multimedia, transmisión de voz y servicios sensibles en las redes IP, lo que implica una mayor demanda de servicios garantizados. El objetivo principal de una sesión de voz en redes basadas en IP radica en cumplir con las recomendaciones de calidad de servicio y, al mismo tiempo, lograr el mayor valor posible del MOS (Mean Opinion Score), incluso en situaciones de congestión en la red.

Dicho esto, para lograr una QoS adecuada, las empresas pueden emplear diversas técnicas y herramientas, como la configuración del tráfico y el uso de buffers de fluctuación. De ahí que, para muchas organizaciones, QoS se convierte en parte integral de sus acuerdos de nivel de servicio (SLA) con sus proveedores de servicios de red, lo que les garantiza un nivel de rendimiento determinado para la red, como se muestra en la figura 3.

Figura 3. *Aplicando reglas con QoS*



Fuente: Tomado de Rudich (2023).

1.6.3. Implementación de QoS

La implementación de herramientas y estrategias de QoS requiere que las organizaciones sigan un proceso de varios pasos. En primer lugar, es importante tener una planificación adecuada. Esto incluye comprender las necesidades de servicio y los requisitos de cada departamento, elegir el modelo correcto y obtener la aceptación de las partes interesadas.

A continuación, la organización debe diseñar una implementación de QoS. Esto incluye el reconocimiento de todos los cambios importantes de software y hardware y la aplicación de modelos QoS seleccionados a las especificaciones de arquitectura de red. Las políticas y configuraciones de

QoS deben probarse en un entorno de prueba seguro y controlado para que los errores puedan corregirse antes de la implementación.

Después de la prueba, la política de QoS debe implementarse paso a paso y de forma iterativa. Las organizaciones pueden optar por implementar políticas por segmento de red o por características de QoS individuales, según lo que logre cada política.

Finalmente, es importante monitorear y analizar el rendimiento de la red para ajustar las políticas de QoS y mejorar el rendimiento de la red de acuerdo con los datos obtenidos.

También Strzeciwillk (2021) explica que, la determinación de los parámetros y prioridades de QoS adecuados para el tráfico de voz no es una cuestión directa y depende en gran medida del diseño y las necesidades comerciales de la organización. Sin embargo, existen algunas reglas generales que indican buenas prácticas para establecer los parámetros de QoS para el tráfico de voz:

- Evitar asignar clases de servicio de prioridad IP con un valor igual a 6 o 7, ya que estos valores están reservados para el Control de Internetwork y el Control de red.
- Los paquetes de voz RTP deben ser marcados con el valor de clase DSCP 5: EF.

- El tráfico de datos debe tener una prioridad más baja en comparación con el tráfico de voz.

1.6.4. Técnicas de QoS

Según Refaet (2020) la técnica de Colas Justas con Asignación Ponderada (WFQ) logra la calidad de servicio asignando de manera equitativa un ancho de banda dedicado a diferentes tipos de tráfico, con el objetivo de controlar el retardo, el jitter y la pérdida de datos. La idea principal de las Colas Justas es asignar un buffer dedicado para cada flujo actual y después el enrutador administra estas colas utilizando un sistema round-robin, WFQ asigna un peso a cada cola o flujo, lo cual determina el porcentaje de ancho de banda del enlace que utilizará cada uno.

Simultáneamente, Refaet (2020) manifiesta que, los principios de encolado del plan de prioridad (PQ) se cimienta en la prioridad asignada a los paquetes (IPP o DSCP), donde se transmite primero el paquete de mayor prioridad desde la interfaz de salida, seguido de los paquetes de datos de baja prioridad. PQ usa diferentes colas asignadas al puerto de salida de la red, cada una con un nivel de prioridad específico. Posteriormente, cuando los paquetes llegan a la cola de alta prioridad, PQ interrumpe cualquier otra actividad en curso para enviar esos paquetes. Al transmitir un paquete, se escanean las colas de alta prioridad (buffers) de ese puerto en busca de nuevos paquetes. Las colas de mayor prioridad se escanean primero, seguidas de la cola de prioridad media y así sucesivamente.

1.6.5. Herramientas para evaluar QoS

Existen herramientas de QoS que pueden llevar a cabo una o varias de estas funciones, y muchas de ellas se encargan de administrarlas automáticamente, permitiendo a los administradores la opción de modificar las políticas y la configuración según sus necesidades. Hay varias herramientas populares de monitoreo de QoS, tales como:

- TCPdump

- NetworkMiner
- Wireshark

Se detalla una comparación de las herramientas mencionada entre sus características principales y funciones.

1.6.6. TCPdump

Es una herramienta de línea de comandos muy poderosa que permite el seguimiento de las redes. La cual, es manejada en la industria para la captura y análisis de paquetes de protocolo TCP/IP. Utilizar TCPdump puede ser muy beneficioso para solucionar problemas de red. Es posible guardar los paquetes capturados en un archivo y analizarlos en su posterioridad. Se recomienda ejecutar TCPdump periódicamente para monitorizar su red (Khurana, 2022).

1.6.7. NetworkMiner

La presente herramienta de análisis de redes forenses se encuentra disponible para Windows (también se puede emular en GNU/Linux con Wine). Su propósito es recolectar información detallada sobre los hosts de la red como evidencia forense, en lugar de simplemente recopilar información sobre el tráfico de la red. Acorde Córtez (2018) puede funcionar como un sniffer pasivo o una herramienta de captura de paquetes para detectar detalles específicos del host, como el sistema operativo, el nombre de host, las sesiones, etc., sin generar ningún tráfico adicional en la red.

1.6.8. Whireshark

Este software ha sido líder en el mundo de las redes durante muchos años, evolucionando y mejorando continuamente. Permite el análisis en tiempo real de la red y también importar archivos que contienen paquetes de información para su análisis. Los administradores de sistemas y redes utilizan esta herramienta para detectar dispositivos con problemas que descartan paquetes, problemas de latencia causados por máquinas defectuosas que enrutan el tráfico de red a cualquier parte del mundo, así como para detectar intentos de exfiltración de datos, malware o ataques cibernéticos contra la organización. Acorde con Altube

(2023) este analizador de redes es una herramienta poderosa que requiere un sólido conocimiento de los conceptos de redes. Las empresas modernas deben comprender los protocolos HTTP y sus servicios, la pila de TCP/IP, analizar y comprender los encabezados de los paquetes, que a veces contienen metadatos complejos, así como el enrutamiento, el reenvío de puertos y DHCP.

1.6.9. Comparativas de herramientas de para medir los parámetros de QoS

TCPdump, NetworkMiner y Wireshark son herramientas de análisis de red que permiten a los usuarios capturar y analizar el tráfico de red. Basado a las características y funcionalidad con una comparación de estas tres herramientas como se observa en la tabla 2:

Tabla 2. Comparativas de herramientas de para medir los parámetros de QoS

Característica	Funcionalidad	Tipo	Interfaz	Sistema empleado
TCPdump	Captura y visualización de paquetes en una interfaz de red	Línea de comandos	Ninguno	Unix-based systems: Linux, macOS
NetworkMiner	Extracción de archivos y metadatos del tráfico de red	Basado en GUI	Fácil de usar	Windows, Linux
Wireshark	Análisis y solución de problemas de red, filtrado de paquetes, decodificación	Basado en GUI	Avanzado	Windows, macOS, Linux

	de protocolos, análisis de paquetes			
--	-------------------------------------------	--	--	--

Fuente: Elaboración propia.

La tabla 2 resume las principales características de TCPdump, NetworkMiner y Wireshark. TCPdump es una herramienta de línea de comandos que se utiliza para la captura, filtrado, decodificación, análisis y personalización de paquetes. NetworkMiner es una herramienta basada en GUI que está diseñada para la captura de paquetes, extracción de archivos y metadatos, y análisis. Wireshark es una herramienta basada en GUI que está diseñada para la captura avanzada de paquetes, filtrado, decodificación, análisis, soporte de protocolos y extensibilidad de plugin.

1.7. Softphones

De acuerdo con Cabrera (2022) declara que un softphone es un software que permite hacer llamadas como si fuera un teléfono convencional, pero con la ventaja de poder instalarlo en diversos dispositivos como PC, laptops, tablets o smartphones. Esto significa que puedes hacer llamadas a otros dispositivos que tengan un softphone instalado o a un teléfono fijo, por ejemplo, desde una Tablet a una laptop, desde un smartphone a una PC o desde tu PC a la oficina. El softphone expande tus opciones de comunicación en cualquier lugar en el que te encuentres. El softphone se basa en el protocolo de voz sobre IP, también conocido como telefonía IP. En términos generales, el softphone convierte tu dispositivo en un teléfono multimedia que puede manejar voz, datos e imagen.

1.7.1 Funcionamiento de Softphone VoIP

Los sistemas de telefonía IP utilizan los mismos protocolos y rutas que el correo electrónico para enviar los datos de voz a través de Internet. Para ello, los datos se fragmentan en segmentos y se codifican en binario con el uso de un hardware denominado códec. Para explicarlo de una manera más fácil de entender, se puede decir que lo que permite a un softphone conectarse con teléfonos fijos es que, aunque se trate de una aplicación web, puede asociarse a un número de

teléfono real, incluso con su código de área local. Según Citelia (2022) cambiar de un sistema telefónico tradicional a uno basado en softphone es muy sencillo, especialmente con una solución en la nube. No se necesita hardware adicional para adaptarse al sistema, ya que las centralitas iCloud funcionan a través del navegador web, de una aplicación de escritorio o móvil que puede descargarse.

El funcionamiento de un softphone se puede describir de manera muy simple:

- Primero, se deben configurar los datos de la línea virtual o extensión proporcionados por el operador VoIP en el softphone.
- Una vez que se ha realizado esta configuración, el softphone se conecta mediante Internet para tomar la línea telefónica.
- En el momento en que se establece la conexión, se obtiene la línea y se pueden hacer y recibir llamadas con el softphone.
- Si alguien llama al número virtual fijo, la llamada se recibirá en el softphone y si se llama a alguien desde el softphone, la persona que recibe la llamada verá un número virtual fijo.

1.7.2. Ventajas de utilizar un softphone VoIP

Las ventajas principales de utilizar un softphone en lugar de un teléfono IP se centran en el ahorro y la movilidad. En cuanto al ahorro, el uso de softphones gratuitos disponibles para smartphones u ordenadores permite evitar el gasto inicial de adquirir un teléfono IP o un adaptador IP, y también puede resultar en un ahorro mensual al elegir las tarifas de telefonía VoIP, que generalmente son más económicas. Menciona Citelia (2022) en cuanto a la movilidad, el uso de un softphone en un dispositivo móvil permite llevar la extensión de la oficina a cualquier lugar sin limitaciones, y si se está fuera de la oficina, basta con instalar un softphone en el smartphone para poder responder a las llamadas a la extensión fija, lo que significa que las llamadas cuestan lo mismo independientemente de la ubicación del usuario.

1.7.3. X-lite

Uno de los softphones más conocidos, el X-lite, funciona en base al protocolo SIP (Matango, 2019). Esta práctica aplicación permite llamar desde el PC entre todos los usuarios a nivel global, también facilita realizar videollamadas por medio de una webcam, enviar MSM, elementos multimedia, música, videos e incluye una agenda personal para anotar todos los datos de los contactos.

1.7.4. 3CX

Este softphone se fundó en 2005, cuando VoIP aún era una tecnología emergente, convirtiéndose en un líder mundial en comunicaciones comerciales, buscando aprovechar las tecnologías estándar abiertas y PSTN Web, evolucionó de un teléfono de sistema a una plataforma de comunicación completa, brindando a los usuarios un fácil, solución flexible y económica para realizar llamadas, chat en vivo o conferencias de audio/video, disponible para iOS y Android, garantiza una mayor productividad, una mejor experiencia del cliente y reducciones significativas en los costos operativos y de administración (3CX, 2023).

1.7.5. Zoiper

Es un programa que funciona en múltiples sistemas operativos, como Windows, Linux, MAC, iPod Touch, iPad, iPhone, tabletas y Android, y está diseñado para trabajar con sistemas de comunicación IP basados en el protocolo SIP. Es desarrollado por la compañía Zoiper y cuenta con una versión gratuita, así como versiones comerciales que ofrecen soporte del software y características adicionales (IP, 2023).

1.7.6. Linphone

Linphone es un softphone que proporciona gestión de llamadas, videoconferencias, mensajería instantánea, uso compartido de archivos, presencia, encriptación y compatibilidad con SIP.

En otro estudio menciona Ortega (2018) evaluó la calidad de voz y QoS en llamadas reales usando diferentes códecs VoIP y descubrió que el códec iLBC-13.33 tenía los mejores resultados para el caso de estudio. Además de que un estudio realizado por Kapinda (2018), el protocolo de transporte seguro en tiempo real (SRTP) se clasifica según el rendimiento de VoIP. El estudio concluyó que agregar protección SRTP al tráfico de VoIP sobre RTP tuvo un efecto insignificante en la calidad de la voz y que el rendimiento de VoIP con SRTP fue aproximadamente un 2 % mejor que usar RTP solo. En general, Linphone es un softphone versátil que se puede utilizar en varios sistemas de VoIP y ofrece una serie de funciones de comunicación y seguridad.

1.7.7. Comparación de Softphone IP

Basado en las características y funcionalidades de los siguientes softphones X-Lite, 3CX, Zoiper y Linphone pueden utilizarse para comunicaciones de voz sobre IP (VoIP), como se observa en la tabla 3:

Tabla 3. Comparación de Softphone IP

Herramienta	Tipo	Interfaz	Funciones
X-Lite	Softphone	Basado en GUI	Gestión de llamadas, grabación de llamadas, videoconferencia, mensajería instantánea, uso compartido de archivos, presencia
3CX	PBX	Basado en GUI	Gestión de llamadas, grabación de llamadas, videoconferencia, mensajería instantánea, uso compartido de archivos, presencia, conferencia web, integración CRM
Zoiper	Softphone	Basado en GUI	Gestión de llamadas, grabación de llamadas, videoconferencia, mensajería instantánea, uso compartido de archivos, presencia, soporte de fax
Linphone	Softphone	Basado en GUI	Gestión de llamadas, videoconferencia, mensajería instantánea, uso compartido de archivos, presencia, cifrado, compatibilidad SIP

Fuente: Elaboración propia.

CAPÍTULO 2

2. METODOLOGÍA DEL PROCESO DE DESARROLLO DE LA PROPUESTA TECNOLÓGICA

En el presente capítulo se procede a describir los métodos con los cuales se desarrolla el presente proyecto. Los métodos a seguir para cumplir con el objetivo de este trabajo de Implementación de un sistema de telefonía VoIP con políticas de QoS para mejorar la comunicación empresarial en SEPRIVZAM CIA, son los siguientes.

2.1. Enfoque de la Investigación

Según a Solís (2020), resulta que método de investigación se refiere a la naturaleza de la investigación y se clasifica en cuantitativa, cualitativa o mixta. Este enfoque cubre todas las etapas del proceso de investigación, desde la definición del tema y el planteamiento del problema, hasta la formulación de perspectivas teóricas, la selección de estrategias metodológicas y la recopilación, el análisis y la resolución de problemas.

Acorde a la revista científica mundo de investigación y conocimiento (2020), existen tres enfoques diferentes para llevar a cabo la investigación descriptiva basado en:

- El método de observación es el más efectivo en este tipo de investigación, y se emplean tanto la observación cuantitativa como la observación cualitativa.
- La observación cuantitativa se enfoca en recopilar datos objetivos que se centran en números y valores. Los resultados de la observación cuantitativa se obtienen mediante métodos de análisis estadísticos y numéricos, como la edad, la forma, el peso, el volumen, la escala, entre otros.
- La observación cualitativa se limita a medir las características de los elementos investigados. El investigador observa a los encuestados desde cierta distancia. Dado que se encuentran en un entorno cómodo, las características observadas son naturales y genuinas.

2.1.1. Investigación Cualitativa

La investigación cualitativa según Rodríguez (2020), se basa en recopilar datos que no son fácilmente cuantificables, por lo que tiende a abordar aspectos descriptivos o valorativos de su análisis.

2.1.2. Investigación Cuantitativa

Para Rodríguez (2020), la investigación cuantitativa se centra en el análisis de un fenómeno específico y se lleva a cabo en un contexto en el que los elementos son completamente medibles. El enfoque cualitativo de la investigación permite realizar un análisis sistemático de información de naturaleza más subjetiva.

Para comprender adecuadamente el enfoque cualitativo o cuantitativo, es importante considerar los siguientes aspectos clave:

- El tipo de realidad que se estudia.
- Los objetivos de la investigación.
- La lógica del proceso de investigación.
- El tipo de datos que se analizan.

Estos factores ayudan a determinar la metodología de investigación adecuada y brindan una base sólida para el diseño y desarrollo de la investigación sobre los enfoques metodológicos y el manejo de los datos recopilados.

En resumen, este proyecto consiste en una investigación cualitativa en la que se aplican herramientas para recolectar información y luego analizarla de acuerdo a la situación actual de la empresa. Asimismo, se utiliza un método cuantitativo para analizar los resultados obtenidos a partir de los datos, generar pronósticos y promedios que contribuyan al buen desarrollo del proyecto.

2.2. Métodos de Investigación

Para Ramos (2021) la utilización de métodos y enfoques de investigación es fundamental e indispensables para la realización de un estudio en cualquier área. Los métodos establecen la orientación a seguir y son flexibles, en cambio, las

técnicas determinan el modo en el cual progresa en ese camino y son menos flexibles.

2.2.1. Investigación Descriptiva

Por otra parte, según Jervis (2018), la investigación de tipo descriptivo se enfoca en identificar y explicar las características esenciales de conjuntos similares de fenómenos. Emplea criterios sistemáticos para determinar la estructura y el comportamiento de los fenómenos bajo estudio, generando información sistemática y comparable con otros recursos.

Desde el punto de vista de Guevara (2020), la meta de la investigación descriptiva es obtener un conocimiento profundo de las situaciones, costumbres y actitudes predominantes a través de una descripción precisa de las actividades, objetos, procesos y personas involucradas.

El método descriptivo lo detalla la revista Liferder (2020), este enfoque se centra en las características fundamentales de un problema y constituye la principal preocupación del investigador. En esta perspectiva, los hechos a describir son seleccionados cuidadosamente según criterios bien definidos con el objetivo de demostrar relaciones de interés.

2.2.2. Investigación Explicativa

El método explicativo lo detalla según la revista Liferder (2020), este enfoque se emplea para explorar las conexiones existentes entre el origen, la causa y el efecto de una situación específica.

El método de investigación explicativo busca ampliar el conocimiento existente sobre algo que es poco conocido o desconocido, según Rus Arias (2020), busca aumentar el nivel de conocimiento disponible sobre algo que es poco conocido o desconocido. Su propósito es centrarse en los detalles para obtener un entendimiento más profundo de un fenómeno en particular. De esta manera, permite adquirir un mayor conocimiento sobre el tema en cuestión.

El primer capítulo aborda una amplia gama de temas relacionados con la tecnología VoIP, desde conceptos básicos hasta información sobre la evolución de las telecomunicaciones y la telefonía tradicional hasta la actualidad. También se analizan aspectos relevantes de las comunicaciones, como las políticas de calidad de servicio (QoS) y las herramientas utilizadas para evaluar su rendimiento. Ambos enfoques son considerados fundamentales para el desarrollo de la empresa SEPRIVZAM S.A., dada su relevancia en la actualidad.

2.3. Variables de Investigación

Según González (2020), se entiende por variables de investigación a las diferentes características o propiedades de objetos o fenómenos que son capaces de cambiar y pueden ser observados, medidos, analizados y controlados durante el desarrollo de una encuesta. Estas variables se pueden ver en la tabla 4.

2.3.1. Variable Independiente

El servicio telefónico sobre protocolo IP (abreviado en inglés como VoIP) es una tecnología que permite realizar llamadas telefónicas utilizando una conexión a Internet en lugar de la infraestructura telefónica tradicional. Este tipo de servicio ofrece muchas ventajas, como la reducción de costos en comparación con las llamadas telefónicas tradicionales, la realización y recepción de llamadas desde dispositivos móviles flexibles, la integración de funciones avanzadas como el desvío de llamadas, el correo de voz y las conferencias en línea.

Además, el servicio de telefonía IP puede proporcionar una mejor calidad de voz y una mayor eficiencia de transmisión de datos porque utiliza tecnología de paquetes para enviar llamadas en lugar de circuitos tradicionales. Esto aprovecha al máximo el ancho de banda disponible y brinda la posibilidad de combinar el teléfono con otros servicios basados en Internet, como la mensajería instantánea y el correo electrónico.

2.3.2. Variable Dependiente

Las políticas de QoS son fundamentales tanto en seguridad como en el control de llamadas en un entorno de comunicaciones. Estas políticas permiten gestionar y priorizar el tráfico de red, asegurando que los recursos se asignen de manera adecuada para garantizar la calidad y confiabilidad de las llamadas.

En cuanto a la seguridad, las políticas de QoS se utilizan para establecer medidas de protección y control en la red. Esto implica la implementación de mecanismos para identificar y mitigar posibles amenazas, como ataques de denegación de servicio (DDoS) o intrusiones maliciosas. Las políticas de QoS también pueden incluir la aplicación de técnicas de encriptación y autenticación para asegurar la confidencialidad e integridad de las comunicaciones.

En el ámbito del control de llamadas, las políticas de QoS permiten gestionar aspectos como la priorización de llamadas, asignación de ancho de banda y control de congestión. Esto se logra estableciendo reglas y prioridades para diferentes tipos de llamadas, como las de emergencia, las críticas para el negocio o las de voz sobre IP (VoIP). Además, se implementan mecanismos para controlar la carga de la red y evitar la saturación, asegurando así una comunicación fluida y de calidad.

Tabla 4. Variables de investigación.

Variable	Definición	Indicador	Medio
Independiente: Servicio de Telefonía VoIP	La telefonía IP es una tecnología que mejora la comunicación integrada entre los empleados y asegura una mayor productividad en la empresa.	Las herramientas de software sólidas y sin licencia ahorran costos y mejoran la eficiencia del proceso.	Entrevista a gerente de la empresa SEPRIVZAM CIA LTDA

Dependiente: Política de QoS para mejorar la comunicación empresarial de SERVIZAM CIA.	Poder controlar de una forma más eficiente las llamadas para mejorar la comunicación en la empresa de la misma manera con parámetros de seguridad QoS.	Diagnóstico del sistema VoIP y los parámetros de QoS en la comunicación.	Encuesta para evaluar los miembros de la empresa con los resultados finales.
--------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------	------------------------------------------------------------------------------

Fuente: Elaboración propia.

2.4. Período y lugar donde se desarrolla la propuesta tecnológica

2.4.1. Periodo

El desarrollo de la propuesta tecnológica tuvo un periodo aproximado de dos meses, desde mayo del 2023 hasta julio del 2023, se tuvo el apoyo y la autorización se puede visualizar en anexo 3 para el desarrollo del proyecto de titulación.

2.4.2. Lugar

- **Nombre:** Compañía de seguridad Zambrano (SEPRIVZAM) CIA. LTDA.
- **Dirección:** Guayaquil, Calle Alejo Lascano 1411 y Los Ríos.
- **Número de colaboradores:** 22
- **Actividad económica:** Brinda servicio de seguridad en diferentes empresas
- **Tipo de empresa:** Pequeña

2.5. Universo y Muestra

2.5.1. Universo

Respecto al universo o la población Moreno (2021), les describe como el conjunto completo de unidades de análisis que conforman un fenómeno de estudio específico. Esta población debe ser cuantificada para un estudio en particular y está compuesta por un conjunto de entidades, denotado como N, que comparten una característica particular. Se denomina población porque representa la totalidad del fenómeno investigado.

El universo del presente proyecto estuvo constituido por 22 personas distribuidas en los siguientes departamentos: gerencia, administración, recursos humanos, financieros, operaciones, marketing, bodega.

2.5.2. Muestra

Acorde a Manterola (2017), una muestra se refiere a un subconjunto o parte de la población que se va a estudiar. La muestra es una parte representativa de la población, y existen procedimientos para obtener la cantidad de los componentes de la muestra, como fórmulas, lógica, y otros

La muestra de estudio para la investigación de esta propuesta tecnológica se basa en la entrevista al gerente de la empresa SEPRIVZAM con el fin de contribuir en la recopilación de información y requisitos para la implementación de la propuesta tecnológica.

En el contexto de esta propuesta tecnológica, la población total estará constituida por todos los empleados de la empresa SEPRIVZAM. En la tabla 5, se presenta información sobre la cantidad de colaboradores y los equipos que utilizan cada uno de ellos:

Tabla 5. Resumen de departamentos, empleados, equipos y teléfonos.

Departamentos	N° de empleados .	N° de PC	N° de teléfonos
Gerencia	1	1	1
Administración.	1	1	1
Recursos Humanos.	2	2	1

Financieros.	2	2	1
Operaciones.	8	4	1
Marketing.	2	2	1
Bodega.	2	1	1
Atención al Cliente.	4	4	4
Subtotal	22	17	11

Fuente: Elaboración propia. Obtenido de: Oficina de recursos humanos de SEPRIVZAM S.A.

De acuerdo con los detalles en la parte superior, se puede identificar esta población de estudio en 22 empleados. Debido al reducido número de empleados, se supone que se puede definir la muestra sin necesidad de aplicar fórmulas estadísticas, la población incluye a 22 personas que tienen acceso a herramientas tecnológicas para realizar su trabajo.

2.6. Métodos e Instrumento de la investigación

Acorde a Godoy (2023), las técnicas y herramientas de investigación son los procedimientos o métodos utilizados para obtener los datos relacionados con el tema de estudio. Estas herramientas son fundamentales para recopilar, organizar, analizar, examinar y presentar la información recabada. Es importante destacar que existen técnicas específicas adecuadas para cada tipo de estudio. Por lo tanto, la elección de la técnica de investigación a utilizar dependerá del problema a resolver y de los objetivos establecidos.

El uso de estas técnicas es imprescindible en cualquier investigación científica, debido a las siguientes razones:

- Permiten obtener los datos necesarios para responder a las preguntas planteadas sobre el tema en estudio.
- La información recopilada a través de estas técnicas permite organizar todas las etapas de la investigación de manera más efectiva.
- Ayudan a controlar el volumen de información obtenida, evitando la saturación de datos innecesarios.
- Contribuyen a verificar la validez de las hipótesis planteadas en la investigación.

Esta propuesta tecnológica se basa en el uso de dos técnicas de investigación para recabar información sobre la opinión de la muestra. Estas técnicas son las entrevistas y las encuestas. Las entrevistas permiten la interacción cara a cara con los participantes, lo que brinda la oportunidad de profundizar en sus respuestas y obtener información. Las encuestas, por otro lado, brindan una forma más estructurada de recopilar datos, lo que le permite llegar a más participantes y obtener una visión más amplia de opiniones e intereses. El uso común de estas dos técnicas de investigación facilita una perspectiva completa y rica en la formulación de la propuesta anterior.

2.6.1. Entrevistas

De acuerdo con Ayala (2021), las entrevistas son una técnica de investigación ampliamente utilizada para conseguir información directa y detallada de los sujetos de estudio. Su objetivo principal es recopilar datos de manera interactiva, lo que permite a los entrevistadores obtener información completa y contextualizada. Durante las entrevistas, se plantean preguntas diseñadas específicamente para explorar los temas de interés y profundizar en las perspectivas, experiencias y opiniones de los participantes.

Según a lo expresado anteriormente, Ayala (2021) explica que, es crucial utilizar las entrevistas como una herramienta esencial para establecer una conversación estructurada con los sujetos de interés, centrándose en los aspectos relevantes para la investigación. Existen diferentes enfoques de entrevistas que se pueden emplear. Las entrevistas rígidas o estructuradas se basan en un conjunto predefinido de preguntas, a menudo presentadas en forma de cuestionarios, que se plantean de manera uniforme a todos los participantes.

En concordancia con lo descrito previamente, Muguirra (2023) opina que, la entrevista es una de las técnicas cualitativas más comunes en la investigación. Por tanto, se exploran las diversas formas de entrevista que se pueden emplear para obtener la información requerida. La entrevista de investigación se presenta como un método valioso para recopilar datos informativos, permitiendo la recolección y análisis de múltiples aspectos, como opiniones, actitudes, sentimientos y representaciones de los participantes entrevistados.

2.6.2. Encuestas

Westreicher (2022) señala que, una encuesta es una herramienta utilizada para recolectar información cualitativa y/o cuantitativa de una población estadística. Para ello, se desarrolla un cuestionario que posteriormente será procesado utilizando métodos estadísticos. En este caso, la encuesta se emplea como instrumento para recopilar información y crear un formulario de preguntas específicas en función del objeto de estudio.

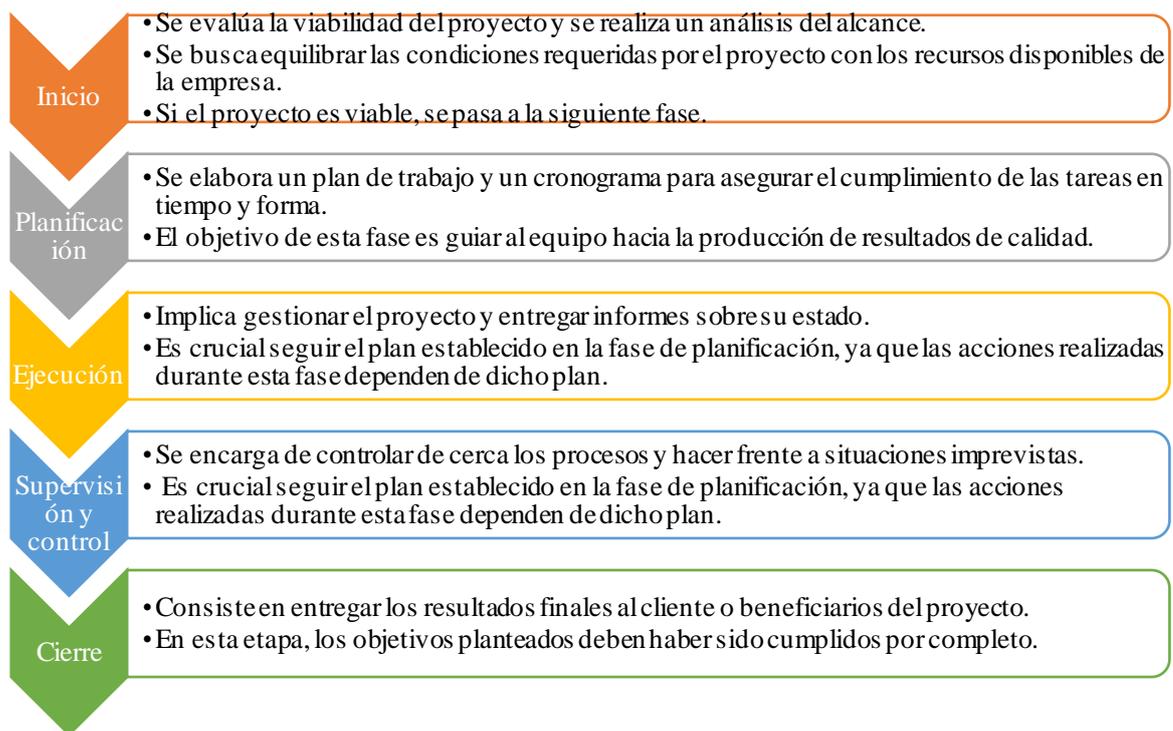
2.7. Metodología de Desarrollo

De acuerdo con el observatorio empresarial para el crecimiento inclusivo (2019) las soluciones tecnológicas con un propósito específico deben ser apropiadas, de fácil acceso, asequibles y adaptadas a la población a la que van dirigidas. Esta tecnología desempeña un papel crucial en cualquier empresa, siempre y cuando la solución tecnológica esté disponible y accesible. En el presente, el acceso a las soluciones tecnológicas ya no está restringido, ya que existen herramientas completamente gratuitas, confiables y fáciles de usar. Dicho esto, la propuesta tecnológica presentada por la empresa SEPRIVZAM se visualiza como una solución ideal para abordar las limitaciones de comunicación de la empresa. El sistema VoIP es completamente accesible y la empresa cuenta con las herramientas necesarias para llevar a cabo este proyecto.

Para el observatorio empresarial para el crecimiento inclusivo (2019) la adopción de tecnología en los proyectos se ve facilitada por la transformación digital de las empresas. Aquellas organizaciones que incluyen la transformación digital como parte de su estrategia empresarial contribuyen a combatir las disparidades tecnológicas. De acuerdo con el autor en el entorno empresarial, la automatización de procesos es fundamental para competir. Las empresas con mayor rentabilidad y éxito en el mercado se encuentran en una especie de "guerra fría", utilizando herramientas tecnológicas para enfrentarse entre sí. Un claro ejemplo de esto es el caso de las plataformas virtuales de los bancos, las cuales se están automatizando cada vez más a medida que pasa el tiempo.

Para el desarrollo del presente proyecto se optó por la metodología PMI, Es un conjunto de lineamientos y procedimientos que guían la dirección y gestión de los proyectos. La metodología de PMI se enfoca en satisfacer las necesidades y expectativas de las partes interesadas del proyecto, mientras se optimiza el uso de los recursos necesarios para ejecutar el proyecto (Vive, 2021). Se observa en la figura 4 las 5 fases básicas de desarrollo de proyectos, que son: inicio, planificación, ejecución, supervisión y control, y cierre.

Figura 4. Fases básicas de desarrollo de proyectos



Fuente: Elaboración propia (2023).

CAPÍTULO 3

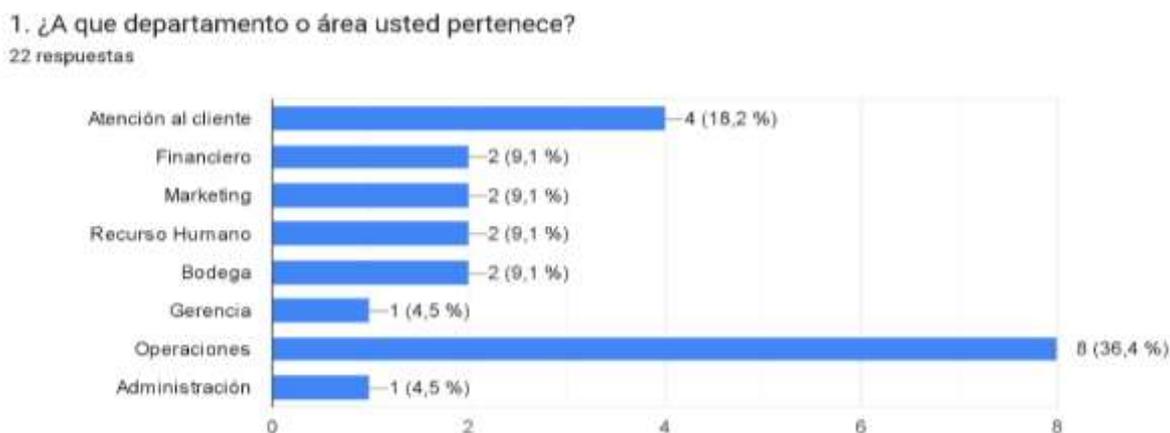
3. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

En este capítulo se analizan y explican los resultados de la entrevista que se detalla en el anexo 2 que se realizó al gerente de SEPRIVZAM para detallar los requerimientos específicos que deseaba en la implementación, acerca del ancho de la red, su topología y el proveedor, además del número de empleados que conforman la empresa, con el fin de obtener una información más precisa y evaluar el rendimiento del servidor. Asimismo, también se procedió a encuestar a una población de 22 trabajadores de la empresa SEPRIVZAM, el 18 de junio del año en curso. Dicha encuesta tiene como objetivo adquirir datos sobre qué es lo más primordial al momento de ejercer el trabajo que ellos requerían y funciones adicionales que le ayuden al día a día, como se detalla en anexo 1 las preguntas realizadas.

3.1. Analizar e interpretar los resultados– Pregunta 1.

En la figura 5 se logra visualizar todas las áreas o departamentos que se benefician con la implementación del sistema VoIP aplicando política QoS en la empresa SEPRIVZAM, totalizando que en operaciones consta de 8 personas con 36.4%, en atención al cliente existe 4 personas que representa el 18.2%, en los departamentos de financiero, marketing, recurso humano y bodega constas de 2 personas por departamentos dando un 9.1%, en administración consta de 1 personas equivalentes 4.5% como también en gerencia que consta de 1 persona que equivale 4.5%. estos son los datos de los empleados.

Figura 5. Departamento o área que pertenece



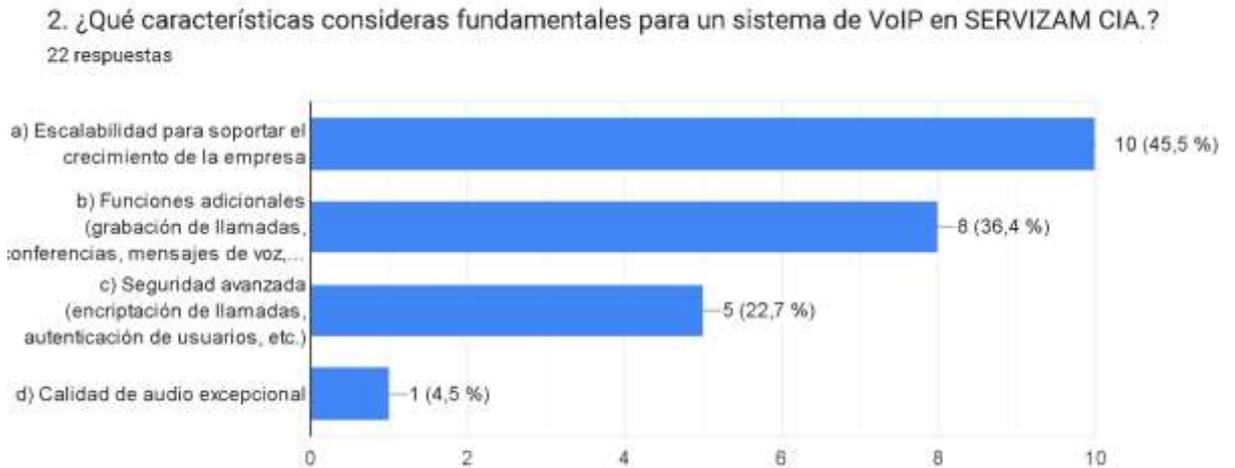
Fuente: Elaboración propia (2023).

3.2. Analizar e interpretar los resultados – Pregunta 2.

En la figura 6 se observa los porcentajes de la segunda pregunta, los requisitos o características principales que desea la empresa con 45.5% se deriva a la escalabilidad, la siguiente son las funciones adicionales que ofrece el servicio VoIP con un 36.4%, en lo que es seguridad avanzada tiene un 22.7% no muy

lejano de las primeras, por último, la calidad de audio que da 4.5% de esta pregunta.

Figura 6. Características fundamentales para un sistema VoIP en SERVIZAM CIA.

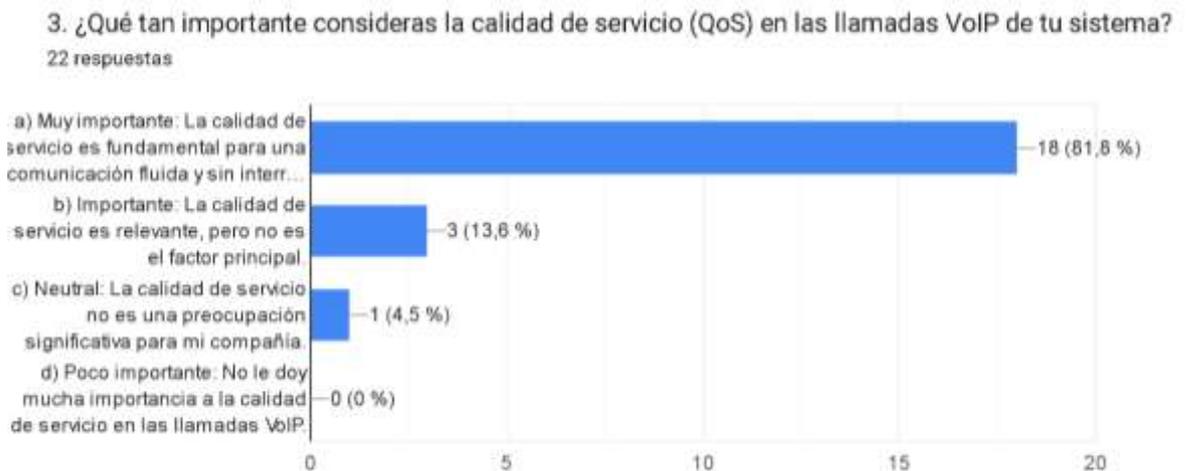


Fuente: Elaboración propia (2023).

3.3. Analizar e interpretar los resultados– Pregunta 3.

En la figura 7 se distinguen las respuestas de la tercera pregunta en donde se evaluó la importancia de la calidad de servicio (QoS) dentro de la empresa donde la mayoría de las personas escogieron la opción muy importante con un 81.8% de los encuestados, con un rango más bajo con un 13.6% es importante, por último, con 4.5% esta neutral ya que poco importante tiene 0%, es decir que para la empresa es muy importante la calidad de servicio.

Figura 7. Importancia de una QoS en las llamadas VoIP

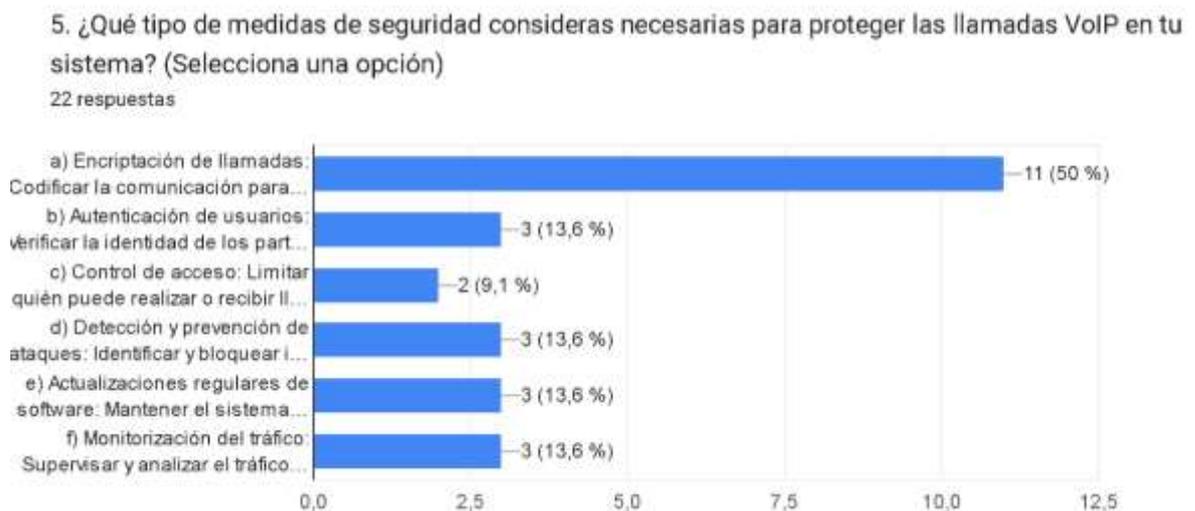


Fuente: Elaboración propia (2023).

3.5. Analizar e interpretar los resultados– Pregunta 5.

En la figura 8 se presenta los resultados de la pregunta cinco donde se observa que el mayor porcentaje lleva encriptación de llamadas con el 50%, en la siguiente se puede observar que se repite en 4 ítems con un 13.6% la autenticación de usuario, detección y prevención de ataque, actualización de software y el monitoreo de tráfico y por último con el 9.1% el control de acceso.

Figura 8. Tipo de medidas necesarias para proteger las llamadas VoIP en el sistema

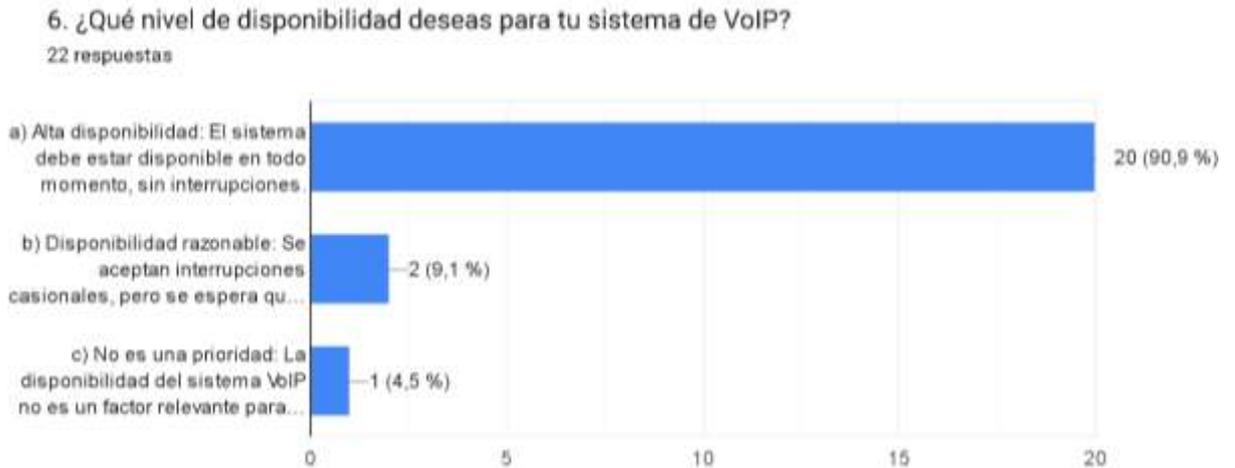


Fuente: Elaboración propia (2023).

3.6. Analizar e interpretar los resultados– Pregunta 6.

Según la figura 9 en la pregunta seis se debe llevar a cabo una alta disponibilidad en el servicio de VoIP con un 90.9% sobre las otras que da un resultado de 9.1% de disponibilidad razonable y 4.5% no es prioridad. En si el servicio debe tener una alta demanda en disponibilidad.

Figura 9. Nivel de disponibilidad en el sistema de VoIP

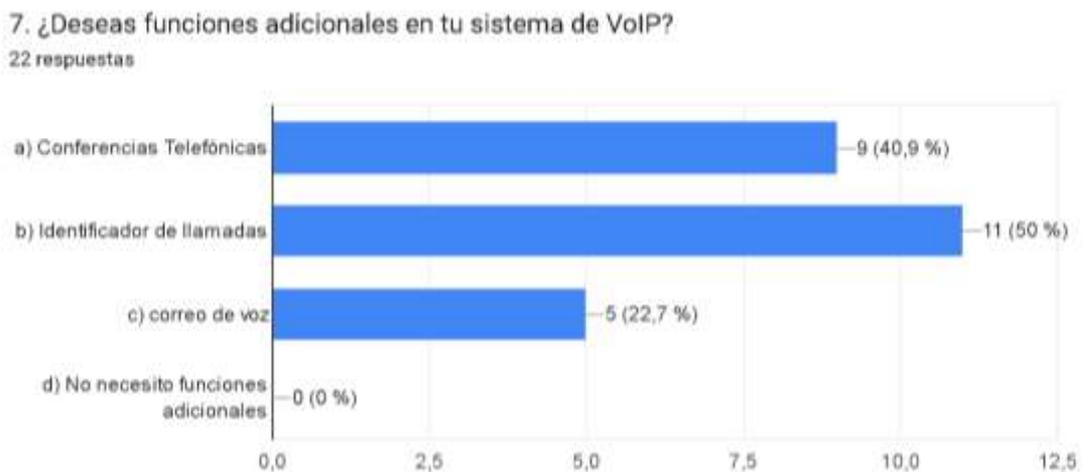


Fuente: Elaboración propia (2023).

3.7. Analizar e interpretar los resultados– Pregunta 7.

En la figura 10 se puede visualizar que en la pregunta siete la identificación de llamada demanda un 50% de los encuestados con un 40.9% a los que desean conferencia telefónica como las funciones adicionales las más demanda y por último con 22.7% el correo de voz.

Figura 10. Funciones adicionales en el sistema de VoIP



Fuente: Elaboración propia (2023).

CAPÍTULO 4

4. IMPLEMENTACIÓN DE LA SOLUCIÓN TECNOLÓGICA

En este capítulo, se detallan las fases realizadas para la implementación del sistema de VoIP, habiéndose seleccionado Issabel PBX. En primera instancia, en la fase 1 inicio, se describen los requisitos, el estado de la red y las características del servidor. Posteriormente, en la fase 2 planificación, se describe el cronograma de actividades de la implementación. Luego en la fase 3 ejecución, se procede con la descarga del instalador, al mismo tiempo la instalación y configuración del sistema. A continuación, en la fase 4 supervisión y control, se realiza la evaluación de la seguridad del servidor utilizando herramientas como Wireshark y Nmap. Con base en los hallazgos, se procede, que consiste en aplicar medidas de QoS basadas en la seguridad para abordar las vulnerabilidades encontradas. Por último, se presenta la fase 5 cierre, donde se muestran los resultados de la implementación de QoS en el servidor VoIP.

4.1 Fase 1: Inicio

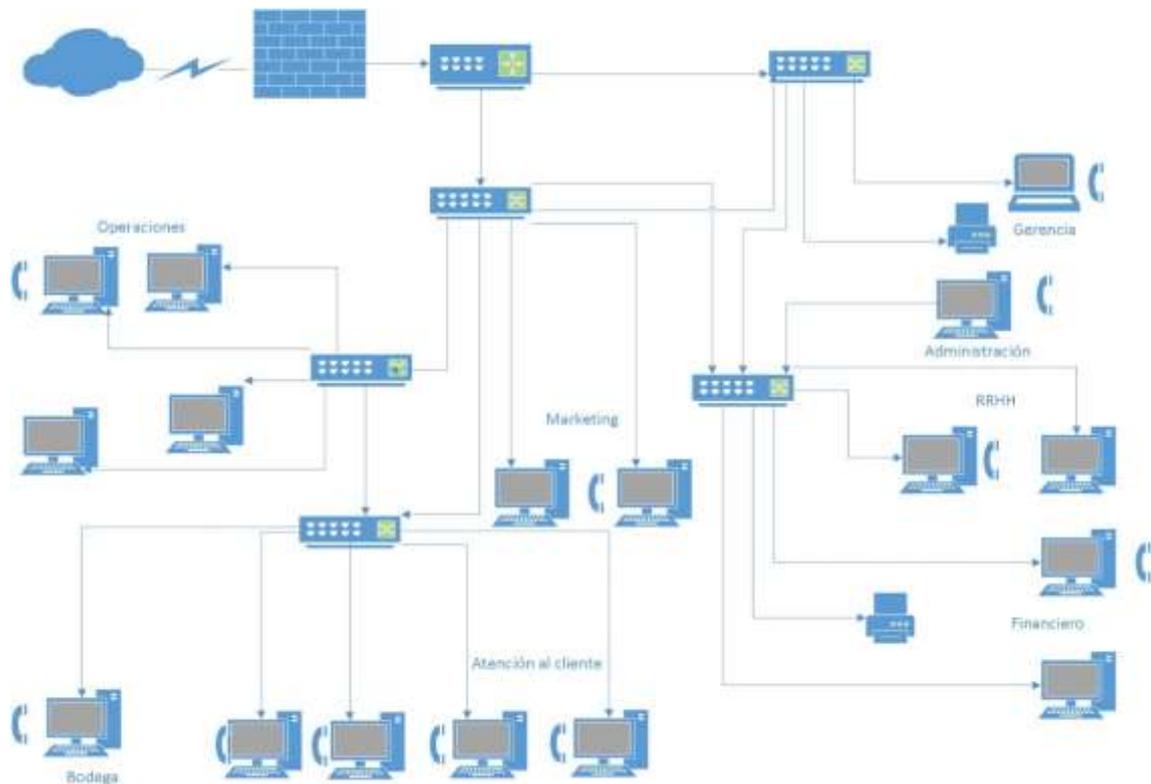
En relación a la etapa 1, se proporciona información detallada sobre el estado de la red en la empresa, así como la tipología del diseño de red utilizado. Además, se describen las características del computador utilizado como servidor de VoIP.

4.1.1. Estado de la Red De Área Local (LAN)

Según los datos proporcionados por los miembros de la empresa, disponen de una red LAN que se presenta en la figura 5.

La red LAN de SEPRIVZAM sigue una topología de árbol, donde las terminales se ramifican para conectar todos los nodos de la red. El diseño de la red es básico y se asemeja al de una red corporativa. El cableado utilizado para conectar los equipos de capa 2 (conmutadores) y capa 4 (enrutadores) es de fibra óptica, lo que garantiza un ancho de banda de 200 Mbps. Además, existe la posibilidad de aumentar esta capacidad según las necesidades de la empresa.

Figura 11. Diagrama de red LAN de la empresa SEPRIVZAM.



Fuente: Elaboración propia (2023).

4.1.2. Servidor

En la actualidad, el acceso a las soluciones tecnológicas ya no está restringido, ya que existen herramientas que son completamente gratuitas, confiables y fáciles de usar. Dicho esto, la propuesta tecnológica presentada por la empresa SEPRIVZAM CIA LTDA se visualiza como una solución ideal para abordar las limitaciones de comunicación de la empresa. El sistema VoIP es completamente accesible y la empresa cuenta con las herramientas necesarias para llevar a cabo este proyecto. Por esta razón, se ha decidido utilizar un ordenador que cumpla la función de un servidor (Figura 12). A continuación, se detallarán las características principales del mismo.

- Marca: Asus
- Modelo: H110M
- Nombre del dispositivo: Issabel. Local
- Procesador: Core i5 6ta Generación
- Memoria RAM: 4 GB

- Sistema Operativo: Linux
- Tipo de sistema: Sistema operativo de 64 bits, procesador basado en x64.

Figura 12. Servidor que será usado para la propuesta tecnológica.



Fuente: Elaboración propia (2023).

4.2. Fase 2: Planificación

En esta fase de planificación se procede a diseñar un cronograma de actividades a través de un diagrama de Gantt se puede visualizar en anexo 4, defendiendo los tiempos que se deben cumplir las actividades planificadas en la fase anterior de inicio en el proyecto.

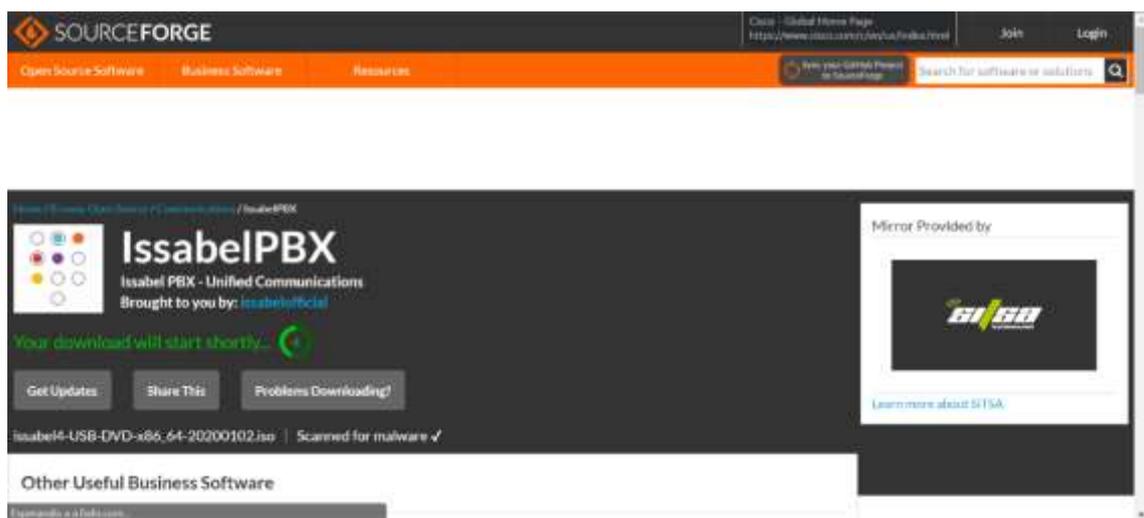
4.3. Fase 3: Ejecución

En la fase 3, a continuación, se detalla la descarga del instalador del servidor. Además, se proporciona información exhaustiva sobre la instalación y configuración, destacando los pasos necesarios para llevar a cabo este proceso. Asimismo, se aborda la creación de las extensiones, junto con las configuraciones correspondientes en los softphones para enlazar dichas extensiones.

4.3.1. Descarga e Instalación De Issabel

Para poder descargar el instalador de Issabel se debe ingresar a la siguiente URL: <https://sourceforge.net/projects/issabelpbx/> Este enlace lleva al repositorio donde se muestra la opción de descarga de la versión issabel4-USB-DVD-x86_64-20200102.iso, que se descarga en formato ISO y espera que se termine el proceso de descarga.

Figura 13. Descarga del archivo de ISO de Issabel.



Fuente: Tomado de Issabel PBX (2023).

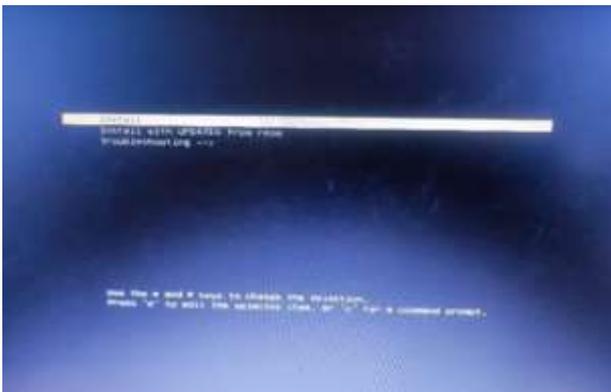
Después de completar la descarga del archivo, se guarda el archivo ISO en un directorio accesible. A continuación, se procede a instalar dicho archivo en una memoria USB para poder utilizarlo en la instalación del sistema operativo en el ordenador.

Posteriormente, se ejecuta el programa Rufus, una herramienta que permite crear una unidad USB de arranque para el archivo ISO de Issabel. Se selecciona la memoria USB deseada y se configura el archivo ISO como booteable. Se etiqueta la unidad USB con el nombre "Issabel 4 x86 x64" y se da inicio al proceso de creación de la unidad de arranque.

Una vez completado este paso, se conecta la memoria USB al ordenador. Al encender la computadora, ésta reconoce la presencia de la memoria USB y comienza el proceso de arranque, permitiendo seleccionar la unidad USB como opción de arranque.

Después de seleccionar la unidad USB, se inicia la instalación del sistema operativo Issabel. Durante este proceso, se muestra en la pantalla el mensaje correspondiente a la figura 14, el cual forma parte de la primera etapa de la instalación.

Figura 14. *Instalación de Issabel en el computador.*



Fuente: Elaboración propia (2023).

Después de ser redirigido a otra pestaña, se muestra una ventana donde se puede visualizar la opción de seleccionar el idioma deseado para la instalación, tal como se muestra en la figura 15.

Figura 15. *Configuración de Idioma de Issabel*

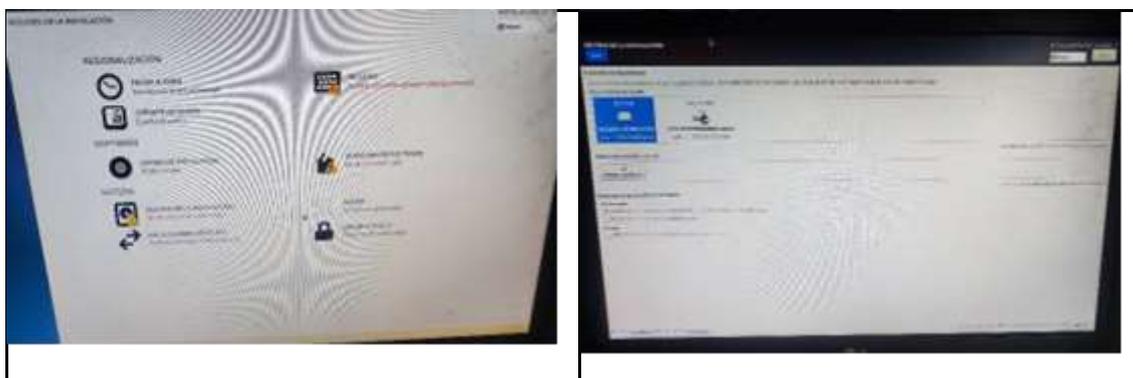


Fuente: Elaboración propia (2023).

A continuación, se presenta una pestaña donde es necesario ajustar algunas configuraciones, como la fecha, la selección del software del teclado y el destino de la instalación. Para la configuración de la fecha, se elige la opción correspondiente al día actual, y para la zona horaria, se selecciona la opción relacionada con la zona horaria ecuatoriana. En el caso de la selección del teclado, se opta por el teclado latinoamericano.

Posteriormente, se procede a elegir la ubicación de la instalación del sistema operativo. En este caso, se selecciona el disco duro SSD como destino, como se puede observar en la figura 16.

Figura 16. Configuración del disco y versión de Issabel.



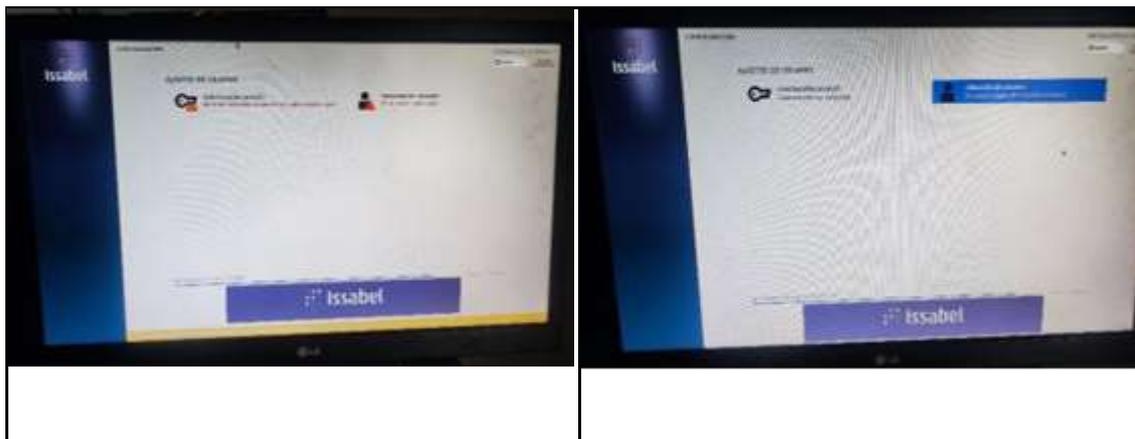
Fuente: Elaboración propia (2023).

Seguidamente, se procede a realizar la configuración de la dirección IP en modo STATIC, en lugar de utilizar el protocolo DHCP, con el fin de evitar posibles inconvenientes causados por variaciones en la asignación de direcciones IP. Esta configuración se realiza para garantizar una conexión estable.

Una vez completada la configuración de la dirección IP, se procede a seleccionar el sistema Issabel 13 para su instalación. Este sistema proporciona acceso a una variedad de servicios y funcionalidades.

Ahora es necesario establecer una contraseña alfanumérica para el superusuario (root) durante el proceso de instalación. Esta contraseña debe incluir letras mayúsculas, minúsculas y caracteres especiales. Se recomienda utilizar una contraseña segura para garantizar la seguridad del sistema y evitar accesos no autorizados, conforme se visualiza en la figura 17.

Figura 17. Configuración de la contraseña de usuario Root.



Fuente: Elaboración propia (2023).

Después de reiniciar el ordenador, se pone en marcha el sistema operativo Issabel. En la siguiente pantalla, se muestra la configuración del usuario "admin" para introducir la contraseña de acceso a la interfaz web.

A continuación, se abre una nueva ventana donde se solicita la contraseña de la base de datos MariaDB del servidor. Una vez ingresada la contraseña, se muestra una ventana donde se debe proporcionar un nombre de usuario o contraseña, conocido como usuario "Root", para acceder a la información del servidor.

Para determinar la dirección IP del servidor, se utiliza el comando "ifconfig", que revela que la dirección IP del servidor es 192.168.1.189. Con esta dirección IP, es posible acceder al servidor desde otros dispositivos en la red.

Luego, se accede a la dirección IP del servidor utilizando el usuario y la contraseña "admin", lo cual muestra una interfaz más gráfica y atractiva para el control del servidor. Esto permite realizar configuraciones esenciales y gestionar el servidor de manera más cómoda.

4.3.2. Creación de extensiones

Para comenzar el proceso de creación de extensiones, se debe dirigir al menú principal del panel de administración y seleccionar la opción "PBX" en la

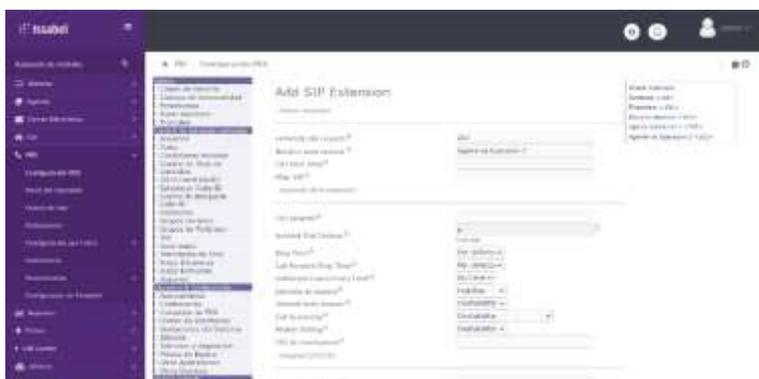
configuración del PBX. A continuación, se despliega un menú y se elige la opción "extensiones".

Al acceder a la sección de extensiones, se muestra un menú con diferentes protocolos para crear la extensión. En este caso, se selecciona el protocolo "generic SIP" y se hace clic en "Agregar" para proceder con la creación.

A continuación, se crea la extensión utilizando un número de 3 dígitos y se asigna un nombre a la extensión. También se establece una contraseña para proteger la extensión. Finalmente, se hace clic en "Crear" para completar el proceso.

Una vez finalizada la creación de la extensión, se recomienda aplicar los cambios correspondientes. Esto permitirá que los ajustes realizados se reflejen en el servidor. Los cambios aplicados pueden ser visualizados en el servidor, mostrando así las extensiones creadas para los diferentes usuarios de los diversos departamentos de la empresa, como se puede observar en la figura 18.

Figura 18. Creación de extensión



Fuente: Elaboración propia (2023).

4.3.4. Grupos de extensiones

En primer lugar, el usuario accede a la página de Issabel, una plataforma de comunicaciones empresariales. En busca de gestionar eficientemente las extensiones de la empresa SEPRIVZAM, procedió a dirigirse al panel de administración. Allí, encuentra una variedad de opciones disponibles para la configuración del sistema.

Con el objetivo de organizar adecuadamente las extensiones, el usuario selecciona la opción específica para crear grupos de extensiones. Dado el considerable número de extensiones presentes en la empresa SEPRIVZAM, se

ha tomado la decisión de crear múltiples grupos, cada uno destinado a los diferentes departamentos de empleados.

Esta elección permite al usuario dividir las extensiones en grupos más pequeños y específicos, facilitando así la gestión y el enrutamiento de las llamadas dentro de la organización. Al crear grupos de extensiones para los departamentos respectivos, se establece una estructura clara que refleje la organización interna de la empresa.

4.3.4. Registros de llamadas

Dentro del panel de administración, se encuentra disponible la opción de acceder a los registros de llamadas, los cuales proporcionan información sobre el flujo de llamadas dentro del conmutador. Para acceder a estos registros, se debe seguir el siguiente proceso:

1. Diríjase al menú principal del panel de administración.
2. En el menú principal, seleccione la opción "Informes".
3. Una vez dentro de la sección de informes, haga clic en "Registros de llamadas".

Al seleccionar esta opción, se abrirá una nueva página o ventana que mostrará los registros de llamadas. Estos registros contienen información detallada sobre las llamadas realizadas, incluyendo la fecha, hora, duración, números de origen y destino, entre otros datos relevantes.

4.4. Fase 4: Supervisión y control

En la fase 4, se llevan a cabo pruebas de llamada en el servidor VoIP con el fin de identificar posibles inconvenientes en los softphones utilizados. Además, se realiza un análisis de las vulnerabilidades presentes en el servidor para garantizar su seguridad. Para realizar estas pruebas, se utiliza una herramienta específica diseñada para identificar posibles casos de ataques. Se emplea una distribución de Linux llamada Kali, que cuenta con una licencia libre. Kali se ejecuta en un entorno virtualizado, lo que facilita la realización de pruebas sin afectar el sistema en producción. Esta distribución ofrece una amplia gama de

herramientas útiles para validar la existencia de puertos lógicos o puntos de entrada que puedan permitir el acceso no autorizado al servidor. Utilizando Kali Linux, es posible llevar a cabo análisis de seguridad, realizar capturas de datos y visualizar las extensiones utilizadas en el servidor. Estas pruebas permiten identificar posibles vulnerabilidades y potenciales puntos débiles en la configuración del servidor, lo que contribuye a fortalecer la seguridad y prevenir posibles ataques.

4.4.1. Pruebas de funcionamiento

Durante la fase de pruebas, se llevó a cabo la validación del correcto funcionamiento del servidor mediante una llamada inicial. En esta primera prueba, no se detectaron novedades ni problemas.

Sin embargo, al realizar varios intentos adicionales utilizando diferentes softphones virtuales y sus respectivas extensiones, surgió un inconveniente relacionado con los códecs utilizados. Es importante destacar que este problema específico se observó en el softphone X-lite, el cual presenta un problema común en su funcionamiento. Afortunadamente, se trata de una dificultad que se puede corregir, aunque no es especialmente complicada de solucionar.

4.4.2. Corrección de Códec de Software

Durante las pruebas realizadas con el softphone X-lite, se identificó un problema relacionado con los códecs utilizados. Durante las llamadas salientes, no se presentó ningún problema, sin embargo, al recibir llamadas, se producía un error evidente que mostraba un estado ocupado, a pesar de que no había ninguna llamada en curso, tal como se muestra en la figura 19.

Para solucionar este inconveniente, se procedió a realizar una configuración específica de los códecs en el softphone X-lite. Para acceder a la configuración de los códecs, se deben seguir los siguientes pasos:

Ir a las opciones avanzadas del softphone X-lite.

Dentro de las opciones avanzadas, se selecciona la opción de códecs.

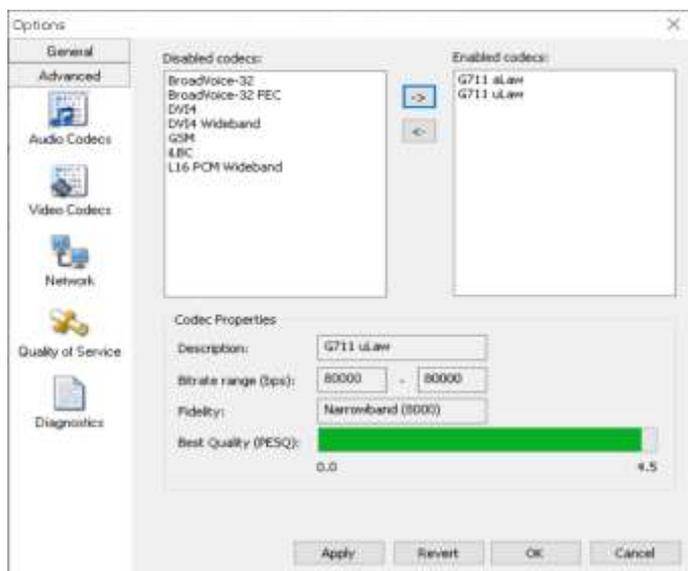
A continuación, se presentan las opciones de códecs disponibles, que incluyen:

- G711aLaw
- G711uLaw

Es necesario seleccionar la opción de códec más adecuada según las necesidades y requerimientos del sistema.

Mediante esta configuración de los códecs en el softphone X-lite, se busca resolver el problema de estar ocupado durante las llamadas entrantes, permitiendo un correcto flujo de las comunicaciones sin inconvenientes.

Figura 19. Configuración de Códec



Fuente: Elaboración propia (2023).

4.4.3. Verificación de Vulnerabilidades en el Servidor

En esta fase, se lleva a cabo la detección de vulnerabilidades presentes en el servidor con el objetivo de garantizar su seguridad. Para lograrlo, se utiliza una herramienta específica diseñada para identificar posibles casos de ataques. En este contexto, se emplea la distribución de Linux llamada Kali, que se ejecuta en un sistema virtualizado con licencia libre.

Dentro de Kali Linux, se encuentran diversas herramientas útiles para validar la existencia de puertos lógicos o puntos de entrada que podrían permitir el acceso no autorizado al servicio o al servidor. Estas herramientas también permiten realizar capturas de datos para visualizar las extensiones y, potencialmente, llevar a cabo ataques.

En este caso, se realizó un pentesting coordinado utilizando el programa VirtualBox. Se instala la distribución de Linux Kali en una máquina virtual para

poder realizar el análisis de seguridad del servidor. El uso de Kali Linux es fundamental para identificar las vulnerabilidades presentes en el servidor y tomar las medidas necesarias para corregirlas y fortalecer la seguridad.

4.4.4. Configuración de herramientas de Vulnerabilidad

En este caso, se realizó un pentesting coordinado utilizando el programa VirtualBox. Se instala la distribución de Linux Kali en una máquina virtual para poder realizar el análisis de seguridad del servidor. El uso de Kali Linux es fundamental para identificar las vulnerabilidades presentes en el servidor y tomar las medidas necesarias para corregirlas y fortalecer la seguridad.

El primer paso en este proceso es seleccionar la herramienta adecuada que ayude a identificar los puertos o posibles puntos de acceso al servidor. Esta herramienta será utilizada para llevar a cabo el escaneo de puertos y evaluar la seguridad del servidor.

Antes de iniciar la fase de pentesting, se procede a instalar la distribución de Linux Kali en VirtualBox. Esta instalación permitirá utilizar las herramientas necesarias para realizar el escaneo de vulnerabilidades en el servidor.

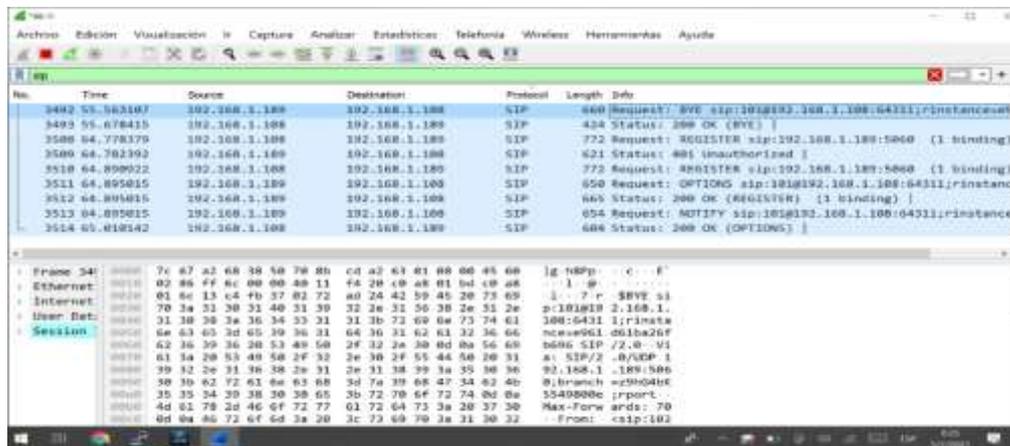
Además, se descarga el programa Wireshark, el cual será utilizado para identificar el protocolo SIP y analizar las comunicaciones de red. Esta herramienta resulta fundamental para realizar un análisis detallado de los paquetes de datos y detectar posibles vulnerabilidades o anomalías en el protocolo SIP.

Una vez que Kali Linux y Wireshark están debidamente instalados, se procede a utilizar Wireshark para capturar y analizar el tráfico de red. Esta captura permitirá identificar y examinar el protocolo SIP en busca de posibles problemas de seguridad o configuraciones erróneas.

La figura 20 muestra la interfaz de Wireshark y proporciona información útil para llevar a cabo el análisis del protocolo SIP.

Al obtener la información mediante el uso de Wireshark, es posible identificar posibles vulnerabilidades presentes en el servidor. Este análisis detallado del tráfico SIP y RTP proporciona una visión más clara de la comunicación y permite identificar cualquier problema de seguridad o debilidad en el sistema.

Figura 21. Rastreo de llamada por el protocolo SIP



Fuente: Elaboración propia (2023).

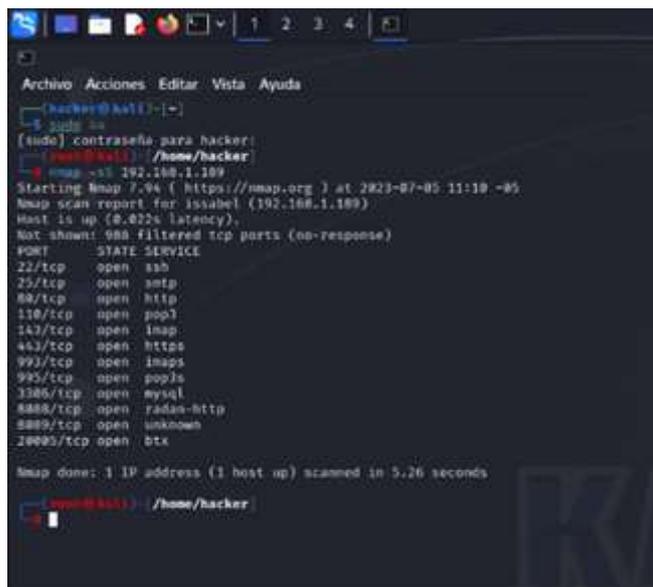
4.4.6. Reconocimiento del servidor

Al utilizar el scanner en el protocolo SIP, se detectan las direcciones IP de los dos dispositivos que participaron en la llamada. A continuación, se llevó a cabo una evaluación utilizando la distribución de Linux Kali y la herramienta Nmap para determinar cuál de las dos IP pertenece al servidor.

Tras el análisis, se identificó que la IP 192.168.1.189 correspondía al servidor. Se procedió entonces a realizar un escaneo de los puertos del PBX utilizando las herramientas disponibles en Kali Linux. Este escaneo permitió identificar las vulnerabilidades presentes en los puertos del PBX, tal como se muestra en la figura 22.

A partir de la información obtenida, se pudo llevar a cabo un ataque de fuerza bruta con el objetivo de falsificar la llamada y obtener acceso al servidor. Este tipo de ataque consiste en probar múltiples combinaciones de contraseñas hasta encontrar la correcta.

Figura 22. Búsqueda de puerto abierto por Nmap



```
hacker@kali:~$ sudo su
[sudo] contraseña para hacker:
hacker@kali: /home/hacker
hacker@kali:~$ nmap -sS 192.168.1.109
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-05 11:10 -05
Nmap scan report for issabel (192.168.1.109)
Host is up (0.022s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql
8888/tcp  open  radas-http
8889/tcp  open  unknown
20005/tcp open  btX

Nmap done: 1 IP address (1 host up) scanned in 5.26 seconds
hacker@kali: /home/hacker
```

Fuente: Elaboración propia (2023).

4.4.7. Aplicación de Política de QoS en Seguridad

En esta fase, el enfoque principal es garantizar que el servidor no presente vulnerabilidades que puedan ser aprovechadas por hackers, evitando así la pérdida de información valiosa. Para lograrlo, se llevan a cabo los siguientes pasos:

- Configuración de políticas QoS: Se establecen políticas de calidad de servicio en el PBX para priorizar y gestionar el tráfico de red relacionado con las comunicaciones de voz. Esto asegura un rendimiento óptimo de las llamadas y evita la degradación de la calidad en situaciones de congestión de red.
- Parámetros de seguridad: Se aplican parámetros de seguridad en el PBX para fortalecer la protección del servidor contra posibles ataques externos. Esto puede incluir configuraciones como el filtrado de paquetes, la limitación de intentos de inicio de sesión fallidos, la detección de intrusiones y otras medidas de seguridad recomendadas.

Al configurar y aplicar estas políticas QoS y parámetros de seguridad en el PBX, se busca garantizar que el servidor esté protegido contra amenazas y ataques cibernéticos, salvaguardando así la información valiosa almacenada en él. Esto

es fundamental para mantener la integridad y confidencialidad de los datos, evitando pérdidas y asegurando el funcionamiento seguro y eficiente del sistema.

4.4.8. Configuración de Firewall

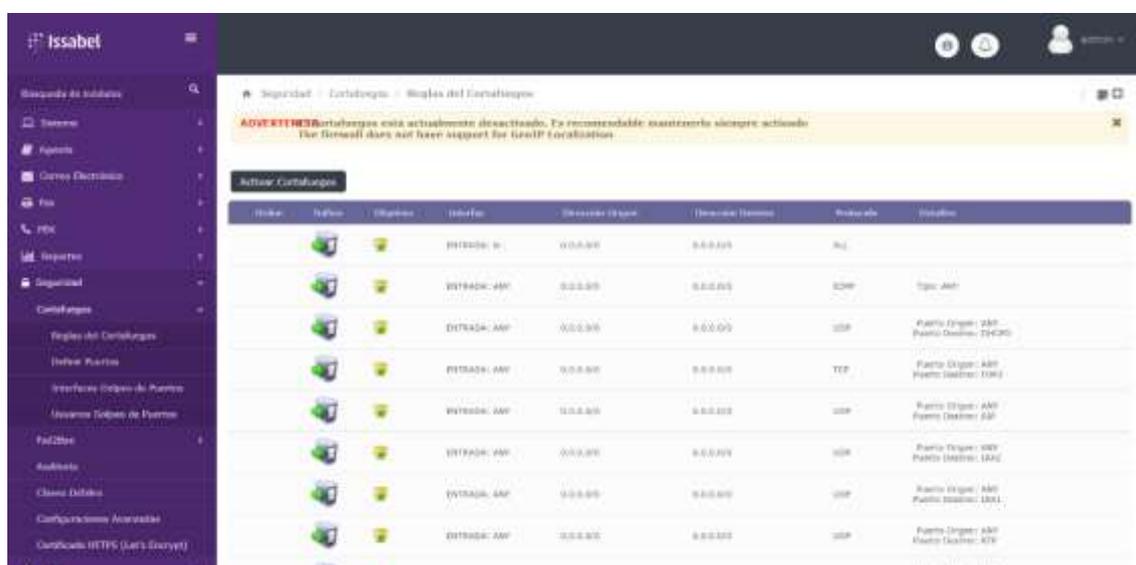
Como primer paso para garantizar la seguridad del servidor, se configuró el Firewall, el cual desempeña un papel fundamental en la protección y la configuración de seguridad.

Para activar el servicio del Firewall, se accede al panel de control y se selecciona la opción "Seguridad". A continuación, se elige la opción "Firewall" y se accede a la sección "Reglas del Firewall".

Dentro de esta sección, se encuentra el botón "Activar Firewall", en el cual se debe hacer clic para activar el Firewall y aplicar las reglas de seguridad correspondientes. Este proceso garantiza que el Firewall esté operativo y que se apliquen las configuraciones de seguridad adecuadas para proteger el servidor de posibles amenazas externas. Se muestra en la figura 23.

Es importante recordar que la configuración del Firewall debe realizarse de manera adecuada y siguiendo las mejores prácticas de seguridad, teniendo en cuenta los requisitos específicos del servidor y las necesidades de protección del sistema.

Figura 23. Activación de Firewall



Fuente: Elaboración propia (2023).

Las reglas del Firewall se configuran cuidadosamente para asegurar que no se comprometa el acceso a los recursos ofrecidos por la plataforma. En este sentido, se establecen reglas específicas que permiten controlar el tráfico y proteger el servidor de posibles amenazas externas.

Además de las reglas generales de seguridad, se creó una regla adicional para bloquear el tráfico basado en geolocalización. Esta regla tiene como objetivo restringir el acceso proveniente de ubicaciones geográficas específicas que puedan representar un riesgo para la seguridad del servidor. Al bloquear el tráfico por geolocalización, se reduce la exposición a posibles ataques y se fortalece aún más la seguridad del sistema.

4.4.9. Cambiar el puerto por defecto del servidor web

En este proceso, se llevó a cabo un cambio en el parámetro de escucha del servidor web para brindar mayor seguridad a la conexión. A continuación, se describen los pasos seguidos:

- Cambio de parámetro de escucha: Se modificó el parámetro "Listen" en el archivo de configuración del servidor web. En este ejemplo, se utilizó el puerto 9666 en lugar del puerto de escucha por defecto, que es el puerto 443. El objetivo de este cambio es fortalecer la seguridad de la conexión.
- Actualización del parámetro "virtualHost_default": Se cambió el parámetro "virtualHost_default:443" por "virtualHost_default:9666" en el archivo de configuración correspondiente. Es importante asegurarse de que el puerto especificado aquí coincida con el puerto utilizado en el parámetro "Listen" para evitar conflictos y garantizar el correcto funcionamiento del servicio.
- Reinicio del servicio web: Para que los cambios de configuración surtan efecto, se reinicia el servicio web utilizando el comando "service httpd restart" o el comando equivalente en el sistema operativo utilizado. Esto permite que el servidor web tome los nuevos parámetros y esté listo para aceptar conexiones en el puerto modificado.

Una vez completados estos pasos, se puede acceder a la página web utilizando la siguiente dirección: "https://192.168.1.189:9666". Esta nueva dirección refleja el cambio de puerto realizado y permite establecer una conexión segura con el servidor web.

Es importante destacar que estos pasos deben llevarse a cabo siguiendo las recomendaciones y mejores prácticas de seguridad, y se debe tener en cuenta la configuración específica del servidor web utilizado.

Figura 24. Cambio del puerto por defecto 443



Fuente: Elaboración propia (2023).

4.4.10. Configurar doble autenticación web

El objetivo de configurar un nivel adicional de autenticación en el servicio web es proporcionar una protección integral a todas las aplicaciones y carpetas alojadas en dicho servicio, evitando así posibles ataques remotos que aprovechen esta vulnerabilidad.

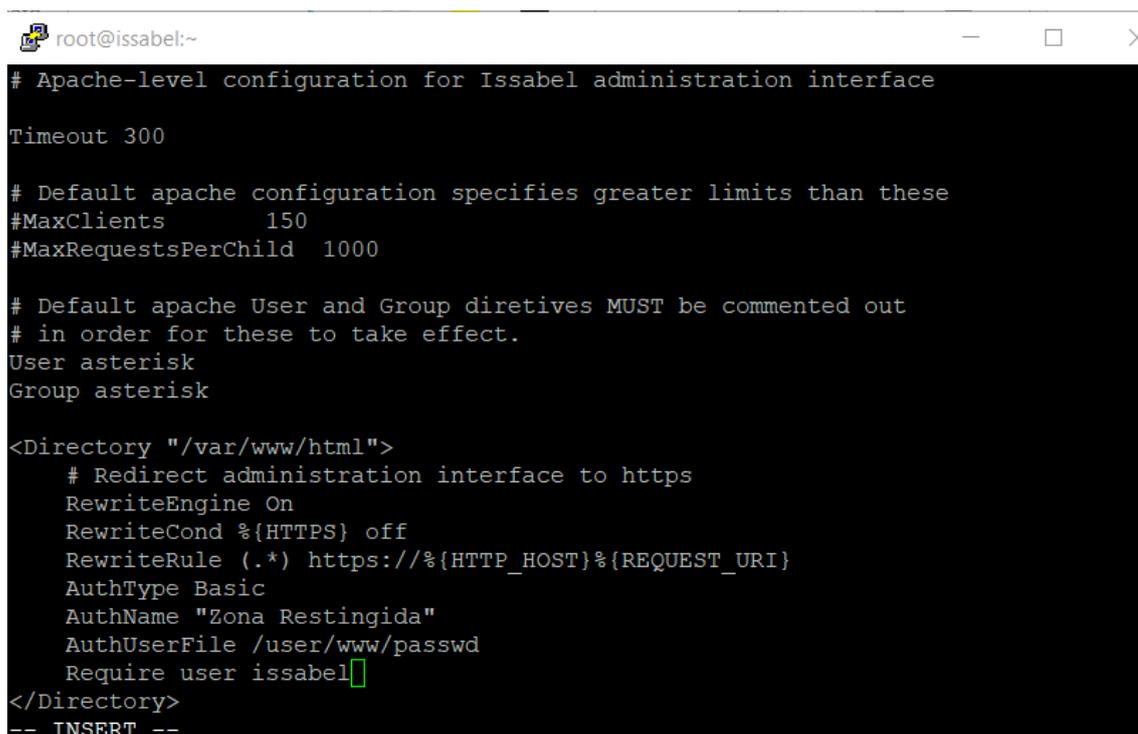
Para llevar a cabo esta configuración, se accede al archivo de configuración de Issabel ubicado en `"/etc/httpd/conf.d/issabel.conf"`. En este archivo, se agregaron los siguientes parámetros para habilitar la autenticación en el servicio web:

- **AuthType Basic:** este parámetro especifica el tipo de autenticación que se utilizará; en este caso, se utiliza la autenticación básica.
- **AuthName "Zona Restringida":** Aquí se establece el nombre de la zona restringida, que se mostrará al usuario al solicitar las credenciales de autenticación.
- **AuthUserFile /usr/www/wwwpasswd:** Se indica la ubicación del archivo que contiene los usuarios y contraseñas para la autenticación. En este caso, se utiliza el archivo `"/usr/www/wwwpasswd"`.
- **Requiere user issabel:** Con este parámetro, se establece que se requiere el usuario "issabel" para acceder a la zona restringida.

Posteriormente, se crea un usuario con el nombre "issabel", el cual se utilizará para acceder al servicio web con las credenciales correspondientes. Una vez completada esta configuración, se reinicia el servicio web utilizando el comando "service httpd restart" para que los cambios surtan efecto como se muestra en la figura 25.

Con estos pasos, se ha establecido un nivel adicional de autenticación en el servicio web de Issabel, lo que garantiza una capa de protección adicional al impedir el acceso no autorizado a las aplicaciones y carpetas publicadas.

Figura 25. Configurar doble autenticación web



```
root@issabel:~  
# Apache-level configuration for Issabel administration interface  
Timeout 300  
  
# Default apache configuration specifies greater limits than these  
#MaxClients 150  
#MaxRequestsPerChild 1000  
  
# Default apache User and Group directives MUST be commented out  
# in order for these to take effect.  
User asterisk  
Group asterisk  
  
<Directory "/var/www/html">  
  # Redirect administration interface to https  
  RewriteEngine On  
  RewriteCond %{HTTPS} off  
  RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}  
  AuthType Basic  
  AuthName "Zona Restingida"  
  AuthUserFile /user/www/passwd  
  Require user issabel  
</Directory>  
-- INSERT --
```

Fuente: Elaboración propia (2023).

4.4.11. Configuración de servicio SSH

La configuración adecuada del servicio SSH es esencial, ya que representa un punto de acceso crítico a toda la plataforma. Para garantizar la seguridad, se deben seguir los siguientes pasos:

- Acceso a la configuración de SSH: Utilizando la línea de comandos, se accede al archivo de configuración de SSH ubicado en "/etc/ssh/sshd_config". Este archivo contiene las opciones de configuración del servicio SSH.

- Cambio de puerto por defecto: Dentro del archivo de configuración, se busca la línea que indica el puerto de escucha del servicio SSH, que generalmente es "Port 22". Se cambia este valor por un puerto diferente, como "Port 25144", con el fin de dificultar los intentos de acceso no autorizados.
- Restricción del acceso al usuario "Root": Se localiza la opción "PermitRootLogin" en el archivo de configuración y se establece su valor como "no". Esto impide que el usuario "Root" pueda acceder al servicio SSH directamente, añadiendo una capa adicional de seguridad.
- Creación de un usuario adicional: Se procede a crear un nuevo usuario en el sistema utilizando el comando correspondiente. Se establece una contraseña segura para este usuario, ya que se utilizará para acceder al servicio SSH.
- Reinicio del servicio SSH: Finalmente, se reinicia el servicio SSH utilizando el comando "service sshd restart" para aplicar los cambios de configuración realizados.

Es importante destacar que al cambiar el puerto y restringir el acceso al usuario "Root", se dificulta el acceso no autorizado al servicio SSH y se mejora la seguridad del sistema como se puede observar en la figura 26.

Figura 26. Configuración de servicio SSH

```

GNU nano 2.3.1          Fichero: /etc/ssh/sshd_config          Modificado
# default value.

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 22
Port 25144
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

^G Ver ayuda  ^O Guardar  ^R Leer Fich ^M Pág Ant   ^H CortarTxt ^C Pos actual
^X Salir     ^J Justificar ^W Buscar   ^V Pág Sig  ^U PegarTxt  ^T Ortografía

```

Fuente: Elaboración propia (2023).

4.4.12. Configuración de Fail2ban

Fail2ban es una herramienta esencial para la protección de plataformas basadas en Linux, incluyendo aquellas que utilizan Asterisk como sistema de comunicación. Esta herramienta ofrece una protección proactiva al bloquear automáticamente los intentos de acceso no autorizados, tanto desde fuentes externas como internas.

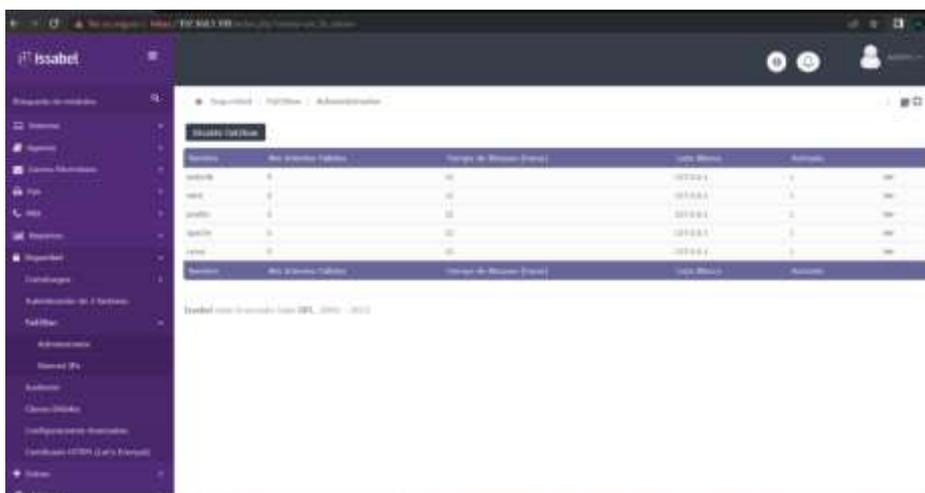
En el caso de Issabel, se ha instalado y configurado Fail2ban de manera predeterminada, lo cual se puede apreciar en la figura 27. Esto brinda protección adicional a servicios como el protocolo SIP de Asterisk y SSH, disminuyendo el riesgo de posibles ataques.

Para activar el servicio de Fail2ban, se accede al panel de control y se selecciona la opción "Security" o "Seguridad". A continuación, se elige la opción "Fail2ban" y se accede a la sección "Admin".

Dentro de esta sección, se encuentra el botón "Enable Fail2ban" o "Activar Fail2ban", en el cual se debe hacer clic para activar el servicio. Al hacerlo, Fail2ban estará activo y comenzará a proteger los servicios configurados, como el protocolo SIP de Asterisk y SSH.

Es importante destacar que Fail2ban funciona mediante la detección de patrones de comportamiento maliciosos en los registros de los servicios protegidos. Cuando se detecta un intento de acceso no autorizado, Fail2ban toma medidas automáticas para bloquear la dirección IP desde la cual se originó el intento

Figura 27. Configuración de Fail2ban



Fuente: Elaboración propia (2023).

Una vez realizada la configuración de Fail2ban, se puede observar que está funcionando de manera conjunta con IPTABLES para brindar una protección eficaz. Se ha verificado que el servicio esté protegido, incluyendo el servidor Apache y otros servicios.

Para configurar la protección de cada servicio, se siguen los siguientes pasos:

Acceso a la configuración del servicio: Se selecciona el servicio correspondiente, en este caso, Asterisk, y se hace clic en la opción "View" o "Ver" en el panel de administración. Luego, se selecciona la opción "Editar" para acceder a la configuración del servicio.

Parámetros de configuración: En la configuración del servicio Asterisk, se establecen los parámetros necesarios para la protección. Algunos de los parámetros comunes incluyen:

- **Count failed Attempts:** Se define la cantidad de intentos fallidos que se deben producir antes de generar el bloqueo de la dirección IP. Esto permite establecer un umbral para detectar posibles intentos de acceso no autorizados.
- **Ban Time:** Se especifica la cantidad de horas durante las cuales la dirección IP estará bloqueada después de haber superado el límite de intentos fallidos. Este parámetro determina la duración del bloqueo.
- **Whitelist:** Se puede configurar una lista blanca (Whitelist) para especificar direcciones IP o segmentos que no serán tomados en cuenta para el bloqueo. Esto es útil para evitar el bloqueo accidental de direcciones IP legítimas.
- **Enabled:** Se habilita o deshabilita la protección del servicio en Fail2ban. Esto permite activar o desactivar la protección según sea necesario.
- **Guardar los cambios:** Una vez realizada la configuración deseada, se guardan los cambios y se aplican en el servicio Asterisk.

Con estos pasos, se configura la protección de cada servicio en Fail2ban. La configuración de parámetros como "Count failed attempts", "Ban Time", "Whitelist" y "Enabled" permite personalizar la protección según las necesidades específicas de cada servicio.

4.4.13. Configuración de ACL a nivel SIP

Una práctica recomendada es implementar reglas de control de acceso a nivel de las extensiones SIP, lo que permitirá que solo las direcciones IP o rangos de IP específicos puedan registrar y utilizar estas extensiones. Para activar esta configuración, se deben seguir los siguientes pasos:

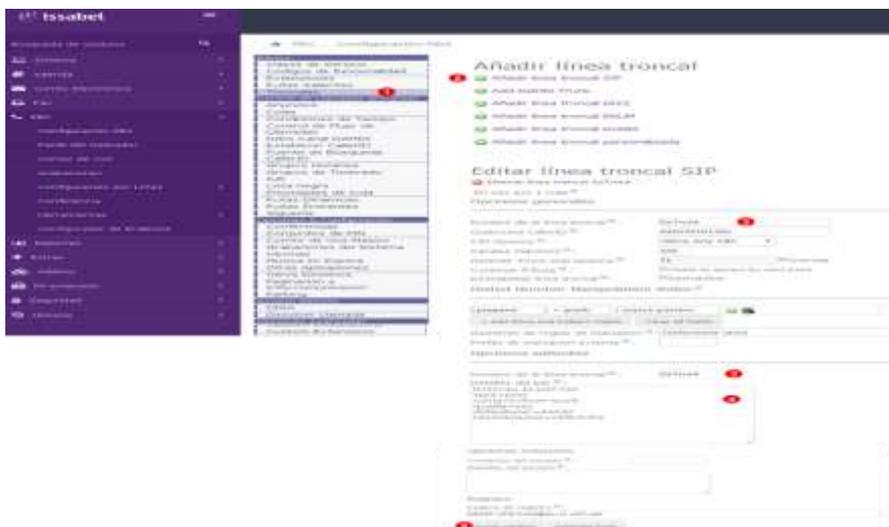
Acceso a la configuración de cada extensión: Se selecciona la extensión que se desea configurar, por ejemplo, la extensión 100, y se accede a la opción de edición en el panel de administración. Esto permitirá modificar la configuración de la extensión.

Configuración de las reglas de control de acceso: Dentro de la configuración de la extensión, se busca la sección relacionada con el control de acceso o las direcciones IP permitidas. En esta sección, se añaden las direcciones IP o rangos de IP que se permitirán acceder y registrar en esta extensión.

Guardar los cambios: Una vez añadidas las direcciones IP o rangos de IP permitidos, se guardan los cambios realizados en la configuración de la extensión.

Siguiendo estos pasos, se activa el control de acceso a nivel de las extensiones SIP. Cada extensión puede ser configurada de manera individual para permitir únicamente a las direcciones IP especificadas acceder y utilizar dicha extensión, como se muestra en la figura 28.

Figura 28. Configuración de ACL a nivel SIP



Fuente: Elaboración propia (2023).

4.4.14. Alertas para llamadas internacionales

El código presentado en la figura 29 muestra una implementación que permite enviar un correo electrónico automáticamente cuando se realiza una llamada internacional. A continuación, se detallan los pasos necesarios para configurar esta funcionalidad:

1. Acceso al código: Se accede al archivo de código fuente correspondiente al sistema de comunicaciones, donde se encuentra el código que controla la funcionalidad de las llamadas.
2. Identificación del evento de llamada internacional: Se busca el fragmento de código que maneja los eventos de llamadas y se identifica el punto en el que se detecta una llamada internacional. Esto se puede determinar mediante una comparación de información relacionada con la llamada, como el código de país o el número de destino.
3. Inclusión del código de envío de correo electrónico: Una vez identificado el punto adecuado en el código, se añade el código necesario para enviar un correo electrónico cuando se detecta una llamada internacional. Esto implica utilizar las funciones y bibliotecas adecuadas para enviar el correo electrónico, incluyendo la configuración de los destinatarios, el asunto y el contenido del correo.
4. Personalización del correo electrónico: Se puede personalizar el contenido del correo electrónico según las necesidades específicas, incluyendo información sobre la llamada realizada, el número de origen, el número de destino y cualquier otra información relevante.
5. Pruebas y validación: Una vez agregado el código, se realizan pruebas para asegurarse de que la funcionalidad de enviar el correo electrónico se active correctamente cuando se detecte una llamada internacional. Se verifica que el correo electrónico se envíe a los destinatarios deseados y que el contenido sea correcto.

Figura 29. *Alertas para llamadas internacionales*

```
1) exten=>_0.,n,System(/bin/echo "Llamada LDN al numero ${NUMERO} Del usuario : ${CONTRASENA} Realizada : ${calltime} " >
/etc/asterisk/email.txt)
2) exten=>_0.,n,System(/bin/mail -s ALERTA-LLAMADA-LDN joliva@silcom.com.pe</etc/asterisk/email.txt)
3) exten=>_0.,n,Dial(SIP/TRONCAL/${NUMERO})
```

Fuente: Elaboración propia (2023).

4.4.15. Alertas ante cambio de configuraciones

La configuración requerida implica la instalación y configuración del servicio INCROND para monitorear los eventos que ocurren en el sistema de archivos. A continuación, se describen los pasos necesarios para llevar a cabo esta tarea:

1. **Instalación de INCROND:** Se debe instalar el servicio INCROND en el sistema. Esto se logra utilizando los comandos adecuados del gestor de paquetes del sistema operativo.
2. **Configuración del monitoreo:** Una vez instalado INCROND, se procede a configurar los eventos y directorios que se desean monitorear. Esto se realiza mediante la creación de archivos de configuración específicos para cada evento o directorio que se desea observar.
3. **Especificación de eventos:** En cada archivo de configuración, se especifican los eventos a los que se desea estar atento. Estos eventos pueden incluir modificaciones de archivos, creaciones, eliminaciones, cambios de permisos, entre otros.
4. **Definición de acciones:** Junto con cada evento, se debe definir una acción específica que se llevará a cabo cuando se produzca ese evento. Esto puede incluir la ejecución de un script, el envío de una notificación o cualquier otra acción requerida.
5. **Reinicio del servicio:** Una vez completada la configuración de los eventos y acciones, se reinicia el servicio INCROND para aplicar los cambios y asegurarse de que esté funcionando correctamente.

Con estos pasos, se logra la instalación y configuración del servicio INCROND para monitorear eventos en el sistema de archivos, como se observa en la figura 30.

Figura 30. Configuración de alerta de cambio

```
root@issabel ~|# yum install incron
Complementos cargados:fastestmirror
loading mirror speeds from cached hostfile
* base: mirror.cedia.org.ec
* centosplus: mirror.cedia.org.ec
* commercial-addons: repo.issabel.org
* epel: mirror.cedia.org.ec
* epel-debuginfo: mirrors.iul3.net
* epel-source: mirrors.iul3.net
* extras: mirror.cedia.org.ec
* issabel-base: repo.issabel.org
* issabel-beta: repo.issabel.org
* issabel-extras: repo.issabel.org
* issabel-updates: repo.issabel.org
* updates: mirror.cedia.org.ec
Resolviendo dependencias
--> Ejecutando prueba de transacción
--> Paquete incron.x86_64 0:0.5.12-11.el7 debe ser instalado
--> Resolución de dependencias finalizada
Dependencias resueltas
```

Fuente: Elaboración propia (2023).

Creación y configuración del archivo "monitor_archivos_issabel": Se crea un archivo de configuración con el nombre "monitor_archivos_issabel" y se realizan las siguientes modificaciones:

1. Se especifica la carpeta que se desea monitorear, en este caso, "/etc/asterisk".
2. Se define el evento que se va a monitorear, en este caso, "IN_MODIFY", que indica una modificación en los archivos.
3. Se establece el script "incron_email.sh" al cual se enviarán los parámetros correspondientes cuando se active el evento.
4. Los parámetros "\$@" , "\$#" , y "\$%" son utilizados para transmitir información sobre el archivo o directorio modificado, su nombre, y el evento que se activó, respectivamente.
5. Creación del archivo "incron_email.sh": Se crea un archivo de script llamado "incron_email.sh" que recibirá los parámetros definidos en el archivo de configuración "monitor_archivos_issabel". Este script puede ser personalizado para enviar una alerta por correo electrónico cuando se detecten cambios en los archivos monitorizados.
6. Configuración de la función fuera del horario laboral (opcional): Si se desea, se puede agregar una función adicional en el script "incron_email.sh" para manejar eventos fuera del horario laboral, como enviar alertas a un grupo de administradores específicos.

Siguiendo estos pasos, se configura el monitoreo de cambios en los archivos `extensions_custom.conf` y `sip_general.conf` utilizando el servicio INCROND.

Cuando se produzca una modificación en cualquiera de estos archivos, se activará el evento correspondiente y se enviarán los parámetros al script "incron_email.sh", permitiendo el envío de alertas por correo electrónico.

4.4.16. Certificación del servidor y Cliente

La configuración de un certificado en el servidor es una medida importante para proteger la información y evitar que sea accesible por terceros no autorizados. A continuación, se detallan los pasos necesarios para llevar a cabo esta configuración:

1. Descarga el certificado para el servidor: En primer lugar, se debe obtener un certificado adecuado para el servidor. Esto puede implicar obtener un certificado de una autoridad de certificación reconocida o generar un certificado autofirmado.
2. Apertura del FTP: Se abre el servicio de FTP en el servidor para permitir la transferencia del certificado desde una ubicación externa al servidor. Esto implica configurar y activar el servicio de FTP en el servidor.
3. Instalación del certificado en el servidor: Una vez que el certificado se encuentre en el servidor, se procede a su instalación. Esto implica seguir los pasos específicos según el servidor y la configuración utilizada, que pueden variar según el software y el sistema operativo.
4. Descarga del certificado para el cliente: A continuación, se realiza la descarga del certificado desde el servidor para su instalación en los clientes. Esto se puede hacer a través del FTP o de cualquier otro método de transferencia de archivos seguro.
5. Instalación del certificado en el cliente: Una vez que el certificado se encuentre en el cliente, se procede a su instalación. Esto implica seguir los pasos específicos según el cliente y la configuración utilizada, que pueden variar según el software y el sistema operativo.
6. Verificación de la seguridad: Finalmente, se realiza una verificación para asegurarse de que la información ya no sea vulnerable y esté protegida por el certificado. Esto se puede hacer mediante pruebas de conexión segura y verificación de que la comunicación entre el servidor y el cliente esté encriptada.

Es importante tener en cuenta que los pasos específicos pueden variar dependiendo del software, el sistema operativo y la configuración utilizada en el servidor y los clientes.

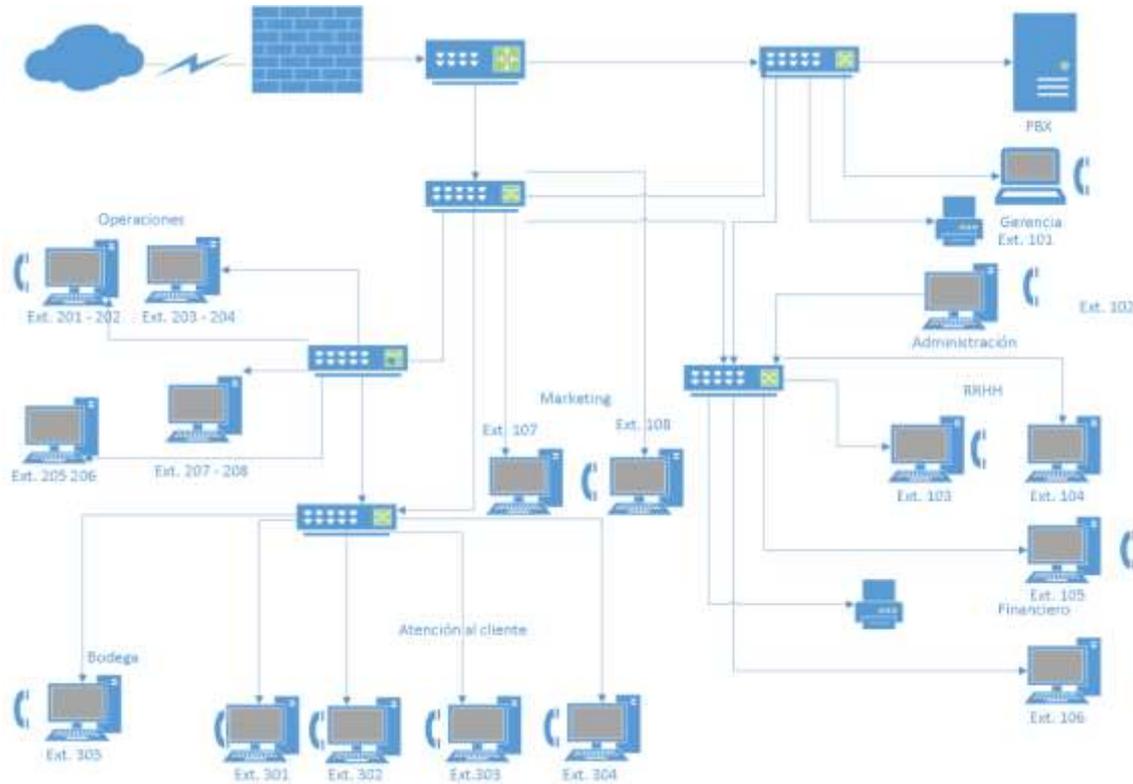
4.5. Fase 5: Cierre

En la fase final de implementación y aplicación de QoS con políticas de seguridad, se presenta un cierre que resume los resultados obtenidos. Este cierre incluye los siguientes elementos:

1. Diagrama de red: Se muestra un diagrama que representa la estructura de la red y las extensiones telefónicas asignadas a cada departamento. Este diagrama proporciona una visión general de la configuración de la red telefónica en la empresa.
2. Tabla de empleados: Se presenta una tabla que detalla la información de los empleados, incluyendo sus nombres, departamentos y números de extensión asignados. Esta tabla proporciona una referencia rápida y clara de la distribución de extensiones en la organización.
3. Evaluación de un experto en telefonía VoIP: Se incluye una evaluación realizada por un experto en telefonía VoIP, en la cual se analiza el desempeño del sistema implementado. Esta evaluación puede abordar aspectos como la calidad de las llamadas, la estabilidad del servicio y la eficiencia de las políticas de seguridad implementadas.
4. Resultados de QoS basados en políticas de seguridad: Se presentan los resultados obtenidos a través de la implementación de políticas de QoS y seguridad. Estos resultados pueden incluir mejoras en la calidad de las llamadas, mayor estabilidad del sistema, reducción de problemas de seguridad y una experiencia general mejorada para los usuarios.

4.5.1. Distribución actual de la red LAN y servicios habilitados

Figura 31. Diagrama de red LAN de la empresa SEPRIVZAM post Implementación



Fuente: Elaboración propia (2023).

Según se aprecia en la figura 31, después de las instalaciones y configuraciones realizadas se logró dotar a cada equipo de la empresa con una extensión, de esa forma cada colaborador podrá hacer uso de los servicios de telefonía IP, videoconferencias y mensajería instantánea. Además, con la configuración e instalación del servidor VoIP se logró comunicar a colaboradores de forma más controlada y con las políticas de QoS se brindó las seguridades al momento de realizar llamadas.

A continuación, se expone en la tabla 6 de los departamentos y los servicios de comunicaciones con las extensiones habilitadas.

Tabla 6. Resumen de departamentos, empleados, equipos, teléfonos y servicios de comunicaciones post implementación.

Departamentos	N° de empleados.	N° de PC	N° de extensión
---------------	------------------	----------	-----------------

Gerencia	1	1	101
Administración.	1	1	102
Recursos Humanos.	2	2	103 -104
Financieros.	2	2	105 -106
Operaciones.	8	4	201,202,203,204,205,206,207,208
Marketing.	2	2	107 – 108
Bodega.	2	1	305
Atención al Cliente.	4	4	301, 302, 303,304
Subtotal	22	17	16

Fuente: Elaboración propia (2023).

En la tabla 6 se puede observar un resumen de los departamentos, los equipos disponibles, el número de colaboradores y los servicios de comunicaciones unificadas habilitados. Con la implementación y configuración del servidor PBX se ha conseguido comunicar a todos los miembros de la compañía. Además, mediante el enlace VPN ahora es posible la comunicación entre matriz principal y sucursales.

4.5.2. Evaluación de resultados por experto en telefonía IP

La evaluación de los resultados de la configuración del servidor PBX de Issabel y la aplicación de QoS basado en seguridad fue realizada por el Ing. Xavier Amable Sánchez Erazo, un reconocido experto en telefonía IP y comunicaciones unificadas, actualmente director de proyectos en la empresa multinacional GEA-ECUADOR, con el número de identificación C.I: 0920744505.

Durante la implementación de las políticas de QoS y seguridad en el servidor PBX de Issabel, se siguieron las siguientes etapas:

Etapas de revisión y configuración básica del servidor: Se realizó una revisión exhaustiva de las configuraciones básicas del servidor, asegurándose de establecer una conexión adecuada, habilitando los puertos de consola necesarios y configurando una dirección IP estática para evitar problemas con los softphones y el acceso al sitio web del servicio. Además, se aplicaron políticas de creación de contraseñas seguras, con una longitud mínima de 13 dígitos, y se aseguró de mantener el servidor actualizado con los últimos repositorios y establecer políticas de seguridad.

Etapa de evaluación y ataque: Se llevó a cabo un ataque simulado al servidor PBX utilizando aplicativos diseñados para vulnerar los puertos lógicos del sistema. Para realizar este análisis, se instaló un entorno virtualizado que permitió realizar pruebas sin afectar la infraestructura de producción. Durante este proceso, se identificaron las vulnerabilidades que permitieron el ataque y se documentaron los resultados obtenidos.

Etapa de implementación de políticas de seguridad: Se implementaron diversas políticas de seguridad para proteger el servidor PBX y los servicios de comunicación de la compañía. Esto incluyó la configuración de firewalls, autenticación de usuarios, configuración de SSH, configuración de Fail2ban para la detección de intentos de acceso no autorizados, alertas de cambios en la configuración y encriptación de datos. También se estableció una política de priorización de tráfico para asegurar que las llamadas de voz y videoconferencias tuvieran prioridad sobre otros tipos de tráfico en la red. Se implementó QoS en el router o switch de la red para garantizar un rendimiento óptimo de los servicios de comunicación.

Estos pasos permitieron mejorar el control y las políticas de QoS y seguridad en el servidor PBX de Issabel, asegurando un medio de comunicación oficial confiable para los colaboradores de la empresa y eliminando los problemas de comunicación previamente identificados. La evaluación realizada por el Ing. Xavier Amable Sánchez Erazo, respaldada por su experiencia en el campo de las comunicaciones, garantiza la eficacia y calidad de las medidas implementadas.

4.5.3. Resultado de la implementación de las políticas QoS basado en seguridad

Tras realizar una evaluación exhaustiva del servidor PBX Issabel utilizando herramientas de vulnerabilidad, se descubrió la existencia de varios puertos lógicos abiertos, lo que permitía el acceso sin restricciones mediante una herramienta específica. Sin embargo, mediante la implementación de medidas de QoS basadas en seguridad, se logró mejorar significativamente la integridad del sistema, proporcionando así una protección sólida contra posibles ataques de hackers.

Con el objetivo de fortalecer la seguridad del servidor Issabel PBX, se realizaron diversas configuraciones tanto en la seguridad básica como en la aplicación Asterisk, garantizando así la confiabilidad de las comunicaciones de la compañía y evitando fraudes o suplantaciones de identidad por parte de miembros no autorizados. Además, se llevó a cabo el cambio de los puertos por defecto y se configuraron certificados SSL para encriptar las comunicaciones, protegiendo así la información confidencial y evitando su exposición.

Para asegurar la efectividad de las medidas de seguridad implementadas y la correcta aplicación del QoS, se llevaron a cabo pruebas exhaustivas y se verificó su funcionamiento adecuado. Se realizó una evaluación final de la configuración del servidor PBX, así como de las políticas de seguridad y QoS aplicadas. Los resultados obtenidos se presentaron junto con recomendaciones detalladas a los responsables de Tecnologías de la Información (TI) de la empresa.

En resumen, la aplicación de políticas de QoS basadas en seguridad ha contribuido a tener un servidor más integrado y una información más segura, lo que previene posibles ataques futuros y el robo de información crucial para la empresa. La evaluación exhaustiva de la configuración del servidor PBX y la implementación de medidas de seguridad y QoS han garantizado un sistema óptimo y seguro, brindando tranquilidad a la organización en cuanto a la protección de sus datos y comunicaciones

Conclusión

Una vez implementada la propuesta tecnológica, se logra concluir que:

- Se realizó una búsqueda de todos los referentes teóricos pertinentes al tema de investigación. Estos conceptos teóricos fueron de primordial utilidad contribuyendo al conocimiento del estudio investigativo, aportando en la esquematización para el diseño del servidor y lograr una mejor adaptación del sistema a las necesidades de la empresa.
- A su vez, se hizo un levantamiento informativo de la situación actual de la empresa, aplicando las herramientas y técnicas de investigación escogidas, a esta información se le dio una serie de análisis que identificó la necesidad de mejorar el proceso de comunicación en la empresa

SEPRIVZAM, puesto que, su problemática era el control de llamadas debido al uso de la telefonía analógica. A pesar de los ataques que la empresa podría sufrir debido a la implementación del sistema VoIP se realizaron varias pruebas de vulnerabilidad para comprobar que la empresa no sufra ningún tipo de ataque al ser implementado el sistema VoIP, pasando con éxito todas las pruebas, haciéndolas seguras para la empresa.

- Se logró esquematizar el diseño del servidor de VoIP con políticas de QoS dotando a cada equipo de la empresa de los cuales hacen uso los trabajadores consiguiendo una importante comunicación entre ellos.
- Se procedió con la instalación y configuración del servidor PBX, se elige el software Issabel por sus excelentes funciones, ya que es considerado como un referente en telefonía IP, este software también ha contribuido a los servicios de otras comunicaciones unificadas como videoconferencia y mensajería instantánea, de acuerdo con las necesidades de la compañía, lo que permitió establecer un medio de comunicación oficial para los colaboradores. Se configuraron extensiones para cada empleado, lo que les permitió contar con servicios de telefonía IP, videoconferencia y mensajería. haciendo que este proceso de comunicación sea ahora más completo y se alineó a los requisitos que posee la empresa para solucionar su problema.
- Se realizó una identificación a través de las herramientas para evaluar QoS por ejemplo Wireshack y Nmap para verificar vulnerabilidades como algún puerto lógico o puerta de enlace que constaba el servidor para evitar posible ataque de Hacker.
- Después, en la implementación se aplicó QoS basados en políticas de seguridad en el servidor PBX de Issabel permitiendo una mayor integridad en el sistema fuera de vulnerabilidades y posibles ataques al servidor.
- Se llevó a cabo una evaluación de los resultados por un experto en telefonía IP. La evaluación de los resultados concluyó que la implementación de la propuesta tecnológica permitió a la empresa SEPRIVZAM da un gran paso hacia la automatización de uno de los procesos más importantes de cualquier empresa como es la comunicación

con la implementación de QoS basado en políticas de seguridad en el servidor Issabel PBX mejorando el control, seguridad y rendimiento de los sistemas de comunicaciones empresariales.

Recomendaciones

Concluido el estudio, se realizan las siguientes recomendaciones.

- Analizar la contratación de otro proveedor de internet para evitar interrupción de servicio.
- Considerar la contratación de un VPN del proveedor para posible expansión a otras sucursales de la empresa.
- Adquirir una licencia comercial para contar con este servicio a largo plazo.
- Proceder con capacitaciones a los empleados de la empresa para que realicen el correcto uso de las herramientas de comunicación y de esta forma aumentar su productividad.
- Ejecutar una evaluación periódica de la calidad del servicio de telefonía IP para asegurarse de que se esté cumpliendo con los estándares de calidad establecidos.
- Realizar pruebas de penetración periódicas para identificar vulnerabilidades en el sistema y mejorar la seguridad.
- Establecer políticas de uso aceptable para los empleados de la empresa para evitar el uso inapropiado de los servicios de comunicación.

Bibliografía

3CX. (2021). *¿Qué son los teléfonos SIP?* Obtenido de <https://www.3cx.es/voip-sip/telefonos-sip/>

3CX. (2023). 3CX. Obtenido de Acerca de 3CX: <https://www.3cx.es/empresa/>

Alemany, A. P. (2022). *Entrenamiento de observación de acciones e imaginaria motora como herramientas de innovación educativa para entrenar habilidades en los alumnos de fisioterapia.* Obtenido de <https://www.semanticscholar.org/paper/Entrenamiento-de-observaci%C3%B3n-de-acciones-e-motora-Alemany-Arbizu/48c577c0ebd803a9f724a2b34f305406e4ce3a09>

Altube, R. (2023). *Wireshark: Qué es y ejemplos de uso.* Obtenido de OpenWebinars.net: <https://openwebinars.net/blog/wireshark-que-es-y-ejemplos-de-uso/>

Amira A. Mohamed, a. A. (2023). *Enhanced Multiple Speakers' Separation and Identification for VOIP Applications Using Deep Learning.* Obtenido de Scopus: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85152563735&origin=resultslist&sort=plf-f&src=s&st1=VoIP+research+method&sid=9ea8f05d6359c61387f0cbee60b668b8&sot=b&sdt=b&sl=35&s=TITLE-ABS-KEY%28VoIP+research+method%29&relpos=0&citeCnt=0&searchTerm=>

Ayala, M. (2021). *¿Qué son los métodos de investigación?* Obtenido de Lifeder: <https://www.lifeder.com/tipos-metodos-de-investigacion/>

- Blass, D. D. (2019). *GlobbIT*. Obtenido de Los sistemas de voz IP (VoIP) pueden reducir los gastos hasta en un 80%, según Masvoz - GlobbIT: <https://www.globbit.com/voz-ip-voip-reducir-gastos-14155/>
- Cabrera, C. (29 de Junio de 2022). *¿Qué es un softphone?* Obtenido de <https://enlaza.mx/blog/que-es-un-softphone/>
- Cano, A. (2007). *Voz sobre IP: otra forma de comomunicación*. Obtenido de <https://www.semanticscholar.org/paper/Voz-sobre-IP%3A-otra-forma-de-comomunicaci%C3%B3n-Cano/49888d5d334b2b28773aa7cdcf30d6dbd7399c6f>
- Carvalho, C. (2021). *Risk Management Applied to Organizational Strategy – A Case Study Applied to a Continuous Billet Forming Machine*. Obtenido de <https://www.semanticscholar.org/paper/Risk-Management-Applied-to-Organizational-Strategy-Carvalho-Antunes/a7eb495ab405cdc88b651abd4e50a83d90a69773>
- Castillo, A. (2020). *Que es IssabelPBX. CoopSys | CoreBank*. Obtenido de <https://www.coopsys.com.do/noticias/blog/que-es-issabelpbx/>
- Chagoza, E. R. (2021). *Métodos y técnicas de investigación*. Obtenido de Gestipolis.: <https://www.gestipolis.com/metodos-y-tecnicas-de-investigacion/>
- Citelia. (2022). *Qué es un softphone y cómo funciona*. Obtenido de <https://citelia.es/blog/que-es-un-softphone-funcionamiento/>
- Cortex. (2018). *NetworkMiner, Herramienta forense de Análisis de Red*. Obtenido de DragonJAR - Servicios de Seguridad Informática:

<https://www.dragonjar.org/networkminer-herramienta-forense-de-analisis-de-red.xhtml>

Criollo, B. M. (Marzo de 2020). *Políticas de QoS en redes empresariales para el análisis de rendimiento, en entornos convencionales y SDN*. Obtenido de Escuela Superior Politecnica de Chimborazo:
<http://dspace.esPOCH.edu.ec/bitstream/123456789/14090/1/20T01328.pdf>

Cuadra, P. E. (29 de Octubre de 2021). *Estudio y diseño de un sistema de comunicaciones unificadas VoIP basado en Elastix con seguridad perimetral*. Obtenido de Estudio y diseño de un sistema de comunicaciones unificadas VoIP basado en Elastix con seguridad perimetral: <http://201.159.223.180/bitstream/3317/17640/1/T-UCSG-PRE-MTEL-205.pdf>

Download IssabelPBX. (2023). Obtenido de <https://sourceforge.net/projects/issabelpbx/files/latest/download>

Galindo, E. M. (2021). *LA POBLACIÓN EN UNA INVESTIGACIÓN*. Obtenido de <https://tesis-investigacion-cientifica.blogspot.com/2013/08/que-es-la-poblacion.html>

Gladys Patricia Guevara Alban, Alexis Eduardo Verdesoto Arguello, Nelly Esther Castro Molina. (2020). *Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción)*. Obtenido de recimundo.com: <https://recimundo.com/index.php/es/article/view/860>

Godoy, F. (2023). *las mejores técnicas de investigación* . Obtenido de Tesis y Másters Colombia: <https://tesisymasters.com.co/tecnicas-de-investigacion/>

- González, G. (2020). *Variables de investigación: tipos, características y ejemplos*.
Obtenido de Lifeder: <https://www.lifeder.com/variables-de-investigacion/>
- IP, M. (2023). *Softphone Zoiper · Qué es, para qué sirve y características*. Obtenido de
Más IP Telecomunicaciones : <https://www.masip.es/blog/softphone-zoiper/>
- Issabel. (2019). *Unified Communications Freedom*. Obtenido de Unified
Communications Freedom.: <https://www.issabel.com/>
- Jervis, T. M. (2018). *Investigación descriptiva: características, técnicas, ejemplos*.
Obtenido de lifeder: <https://www.lifeder.com/investigacion-descriptiva>
- Júnior, S. H. (2021). *PROPOSTA DE REDUÇÃO DE CUSTOS DE TELEFONIA UTILIZANDO GATEWAY GSM: ESTUDO DE CASO NO HOSPITAL DAS CLÍNICAS DA UNIVERSIDADE FEDERAL DE PERNAMBUCO*. Obtenido de
<https://www.semanticscholar.org/paper/PROPOSTA-DE-REDU%C3%87%C3%83O-DE-CUSTOS-DE-TELEFONIA-GATEWAY-J%C3%BAnior-Medeiros/3b5c8217907c01657832e0b2098c3ed3d8394bbf>
- Kapinda, c. (2018). *Implementation of Open-Source and Secure VoIP systems with integrated Softphone Software on Personal Computers and Mobile Devices (Conference ID : CFP / 458 / 2017)*. Obtenido de Semantic Scholar:
<https://www.semanticscholar.org/paper/Implementation-of-Open-Source-and-Secure-VoIP-with-Kapinda/8d00a9f2bd2ed084f17286c4f3f2e2d6e2876ddb>
- Khurana, V. (2022). *¿Cómo capturar y analizar el tráfico de red con tcpdump?* Obtenido de Geekflare: <https://geekflare.com/es/tcpdump-examples/>

- Kozma, A. (2022). *Sistema Telefonico - VoIP* . Obtenido de cloudtalk:
<https://www.cloudtalk.io/es/blog/como-funciona-voip/>
- Lifeder. (2020). *Enfoque de la investigación: tipos y características*. Obtenido de
<https://www.lifeder.com/enfoque-investigacion/>
- ManageEngine. (2022). *Sobre la calidad de servicio (QoS) | Calidad de servicio en redes - ManageEngine NetFlow Analyzer*. Obtenido de
<https://www.manageengine.com/latam/netflow/calidad-de-servicio-qos.html>
- Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio. *International Journal of Morphology*, 35(1), 227 - 232. doi:10.4067/s0717-95022017000100037
- Martínez, D. J. (2018). *Estudio de tecnologías y mercados existentes en el Ecuador para voz sobre IP (VoIP)*. Obtenido de <https://www.semanticscholar.org/paper/Estudio-de-tecnolog%C3%ADas-y-mercados-existentes-en-el-Martinez-Carrasco/fe7af12175ed5eee783f94bf5a42664e4f7af917>
- Matango, F. (2019). *xlite | VoIP*. Obtenido de VoIP:
<http://www.servervoip.com/blog/tag/xlite/#:~:text=Softphone%20X%20%E2%80%93%20lite%3A,basado%20en%20e%20l%20protocolo%20SIP.>
- Muguira, A. (2023). *Tipos de entrevistas y sus características*. Obtenido de QuestionPro:
<https://www.questionpro.com/blog/es/tipos-de-entrevista/>
- Muñoz, A. (2022). *Tecnologías de la información y la comunicación para educar en salud: revisión sistemática*. Obtenido de
<https://www.semanticscholar.org/paper/Tecnolog%C3%ADas-de-la->

informaci%C3%B3n-y-la-comunicaci%C3%B3n-en-Mu%C3%B1oz-
Mu%C3%B1oz/7f972cc3540da554c7b5fdc8cd3b8f2be9dcd3f4

Observatorio empresarial para el crecimiento inclusivo. (2019). *Conclusiones del informe “Tecnología con propósito. El impacto social de la empresa en la era digital”*.

Obtenido de <https://www.crecimientoinclusivo.org/9-conclusiones-del-informe-tecnologia-proposito-impacto-social-la-empresa-la-digital/>

Ortega, M. (2018). *Evaluation of the voice quality and QoS in real calls using different*

voice over IP codecs. Obtenido de Semantic scholar:

[https://www.semanticscholar.org/paper/Evaluation-of-the-voice-quality-and-](https://www.semanticscholar.org/paper/Evaluation-of-the-voice-quality-and-QoS-in-real-IP-Ortega-Altamirano/d2f39626cd2470fd3a338a5ae893fe8a6669bab1)

[QoS-in-real-IP-Ortega-](https://www.semanticscholar.org/paper/Evaluation-of-the-voice-quality-and-QoS-in-real-IP-Ortega-Altamirano/d2f39626cd2470fd3a338a5ae893fe8a6669bab1)

[Altamirano/d2f39626cd2470fd3a338a5ae893fe8a6669bab1](https://www.semanticscholar.org/paper/Evaluation-of-the-voice-quality-and-QoS-in-real-IP-Ortega-Altamirano/d2f39626cd2470fd3a338a5ae893fe8a6669bab1)

Packer, J. (2018). *Accesibilidad VoIP: estudio de usabilidad de los sistemas de voz sobre*

protocolo de internet (VoIP) y encuesta a los usuarios de VoIP con discapacidad

visual. Obtenido de [https://www.semanticscholar.org/paper/Accesibilidad-](https://www.semanticscholar.org/paper/Accesibilidad-VoIP%3A-estudio-de-usabilidad-de-los-de-Packer-Reuschel/a2a422b2b11ba11704e5d0585572c39f5b6923ce)

[VoIP%3A-estudio-de-usabilidad-de-los-de-Packer-](https://www.semanticscholar.org/paper/Accesibilidad-VoIP%3A-estudio-de-usabilidad-de-los-de-Packer-Reuschel/a2a422b2b11ba11704e5d0585572c39f5b6923ce)

[Reuschel/a2a422b2b11ba11704e5d0585572c39f5b6923ce](https://www.semanticscholar.org/paper/Accesibilidad-VoIP%3A-estudio-de-usabilidad-de-los-de-Packer-Reuschel/a2a422b2b11ba11704e5d0585572c39f5b6923ce)

Pantelis Koutroumpis, Aija Leiponen; Llewellyn D.W., Thomas. (2020). Small is big in

ICT: The impact of R&D on productivity. *Telecommunications Policy*, 1-5.

Quiroz, R. A. (2018). *Implementación de la Gestión de Prioridades de una red de*

telefonía IP al interior de una empresa, utilizando SS7. Obtenido de

[https://www.semanticscholar.org/paper/Implementaci%C3%B3n-de-la-](https://www.semanticscholar.org/paper/Implementaci%C3%B3n-de-la-Gesti%C3%B3n-de-Prioridades-de-una-Quiroz-Gutierrez/cc02338b6ed7a15aac2aa37b419c4cc3e30579b0)

[Gesti%C3%B3n-de-Prioridades-de-una-Quiroz-](https://www.semanticscholar.org/paper/Implementaci%C3%B3n-de-la-Gesti%C3%B3n-de-Prioridades-de-una-Quiroz-Gutierrez/cc02338b6ed7a15aac2aa37b419c4cc3e30579b0)

[Gutierrez/cc02338b6ed7a15aac2aa37b419c4cc3e30579b0](https://www.semanticscholar.org/paper/Implementaci%C3%B3n-de-la-Gesti%C3%B3n-de-Prioridades-de-una-Quiroz-Gutierrez/cc02338b6ed7a15aac2aa37b419c4cc3e30579b0)

Refaet, A. (2020). *VoIP Performance Evaluation and Capacity Estimation Using different QoS Mechanisms*. Obtenido de IOP Conference Series: Materials Science and Engineering Open Access: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85090280898&origin=resultslist&sort=plf-f&src=s&st1=QoS+in+voip&nlo=&nlr=&nls=&sid=0f4edd64c2bdf9bd154f29b aa7c47a02&sot=b&sdt=b&sl=26&s=TITLE-ABS-KEY%28QoS+in+voip%29&relpos=83&citeCnt=2&searchTerm=>

Rodríguez, D. (2020). *Estudio de investigación: qué es, tipos y ejemplos*. Obtenido de Lifeder: <https://www.lifeder.com/estudio-de-investigacion/>

Roy, Om Prakash y Kumar, Vinod. (2021). *A survey on voice over internet protocol (VoIP) reliability research*. Obtenido de Open Access: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85100391524&origin=resultslist&sort=plf-f&src=s&st1=QoS+in+voip&nlo=&nlr=&nls=&sid=0f4edd64c2bdf9bd154f29b aa7c47a02&sot=b&sdt=b&sl=26&s=TITLE-ABS-KEY%28QoS+in+voip%29&relpos=62&citeCnt=1&searchTerm=>

Rudich, E. (2023). *Cómo utilizar QoS para garantizar la calidad del acceso a Internet*. VASExperts. Obtenido de <https://vasexperts.com/es/blog/quality-of-service/how-to-use-qos-to-ensure-the-internet-access-quality/>

Sánchez, A. (2021). *El teléfono basado en software, el softphone*. Obtenido de 3CX.es: <https://www.3cx.es/blog/el-telefono-basado-en-software-el-softphone/>

- Sellan, P. F. (Octubre de 2020). *DISEÑO DE UN PROTOTIPO DE SISTEMA VOIP Y VIDEOCONFERENCIA MEDIANTE RASPBERRY*. Obtenido de REPOSITORIO DE UNIVERSIDAD ESTATAL: <http://repositorio.ug.edu.ec/handle/redug/49473>
- Solis, L. D. (2020). *El enfoque de la investigación: La naturaleza del estudio*. Obtenido de Investigalia: <https://investigaliacr.com/investigacion/como-se-escoge-el-enfoque-de-una-investigacion/>
- Strzeciwilk, D. (2021). *Performance Analysis of VoIP Data over IP Networks*. Obtenido de International Journal of Electronics and Telecommunications.: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85126659055&origin=resultslist&sort=plf-f&src=s&st1=QoS+in+voip&nlo=&nlr=&nls=&sid=0f4edd64c2bdf9bd154f29b aa7c47a02&sot=b&sdt=b&sl=26&s=TITLE-ABS-KEY%28QoS+in+voip%29&relpos=64&citeCnt=0&searchTerm=>
- Tandel, H., & Rughani, P. H. (2017). Forensic Analysis of Asterisk-FreePBX based VoIP Server . *International Journal of Emerging Research in Management & Technology*, 166.
- TechTarget, D. (2021). Calidad de servicio o QoS. *ComputerWeekly.es*. Obtenido de <https://www.computerweekly.com/es/definicion/Calidad-de-servicio-o-QoS>
- Terreros, D. (2022). *Hubspot*. Obtenido de VoIP: ¿Qué es y cuál es su función? - Higo.io: Maximiza el flujo de efectivo de tu empresa: <https://blog.hubspot.es/service/que-es-voip>

- Valverde, A. M. (2017). *Semantic Scholar*. Obtenido de Implementar y fortalecer redes computacionales mediante herramientas Open Source para las pymes en Ecuador: <https://www.semanticscholar.org/paper/Implementar-y-fortalecer-redes-computacionales-Open-Valverde-Fajardo/2f689c98f975cce6ab348a55156970fa0954846c>
- Vive, U. (2021). *UNIR*. Obtenido de Metodologías del PMI (Project Management Institute): claves e importancia: <https://www.unir.net/ingenieria/revista/metodologias-pmi/>
- Westreicher, G. (2022). *Economipedia*. (Economipedia, Editor) Obtenido de Encuesta: <https://economipedia.com/definiciones/encuesta.html>

Anexo

Anexo 1

5.1 Encuesta

Esta encuesta se la realizó a una población de 22 trabajadores pertenecientes a la empresa SERVIZAM durante el 21 de junio del presente año.

Sistema de telefonía VoIP aplicando con QoS para mejorar la comunicación empresarial de SERVIZAM CIA.

Este cuestionario está destinado a todos los empleados de SERVIZAM CIA.
El propósito de esta encuesta es determinar las necesidades de comunicación entre los empleados de una empresa.

1. ¿A que departamento o área usted pertenece? *

- Atención al cliente
- Financiero
- Marketing
- Recurso Humano
- Bodega
- Gerencia
- Operaciones
- Administración

2. ¿Qué características consideras fundamentales para un sistema de VoIP en SERVIZAM CIA.?

*

- a) Escalabilidad para soportar el crecimiento de la empresa
- b) Funciones adicionales (grabación de llamadas, conferencias, mensajes de voz, etc.)
- c) Seguridad avanzada (encriptación de llamadas, autenticación de usuarios, etc.)
- d) Calidad de audio excepcional

4. ¿Cuáles de los siguientes aspectos de QoS son prioritarios para tu sistema de VoIP? (Selecciona una opción)

- a) Latencia baja: Minimizar el retardo en las llamadas.
- b) Ancho de banda adecuado: Garantizar suficiente capacidad para transmitir el tráfico de voz.
- c) Jitter controlado: Reducir la variación en el retardo de paquetes.
- d) Seguridad de extremo a extremo: Proteger las comunicaciones VoIP contra amenazas y ataques.

5. ¿Qué tipo de medidas de seguridad consideras necesarias para proteger las llamadas VoIP en tu sistema? (Selecciona una opción)

- a) Encriptación de llamadas: Codificar la comunicación para evitar escuchas no autorizadas.
- b) Autenticación de usuarios: Verificar la identidad de los participantes en las llamadas.
- c) Control de acceso: Limitar quién puede realizar o recibir llamadas.
- d) Detección y prevención de ataques: Identificar y bloquear intentos de ataques en tiempo real.
- e) Actualizaciones regulares de software: Mantener el sistema VoIP actualizado con parches de seguridad.
- f) Monitorización del tráfico: Supervisar y analizar el tráfico de VoIP en busca de actividades sospechosas.

6. ¿Qué nivel de disponibilidad deseas para tu sistema de VoIP? *

- a) Alta disponibilidad: El sistema debe estar disponible en todo momento, sin interrupciones.
- b) Disponibilidad razonable: Se aceptan interrupciones ocasionales, pero se espera que el sistema esté mayormente disponible.
- c) No es una prioridad: La disponibilidad del sistema VoIP no es un factor relevante para mi compañía.

7. ¿Deseas funciones adicionales en tu sistema de VoIP? *

- a) Conferencias Telefónicas
- b) Identificador de llamadas
- c) correo de voz
- d) No necesito funciones adicionales

Anexo 2

5.2 Entrevista

Se realizó una entrevista previa a la implementación al gerente de la empresa SEPRIVZAM.



SEPRIVZAM
SEGURIDAD PRIVADA ZAMBRANO

ENTREVISTA

Esta entrevista esta dirigida al gerente de la compañía de seguridad privada SEPRIVZAM SA.

Correo *

jpzambrano8@gmail.com

1. ¿Que medio de comunicación manejan internamente con sus colaboradores? *

Por el momento nos mantenemos en comunicación con los telefonos convencionales y por grupo de Whatsapp y por radio motorola.

2. En esta nueva propuesta, ¿Que consideran necesario dentro de este sistema?

La seguridad, permitirnos ver quien realiza las llamadas, que las llamadas se mantengan controladas y grabada que únicamente entre nosotros y nuestro cliente, mantener controlada la gestión de los colaboradores, nos interesa mantener nuestros datos y los de nuestros clientes seguros.

3. ¿Alguna vez han manejado este tipo de sistemas?

Si, pero de forma virtualizada

4. Una vez contando con el sistema de VoIP, ¿Cual sería el uso que le van a dar?

Llamadas entre departamentos de la empresa y también a futuro a los clientes en las urbanizaciones.

5. Una vez habiendo probado el uso y manejo del sistema VoIP ¿Considera necesario extender el uso del mismo a departamentos externos de su empresa?

Si, ya que poco a poco crecemos y nos interesa mantener esa comunicación con los demás departamentos.

6. ¿Cuál es su proveedor y la velocidad de conexión de la banda ancha en esta red? *

En la red Consta de fibra óptica, lo que garantiza un ancho de banda de 200 Mbps lo que contratamos.

7. ¿Cuál es la topología de red utilizada en esta red? *

En la empresa manejamos una topología de árbol.

8. ¿Cuántos colaboradores maneja bajo su cargo en el empresa? *

En la empresa consta de 21 personas trabajando en los diferentes departamentos

Anexo 3

5.3. Carta de autorización



CARTA DE AUTORIZACIÓN

Guayaquil, 27 de marzo. del 2023.

Ing. Paul Zambrano Loor
Presidente
SEPRIVZAM CIA. LTDA

De mis consideraciones:

A través del presente, autorizo al señor Fariño Díaz Leonardo Manuel con cédula de ciudadanía N° 0929313260 estudiante de la Facultad Ingeniería de la carrera Ingeniería en Sistemas de la Universidad Ecotec para que pueda recopilar información de nuestra empresa con el objetivo de desarrollar su trabajo de titulación que le permita obtener su grado profesionalizante.

Asimismo, autorizamos la divulgación y publicación de los resultados de su investigación en los repositorios que la Universidad Ecotec tenga destinado para este fin.

Atentamente,


Ing. Paul Zambrano Loor.
PRESIDENTE
SEPRIVZAM CIA. LTDA.



 0995452657
 0997126288
 0997121234

 seprivzam@gmail.com

 Alejo Lascano 1411 y los Rios

Anexo 4

5.4. Cronograma de actividades.

Durante un periodo de 7 semanas, se llevaron a cabo diversas actividades para configurar, implementar y mejorar el sistema de telefonía IP basado en el servidor PBX de Issabel a continuación:



EMPRESA: SEPRIVZAM CIA. LTDA **PERIODO:** 17 de mayo al 5 de Julio.
RESPONSABLE: Leonardo Fariño.

CRONOGRAMAS DE ACTIVIDADES

No	Actividades Detalle	Responsable	Semanas							
			1	2	3	4	5	6	7	
1	Requisitos para la implementación.	Leonardo Fariño	■							
2	Verificación de estado de Red y Topología.	Leonardo Fariño	■							
3	Característica del computador.	Leonardo Fariño	■							
4	Instalación y configuración de Issabel.	Leonardo Fariño		■						
5	Creación de extensión para los diversos departamentos.	Leonardo Fariño		■						
6	Instalación de softphones en los diversos computadores de los departamentos.	Leonardo Fariño		■						
7	Configuración de las extensiones en los softphones en los diversos departamentos.	Leonardo Fariño			■					
8	Verificación del funcionamiento del servidor	Leonardo Fariño			■					
9	Prueba de llamada a diversos Softphone de un departamento a otro.	Leonardo Fariño			■					
10	Verificación de vulnerabilidades en el servidor.	Leonardo Fariño				■				

0995452657
 0997126288
 0997121234

seprivzam@gmail.com

Alejo Lascano 1411 y los Rios

